Information Security Education & Awareness

Ministry of Electronics and Information Technology
Government of India

Information Security Awareness
for Master Trainers

cert-in

सी डैक
CDAC

CONTENTS

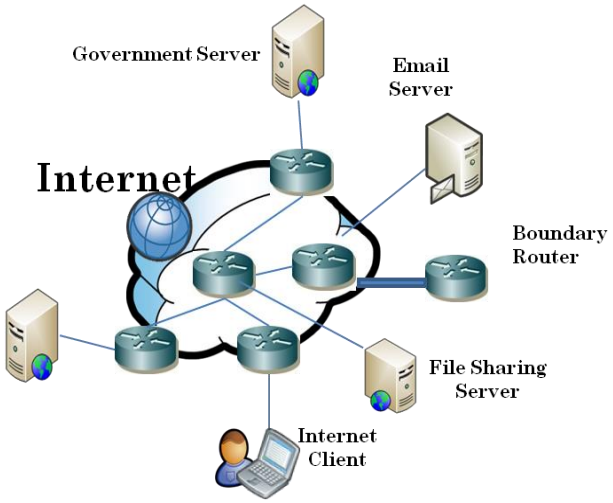
Chapter 1:

Internet Fundamentals

1. INTERNET FUNDAMENTALS

1.0 INTRODUCTION

The **Internet** is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide. It is an international *network of networks* that consists of millions of private, public, academic, business, and government packet switched networks, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), the infrastructure to support email, and peer-to-peer networks for file sharing and telephony.



The origins of the Internet date back to research commissioned in the 1960s to build robust, fault-tolerant communication via computer networks. While this work, together with work in the United Kingdom and France, led to important precursor networks, they were not the Internet. There is no consensus on the exact date when the modern Internet came into being, but sometime in the early to mid-1980s is considered reasonable. From that point, the network experienced decades of sustained exponential growth as generations of institutional, personal, and mobile computers were connected to it

In the present age of information Technology, use of Internet is becoming very popular for accessing information like:

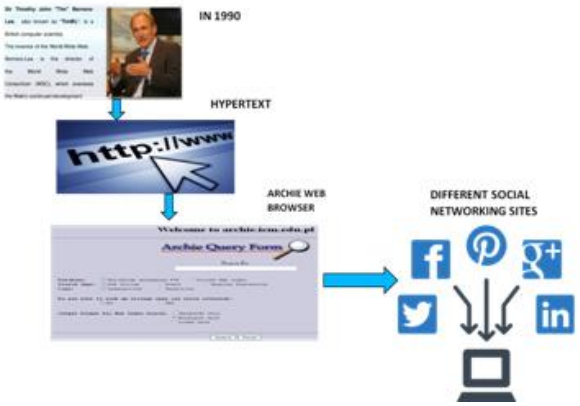
- Instant messaging
- Downloading Documents
- Audio and Video calling
- Listening and Downloading Music
- Internet Forums
- Online shopping etc.

The Internet has enabled and accelerated new forms of human communications through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small traders.

This freedom of Internet helped it to move out of its original base in military and research institutions, into elementary and high schools, colleges, public libraries, commercial sectors even into the shop of a vegetable vendor.

1.1 THE HISTORY

WWW was invented in 1990 by British computer scientist Sir Tim Berners-Lee to use hypertext "to connect and access information of various kinds as a web of computers in which the user can browse. The first Internet search engine named as Archie was found in 1990. Three years later, in 1993, W3Catalog and Aliweb Search engines for the World Wide Web were launched. This was followed by WebCrawler, Aggregator, Go.com and Lycos in 1994 and AltaVista, Daum, Magellan, Excite, SAPO and Yahoo in 1995. 1998 saw the birth of Google and MSN search.



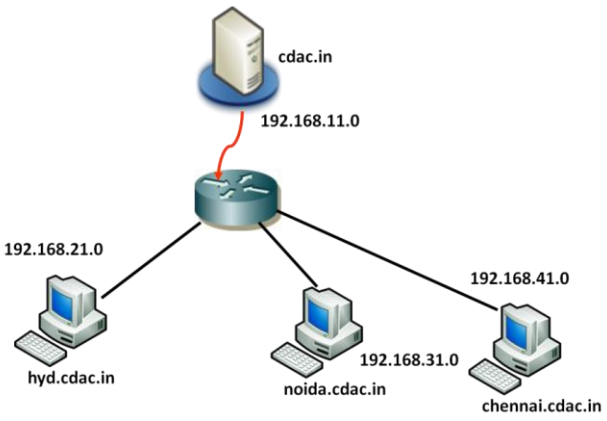
From 1997 to 2007 several social networking websites were launched including Orkut, Facebook, twitter, LinkedIn, YouTube and windows live etc. The major social network to be launched is Google Plus which was launched in 2011.

Tip: Many People think that email is one of the best Internet applications. But in reality email was invented before the Internet.

1.2 HOW INTERNET IS MANAGED

The Internet is managed is managed in below categories:

a) **Naming and Addressing**: Computers talk to one another using an 'Internet Protocol'. It is divided into IP address & Generic top level domains. Internet Protocol (IP) addresses are single numeric identifiers that are required by every device that connects to the global Internet. The numeric identifier is assigned to a device that enables data to be perfectly transported between start and end points within a network or networks.



Internet Assigned Numbers Authority (**IANA**) is responsible for:

- The global organization of the Internet Protocol addressing systems

- The global organization of the Autonomous System Numbers used for routing Internet traffic and
- Other practical parameters connected with Internet

ICANN - Internet Corporation for Assigned Names and Numbers is responsible for IP Address space allocation, its operation, Evolution of Domain Name System and coordination of the policy related to technical parameters to work.

ASO - ICANN Address Supporting Organization

ASO reviews and develops recommendations on Internet number resource policy and advises the ICANN board.

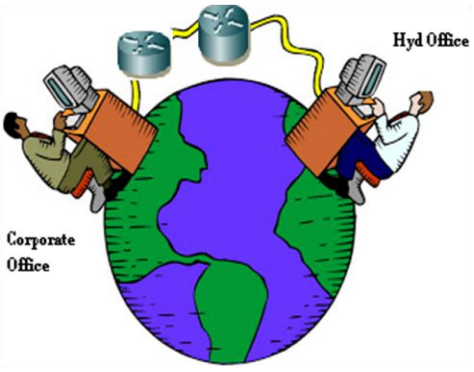
RIRs - Regional Internet Registries

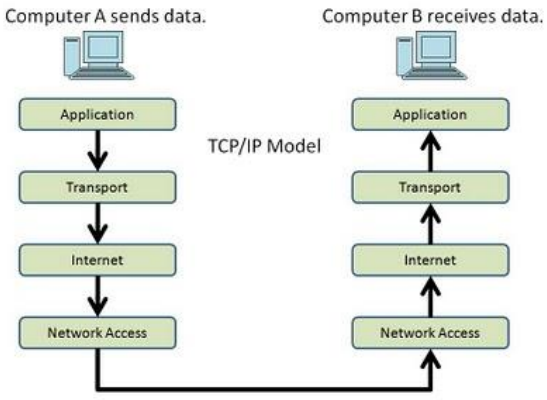
Within their assigned regions, RIRs are responsible for allocating Internet number resources such as globally unique IP addresses (IPv4 and IPv6) and autonomous system numbers. These resources are required by Internet service providers and users to identify elements of the basic Internet infrastructure such as interfaces on routers, switches and computers.

APNIC: Asia Pacific Network Information Centre (APNIC) is the not-for-profit regional Internet registry for the Asia Pacific region. APNIC provides number resource allocation and registration services that support the global operation of the Internet.

1.3 ARCHITECTURE OF THE INTERNET

The basic idea behind the architecture of the Internet is in the specification of the standard TCP/IP protocol. TCP/IP is designed to connect any two networks which may be different in hardware, software, and technical design. Once two networks are interconnected, communication with TCP/IP is enabled end-to-end. This means that any node on the Internet can communicate with other nodes.

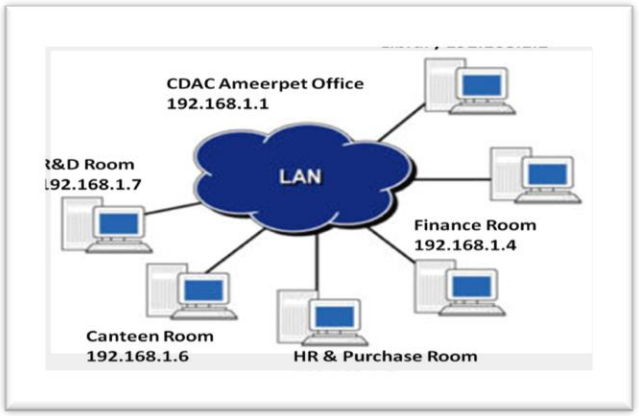




In practice, the Internet architecture looks a small fragment of water like a multi-dimensional river system, with small tributaries feeding medium-sized streams feeding large rivers. For example, an individual's access to the Internet is often from home over a modem to a local Internet service provider who connects to a regional network connected to a national network.

At the office, a desktop computer might be connected to a local area network with a company connection to a corporate Intranet connected to several national Internet service providers.

1.4. BASICS ON NETWORKING



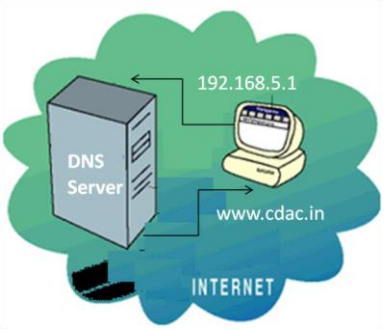
One of the most primary concepts while understanding the working of the Internet is IP address (Internet Protocol address). Every computer on the Internet has a unique identification number called an IP address. Computers identify each other by IP addresses, which are numbers. The other essential concept is that of domain names. Consider a website such as www.google.com which is hosted on a computer having some IP address.

LOCAL AREA NETWORK (LAN):
A local area network is a computer network that interconnects computers within a limited area such as a home, school, and computer laboratory, or office building, network using Media

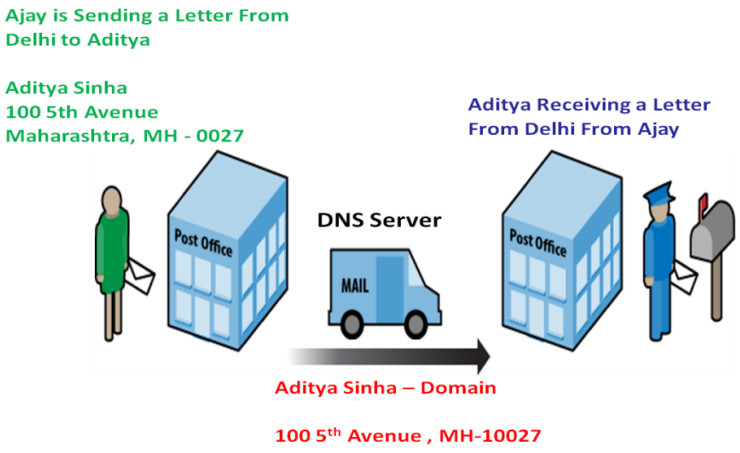
METROPOLITIAN AREA NETWORK (MAN):
A data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are generally characterized by very high-speed connections.

WIDE AREA NETWORK (WAN):
A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area network

DNS: The Domain Name System (DNS) is a system used to convert a computer's host name into an IP address on the Internet. For example, if a computer needs to communicate with the web server **www.cdac.in** your computer needs the IP address of the web server www.cdac.in. It is the job of the DNS to convert the host name to the IP address (**192.168.5.1**) of the web server.



It uses TCP & UDP port 53 and when you type www.cdac.in into your browser, your browser sends a query over the Internet to find the website www.cdac.in.

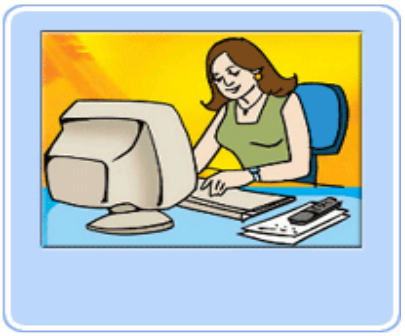


The Domain Name System is a collection of root servers that consists the Internet Protocol (IP) addresses of the DNS name servers that have authority over individual domains of every registered Internet domain name.
With this system, web site users only need to know your domain name to find your web site, it does not matter to them what the IP address is for the individual server on which your site is housed. DNS is very similar to the postal addressing system with two main components: a name, and a further full, numerical address. If you're sending a letter to someone, say, Aditya who lives in Maharashtra, you'd address it such:

With the Internet, the "name" is called a domain, and the "numeric address" part is an IP (Internet Protocol) address. But unlike sending a letter, as a regular user on the Internet, you don't have to know the numeric address of your site, just the domain name!

Aditya Sinha, 100 5th Floor, Maharashtra, MH 10027
DNS syncs up domain names with IP addresses enabling humans to use memorable domain names while computers on the Internet can use IP addresses.
For Example: We will take the following website as an example **www.abc.com**
Fully Qualified Domain Name (FQDN) – **www.abc.com**
The left most name before the first period is always the host name or the name of the server.
In this case the server's zone is "abc.com".
"ABC" is a subzone of ".COM", while ".COM" is a subzone of the root zone "."

1.5. HOW INTERNET WORKS



There are several different ways that Internet works, the following are the terms discussed below:

CONNECTING TO THE INTERNET:

Step 1: To connect to the Internet, your dialer software calls an access number:

Step 2: Your modem converts the signals from your computer to signals that travel over wire lines to an Internet Service Provider (ISP)

Step 3: Your ISP provides a connection to the Internet

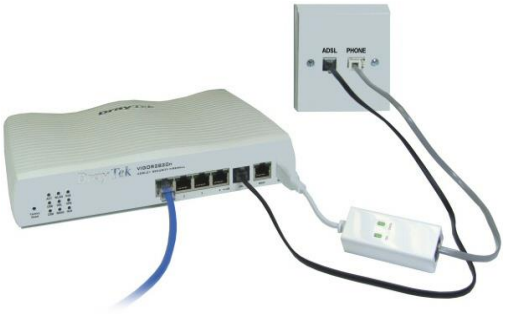
Step 4: Imagine you want to go shopping

1. You get in your car
2. You tell the gate operator where you are going
3. He sends you down the correct path

Tip: Modems recognize addresses as **www.abcgoing.com** or **http://abcgoing.com**
It's just like someone giving you their street address, these address identify where a website sits on the web, they are also known as domain names.

a) Dial-up: With a dial-up connection, the Internet user can connect to the Internet via telephone line and an Internet service provider (ISP).

b) Broadband: Cable and DSL are in this category. With a cable connection, the user must subscribe to a cable-television/Internet service. These connections offer speeds up to 70 times faster than dial-up.



BROADBAND INTERNET SECURITY

Broadband refers to high-speed network connection**.** Traditional Internet services are accessed in "dial-on-demand" mode, whereas broadband Internet is an "always-on" Connection, therefore security risk is very high

Without our knowledge, computer can be compromised and it can also be used as a launching pad for carrying out disrupting activities on other computers. Since broadband Internet is widely used, it is very important for every citizen to securely configure it for safe usage

BROADBAND SECURITY THREATS:

- As broadband Internet connection is "Always On" , it leads to intentional misuse through
  - Trojans and backdoors
  - Denial of Service
  - Intermediary for another attack
  - Hidden file extensions
  - Chat clients
  - Packet sniffing
- Default configurations are extremely vulnerable

TYPES OF BROADBAND MODEM:

- Wireless Fidelity (Wi-Fi)
- Digital Subscriber Line (DSL)
  - Asynchronous Digital Subscriber Line (ADSL)
  - Very high speed Digital Subscriber Line (VDSL)
- Cable Modem
- Satellite
- Broadband over Power lines (BPL)
- Terminal Adapter Modem
- Universal Serial Bus (USB)

Anti-socialism groups use unsecured Wi-Fi networks to send terror e-mails and Prevent your wireless network to become such a hot spot by securing it

BROADBAND MODEM SETUP:

- Always read the manufacturer's manual carefully and follow the guidelines, while setting up broadband modem.
- Insert the power source into the modem and then plug the other end of it into the wall socket.
- Before connecting the modem to the computer, check for proper functioning of the computer.

- While setting up the modem, follow instructions specific to the type & model of the modem.
- In case of signal via cable, connect the modem with the cable wire provided.
- In case of Ethernet, connect the modem to the Ethernet port of the computer.
- In case of USB connection, connect the modem after the computer is properly initialized.
- Wait until the indicators on the modem are lit.
- Install the modem driver and associated software provided along with the modem.
- To initialize the connectivity the proper user credentials need to be given and response should be awaited before use.

GUIDELINES FOR SECURING BROADBAND INTERNET ACCESS:

Do's

1. Always download broadband drivers from the legitimate websites recommended by the manufacturer.
2. Regularly download the firmware (driver code)
3. Always use the power adapter supplied by the manufacturer along with the modem.
4. In case of terminal adapter modem make sure that filter is enabled for broadband lines. To filter unnecessary noise generated during the transmission.
5. Change Default Administrator (Passwords and User names) :

In order to allow only authorized access to the equipment, change the default administrator or admin password of broadband router modem, as these details are given by the manufacturer which are common to all modems and can be misused by anyone.

6. Assign Static IP Addresses to Devices:

Most of the home users are allotted dynamic IP addresses, as DHCP technology is easy to setup. This may even help the attackers who can easily obtain valid address from DHCP pool. Therefore turn off DHCP option in router or access point and use fixed IP address range.

6. Enable MAC Address Filtering:

Every device is provided with a unique MAC address. Broadband access points and router & provide an option for the user to combine the MAC address of the home equipment for access. This facilitates to allow connections only from those devices.

7. Enable Wireless Security*:*

Modem routers support wireless security. User can select any one protocol and a protection key. The same wireless security protocol and protection key has to be enabled in computer.

8. Turn on (Compatible) WPA / WEP Encryption:

All Wi-Fi enabled modems/router support some form of encryption technology, which has to be enabled.

9. Change the Default SSID (Service Set Identifier):

All the access points and routers use a network name called SSID. Manufacturer normally ships their products with the same SSID set. As it can be misused by the attacker to break into the network / computer, it is necessary to change the default SSID while configuring wireless security.

10. Use effective end point security solution (with anti-virus, anti-spyware, desktop firewall etc.) to protect computer/ laptop from broadband Internet security threats.

11. Enable Firewall on Modem Router as well as Computer:

Broadband modem routers contain built-in firewall feature, but this option has to be enabled. Computer connected to the broadband modem also needs to be protected with desktop firewall.

12. Turn off Modems during extended periods of Non-Use:

Shutting down a network will certainly prevent outside unauthorized people breaking into the network. Since it is very difficult to frequently turn on and off the devices, it can be considered during travel or extended offline period.

13. In case of USB broadband modem, disconnect and remove the device after usage.

14. Install broadband Internet bandwidth usage monitoring tool.

15. Enable SSH (secure channel) for remote administration.

GUIDELINES FOR SECURING BROADBAND INTERNET ACCESS:

Don'ts:

- Don't enable the option for remote administration (via Internet), as it is not required for a home user.
- Don't enable the option "**Restore Factory Default Setting**" in broadband modem.
- Don't use connection without a filter for each broadband Internet line.
- Don't tap the line before the splitter (a small device that separates phone line from data / PC port).
- Don't use USB broadband modem with insecure computer/laptop.
- ***Do not Enable SSID Broadcast:***
  In Wi-Fi networking, wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses as well as to access public hotspots. For a home user this feature is unnecessary and can be an entry point to break into the network.
- ***Do not Enable Auto-Connect to Open Wi-Fi Networks:***
  In case if Auto-Connect setting are enabled, computer with Wi-Fi interface can connect automatically without notifying to the user. This may expose our computer to security risks. This setting should not be enabled except in specific cases.
- Do not leave broadband connectivity open when it is not utilized.

- Never connect to unknown or untrusted network in case of Wi-Fi.

Points to be remembered: *The setup, configuration and the features may vary from model to model. For more information please refer manufacturer's manual. Many home computers are victims of cyber criminals and prevent your computer from becoming a victim by securing it*

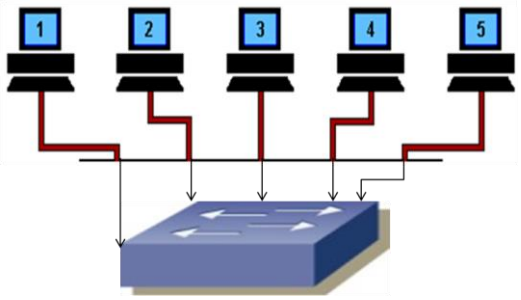
c) A **client** is computer on the network that requests services from another computer on the network. For doing this client should have enough access permissions.

d) Server: A server is a computer that receives requests from client computers, processes these requests, and sends the output to the respective client computers that had placed the requests.

e) Web Server: A Web server is a computer that is dedicated to provide Web services to clients on the Internet. Web services are often provided through Web sites that are hosted on a Web server that is accessed by a client.

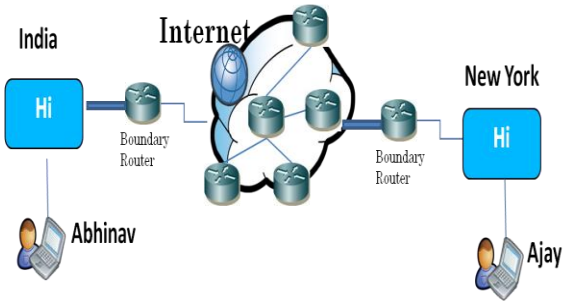
f) Browser: To access the content of a Web site, users must have a browser that can help them locate a Web site on the Internet and then view the content of a Web page. Users can also use the browser to download and upload files on the Internet.

g) Wi-Fi: It's still possible to connect to the Internet wirelessly from home or while you are out. Wireless technology allows users to have mobile connections, accessing the web where and when they need to. Wi-Fi networks can be found at many businesses, restaurants, and other public areas (Airports, parks, schools, libraries, shopping malls etc.) or a home connection can be set up through your ISP.



h) Switch: A network switch is a networking device that connects devices together on a computer network, by storing a MAC address of the devices to forward data to the destination device. Switches create a network.

I) Router: It is a network device which connects two different networks. A router links computers to the Internet, so users can share the connection. It also decides for the best path data should travel to destination address.



g) Firewall: It is a network security system that controls the incoming and outgoing network traffic based on an applied rule set.

1.6. FEATURES OF INTERNET

Email is now an essential communication tools in today's world and you can send and receive instant electronic messages, which work like writing letters. Your messages are delivered directly to people anywhere in the world. Email is free, fast and very cheap when compared to telephone, fax and postal services. And moreover it is available 24 hours a day - 7 days a week: Internet is available, 24x7 days for usage.

Tip: Share your e-mail address with only trusted sources

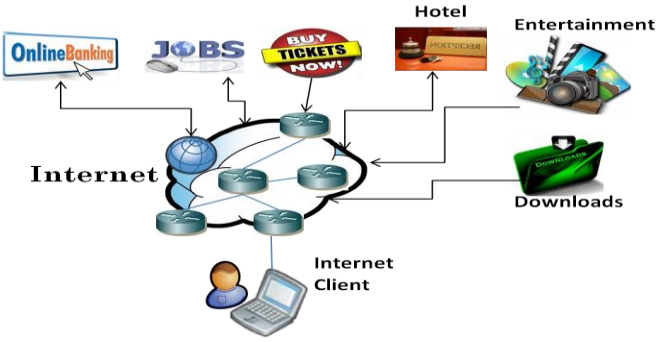
Information: Information is the major advantage Internet is offering. There is a vast amount of information available on the Internet every subject, ranging from government law and services, Business fairs and conferences, market information, new ideas and technical support. You can almost find any type of data on almost any kind of subject that you are looking for by using search engines like Microsoft Internet Explorer, Goggle, Yahoo, msn, Bing etc.

Tip: Do not enclose your personal information like Name, Age; Mobile number and Bank PIN number to the pop-up's displayed during Internet browsing.

Online Chat: You can access many chat rooms on the web that can be used to meet new people, make new friends, as well as to stay in touch with parents, friends and old friends.

Tip: Protect yourself by using a nickname for your IM screen name. Never accept strangers into your IM groups.

Services: Many services are provided on the Internet like net banking, job searching, purchasing tickets, hotel reservations, guidance services on array of topics engulfing every aspect of life.



E-commerce: You can shop online using some retail sites available on the Internet that can be used to look for products as well as buy them using your debit, credit card, Internet banking and Cash Wallet option available on the website's provided. You do not need to leave your home and can do all your shopping from the convenience from your home. It has got a real amazing and wide range of products

from household needs, electronics to entertainment etc.

Tip: Always Shop online and banking related activities using through Secure Socket Layer websites i.e. https

Entertainment: Internet provides facility to access wide range of Audio/Video songs, plays films. Many of which can be downloaded. One such popular website is YouTube.

Tip: Always respect the software piracy and read "Terms & Conditions" while downloading any documents, music files, films and any software's from the Internet

Software Downloads: You can freely download innumerable, software's like utilities, games, music, videos, movies, etc. from the Internet.

1.7. LIMITATIONS OF INTERNET

Geographic sharing

The geographic sharing of the Internet continues to spread, around the world and even beyond. A main feature of the Internet is that once you have connected to any part of it, you can communicate with all of it.

Architecture

The architecture of Internet is most ever communication network designed. The failure of individual computers or networks will not affect its overall reliability. The information will not change or destroy over time or while transferring in between sites.

Universal Access

It is easy to access and make the information like text, audio, video and also accessible to a worldwide people at a very low price. The access to the Internet is same to everyone no matter where they are. You can connect to any computer in the world, and you can go to many excited places without leaving your chairs.

- The Internet is data and information loaded, including a range of medium. The Search engines that are available online are, fast and powerful.
- The Internet is easy to use and using it students can become researchers because of easier access to data.
- The Internet appeals to different learning styles. Unlike paper the web can present dynamic data sources which change over time.
- The characters in an e-Mail don't get transposed or mixed up when they are sent over long distances and can access to libraries around the world.

The Internet is a time-efficient tool for teachers that enlarge the possibilities for curriculum growth. Learning depends on the ability to find relevant and reliable information quickly and easily, and to select, understand and assess that information. Searching for information on the Internet can help to develop these skills. Classroom exercises and take-home assessment tasks, where students are required to compare website content, are ideal for alerting students to the requirements of writing for different audiences, the purpose of particular content, identifying

and judging accuracy and reliability. Since many sites adopt particular views about issues, the Internet is a useful tool for developing the skills of distinguishing fact from opinion and exploring subjectivity and objectivity.
The Internet is a great tool for developing student's or children communication and collaboration skills. Above all, the Internet is an effective means of building language skills. Through e-Mail, chat rooms and discussion groups, students learn the basic principles of communication in the written form. This gives teachers the opportunity to incorporate Internet-based activities into normal literacy programs and bring a variety to their teaching strategies.

Collaborative projects can be intended to improve students' literacy skills, generally through e-Mail messaging with their peers from other schools or even other countries. Collaborative projects are also useful for engaging students and providing significant learning experiences. In this way, the Internet becomes an effective means of advancing intercultural understanding. Moderated chat rooms and group projects can also provide students with opportunities for collaborative learning.

Privacy Issues

Many children are skilled navigators of the Internet. They are comfortable using computers and are fascinated by the information and images that can be explored at the click of a mouse. Recent figures show that 90% of school-age children have access to computers either at home or at school. The ability to interact and communicate with others is one of the biggest attractions of the Internet for children. We are watching about spending time with people in chat rooms and instant messaging through mobiles, playing games, entering contests and filling forms in popular online activities. Unfortunately, most parents don't really understand how such activities can put their children's privacy at risk or even threaten their safety. Surprisingly in India, Most parents never know about some of the activities how their child is participating in Internet.

In today's Internet communications scenario, the personal data is a valuable and protecting the same has become a skill that the children need to understand and learn.

Children privacy can be compromised in certain online activities:

- On filling forms for various surveys, contests, download games on commercial or free web sites.
- Giving details about personal information when registering for e-mail access, Chat access.
- Providing information when registering for free game downloads.
- Providing information when registering for social networking web sites.

Some websites prompt students to complete a form revealing their name, e-Mail address, age and gender, and sometimes even their telephone number and postal address, in order to access information. Some requests are legitimate: much depends on the nature of the website

requesting the information. Providing personal information online can result in a student being targeted for spam (unsolicited e-Mail), advertising materials and/or viruses. Privacy issues also apply to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illicit purposes.

Peer To Peer (P2P) Networking

A peer to peer (or P2P) computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core services. Sharing content such as audio, video, data or any form of digital data by connecting the nodes via largely ad hoc networks.

Risks in Peer to peer networking due to their unstructured networks and sharing with unknown computers or persons may rise to affect or infect your computers with viruses, spams.

Exposing your Computer to Unwanted Software

Usually, many peer-to-peer file sharing programs do not employ good security or access control. If users are not familiar with the programs or improper configuration of the settings, it will be dangerous for all the contents stored in user's hard disk to be exposed to other users.

Contracting Computer Viruses

Besides, the computers of P2P software users can easily contract computer viruses especially when the file downloaded is from an unknown source. Moreover, these P2P programs may also contain viruses and worms, which prevent users' computers from functioning properly.

Infringing Copyright

Many copyright laws infringing copies of entertainment files e.g. MP3 Music files, VCD video files etc. and software are often shared by P2P software.
The act of unauthorized uploading of a copyright works for others to download may attract civil or even criminal sanctions. Unauthorized downloading of copyright works entails civil liability.

Slowing down your School Internet Speed

Last but not least, if you host a large amount of files for other people to download through P2P software via the School campus network, the network traffic thus created can slow down the entire campus network.

Tips for P2P Networks

- Install file sharing (P2P software) carefully so that what files or Directory you are sharing and what's being shared to other systems in P2P network.
- Use filtering software you trust to filter the data communication from your system.
- Use file sharing program controls and adjust the P2P program to run whenever you required. Disable automatic starting.
- Always update Operating System, Antivirus and Anti Spyware packages.

- Do not use an administrative account. It may expose the whole system to other users in P2P networks. Create separate account for normal operations.
- Treat all download files with suspicion.
- Take back up of important files. This will help you in recovering the files.
- Delete any pirated software, files, etc. Alternatively, do not download them at all.

1.8. CONCLUSION

The Internet is used mainly for communication, to gather information, education, entertainment, current affairs, online learning, commerce, publishing, etc. By the Internet, hundreds of thousands of people around the world are making information accessible from their homes, schools, and workplaces. The architecture of Internet is most ever communication network designed. The failure of individual computers or networks will not affect its overall reliability. The information will not change or destroy over time or while transferring in between sites.

It is easy to access and make the information like text, audio, video and also accessible to a worldwide people at a very low price. The access to the Internet is same to everyone no matter where they are. You can connect to any computer in the world, and you can go to many excited places without leaving your chairs.

The Internet is a very big storeroom of learning material. As a result, it significantly expands the resources available to students beyond the standard print materials found in school libraries. It gives student's access to the latest reports on government and non-government websites, including research results, scientific and inventive resources in museums and art galleries, and other organizations with information applicable to student learning.

The Internet is used mainly for communication, to gather information, education, entertainment, current affairs, online learning, commerce, publishing, etc. In the usage of Internet, publishing means it is not just used for organization or businesses; anyone can create their own web sites and publish their information or files on the Worldwide.

By the Internet, hundreds of thousands of people around the world are making information accessible from their homes, schools, and workplaces. The Internet is a global collection of computer networks, help with each other to exchange data using a common software standard. Internet users can share information in a variety of forms.

The user can connect easily through ordinary personal computers and share the knowledge, thoughts by making the use of an Internet. We can send electronic mail (e-Mail) to family members and friends with accounts on the Internet, which is similar to sending letters by post. The E-mail can be sent within minutes no matter where they are without waiting for some procedures like postal stamps etc. We can post information that can be accessed by others and can update it frequently. We can access multimedia information that includes video, audio, and images. We can learn through Web-Based Training and Distance Learning on the Internet.

Chapter2:

Information Security Concepts

2. INFORMATION SECURITY AWARENESS

2.0. NEED FOR INFORMATION SECURITY

In this information age, information is power. Every individual, every organization and every government needs to protect information. An individual is concerned about his or her privacy and hence individual tries to protect his or her information stored in computers. Every organization has to protect its intellectual property to maintain competitive edge and hence protecting information is of paramount importance. A design organization has to protect its designs, a marketing agency has to protect its market strategy information and a hospital has to protect the patients information. Governments need to protect the information for providing national security and public safety.

20th century's greatest innovations are the PC and the Internet. These two have brought in profound changes on all aspects of human life entertainment, education, business, health care, banking, transportation etc. We are all dependent on computers and the Internet even for daily activities. Global village is no longer a dream or utopia, it is a reality. Access to any type of information is just a mouse click away!

As the capabilities of the Internet are enhanced day by day, the need for effective measures for information security also increases tremendously.

2.1. INFORMATION SECURITY:

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Definitions:

The definitions of InfoSec suggested in different sources are summarized below (adopted from).

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)
4. "Information Security is the process of protecting the intellectual property of an organization." (Pipkin, 2000)

5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)
6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)
7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)
8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

2.2. IT SECURITY:

IT security sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

2.3. SECURITY THREATS

Any technology can be used for the human benefits. But any technology can also be used by criminals and anti-social elements. The Internet is now become an excellent platform for criminals. The Internet users now face a number of problems due to the security threats.
Periodically, our computers are affected by viruses. Viruses damage or destroy the information on the computers and they spread very fast. Credit card information is stolen by hackers. The terrorists use the Internet extensively to plan attacks; and information wars are initiated by bombing servers with unwanted malls/network connections.

Security threats will adversely affect individuals. They lose their privacy; they lose confidence in using the Internet for e-commerce transactions; and they lose confidence in the public safety measures if those measures still do not protect them.

If the individuals lose confidence, then the business of enterprises involved in e-commerce is also affected. Enterprises lose millions of dollars due to fraud on the Internet. Enterprise espionage causes both direct and indirect losses to the organization. And, unfortunately, many employees and ex-employees are responsible for enterprise espionage.

2.4. PEOPLE, POLICY, PROCEDURES AND PRODUCTS:

In this information age, every individual should have a good awareness of the security issues, security policies of the organization in which he or she is working and also the laws related to information security. People should also be aware of ethical issues concerning use/misuse of information systems. As information systems are technology-driven, people should also have the necessary technical exposure to security systems and technologies.

Every organization should have a security policy. This security policy reflects the management's commitment to provide secure information systems while protecting the privacy of individuals. Policy also should Indicate the managements approach to introduce new technologies and services and training the employees on information security.

Every organization should work out the detailed procedures for developing information security systems. The procedures should include: identification of the critical information assets, identification of threats to the information systems, finding out the vulnerabilities, taking preventive measures to avoid the threats; working out mechanisms for detection of fraud and recovery of systems after attacks, and for training the people.

For providing security, a number of security products need to be installed in the enterprise. These products include anti-virus software, firewalls, surveillance systems, intrusion detection systems etc. However, just installing these products alone will not provide the necessary security people, policies and procedures are very important.

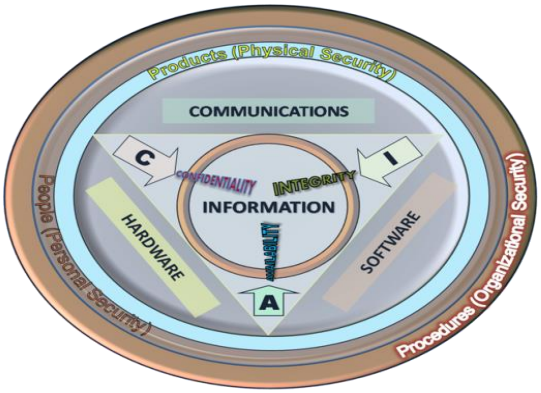
It needs to be emphasized again that people, policies, procedures and products are the four pillars of any security system. Together, they provide the solution for providing physical security, computer security and network security. During the course of this entire training program on Cyber Security, we will study the various aspects of providing this big solution . At this point of time, we all need to appreciate that providing security is not a very easy task, it is a challenge, a great challenge.

2.5. BASIC PRINCIPLES OF INFORMATION SECURITY:

A security system has to provide services for information security. These services are called information security services.

The four services are:

- Confidentiality
- Integrity
- Availability



CONFIDENTIALITY:

Confidentiality service is to ensure the secrecy of information. Only authorized users should be able to gain access to the information. Confidentiality has to be ensured for information stored in the computers in the form of files. Also, while this information is being transmitted through physical means or through a network, it should be ensured that the information reaches only the authorized users.

Another important aspect is to ensure that information about the traffic flow between two end points is kept secret. For example, assume that two organizations A and B are negotiating a merger. It is likely that there will be lot of traffic flow (telephone calls, emails etc.) between the two offices of A and B. If an attacker comes to know that the traffic flow has increased, it is an important input for him as he comes to know that some negotiations are taking place. Confidentiality of traffic flow is also important in such a case.

The access attacks are mainly to obtain confidential information. Hence, confidentiality service tries to prevent access attacks.

INTEGRITY:

Integrity service is to ensure correctness of information. If A sends some information to B, A should be sure that the information received by B is same as that has been sent. B also should be sure that the information sent by A is same as that has been received. Well, there is a possibility that during transit, someone would have modified that information. Integrity service ensures that such a thing has not happened. Integrity service has to be provided for information stored in the computers as well as for the information that is transmitted. Integrity service tries to prevent modification attacks.

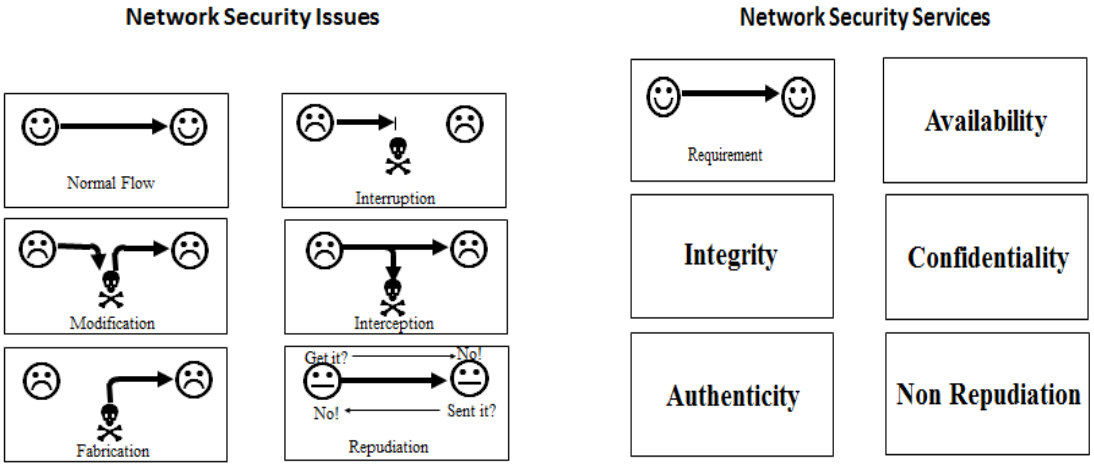
Suppose you receive a credit card bill which says that you purchased a book from an online book store. One possibility is that you have really purchased that book and you got the bill. other possibility is that you did not purchase the book; someone stole your credit card information and made the purchase. It is important for integrity service to ensure that such repudiation attacks are prevented.

AVAILABILITY:

The information infrastructure such as the computers and networks are valuable assets for any organization. If the authorized users are unable to access these computers, then it is a denial-of-service attack. Availability service ensures that the information infrastructure is available to the authorized users. Availability of information stored in computers is ensured through a backup procedure. In case of natural calamities or man-made attacks, the infrastructure may be damaged. In such a case, availability is ensured through a disaster recovery plan.

The attacker may try to destroy the communication Jinks. Availability has to be ensured by providing the necessary redundancy to the communication links. For example, if a leased

line is used for communication between two offices, a redundant link can be obtained through dial-up connections. Availability service is to prevent denial-of-service attacks.



2.6. SECURITY MECHANISMS:

Cryptology:

Cryptology is considered a branch of mathematics and computer science. It has two branches: Cryptography and Cryptanalysis. Cryptography is the science of keeping data secure. Cryptographer will use cryptography to convert plaintext into ciphertext. Cryptanalysis is the science of making encrypted data unencrypted. Cryptanalyst will use cryptanalysis to attempt to turn that ciphertext back into plaintext.

Basic Cryptographic Terminology:

- Plaintext - the original message
- Ciphertext - the coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering plaintext from ciphertext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (code breaking) - the study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - the field of both cryptography and cryptanalysis

2.7. SECURITY SERVICES PROVIDED BY CRYPTOGRAPHY:

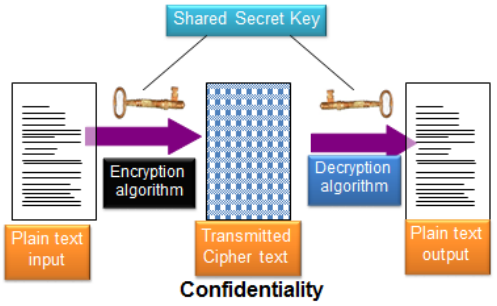
To provide secure communication, cryptography is extensively used. Cryptography facilitates providing the three information security services viz., confidentiality, integrity and non-repudiation. Confidentiality is ensured because only those who know the encryption key can decode the information. Integrity is ensured, to some extent, because only those who know the encryption key have sent the information. Certainly, since authorized users only can send the encrypted information, a user cannot deny that he sent the information and hence non-repudiation is also ensured.

Categories of Encryption:

Encryption can be broadly divided into two categories: Private key encryption and public key encryption.

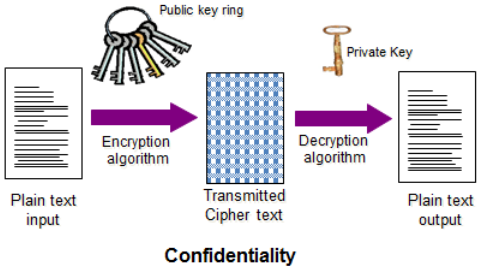
Private Key Encryption:

Private key encryption is also known as symmetric key encryption because the same key is used by both the sender and receiver. As we discussed earlier, the encryption algorithm can be made public that is, known to everyone. However, the encryption key must be kept secret. It is important for the sender and the receiver to come to an understanding which key has to be used. So, a mechanism for distribution of the keys amongst the authorized users needs to be worked out.



Public Key Encryption:

Public key encryption is also known as asymmetric key encryption. In this scheme, there will be two keys one is called public key and one is called private key. Public key is known to everyone you can put all the public keys in a database and make it available on the Internet. Associated with each public key, there will also be a private



key and this key has to be kept secret. So, in public key encryption, there will be a pair of keys one public and one private. As usual, you can make the algorithm public but the private key must be kept secret.

Public key encryption is a very interesting scheme. Its beauty lies in the pair of keys this pair is chosen using number theory.

The Public Key Encryption mechanism is shown in this figure. As mentioned earlier, there will be two keys Key 1 and Key 2. One of the keys is public and one is kept secret. Encryption is done using one key and decryption is done using the second key in the key pair.

Hash Functions:

Hash function is a one-way function i.e., you can create the checksum from the message but you cannot create the message from the checksum. It should also be difficult to create two messages having the same checksum. However, the second property cannot be met always.

Hash functions are of two types: keyed Hash functions and keyless Hash functions. As the names suggest, you need a key to be shared by the sender and receiver in the case of Keyed Hash functions. In the case of keyless Hash functions, there is no need for such a key.

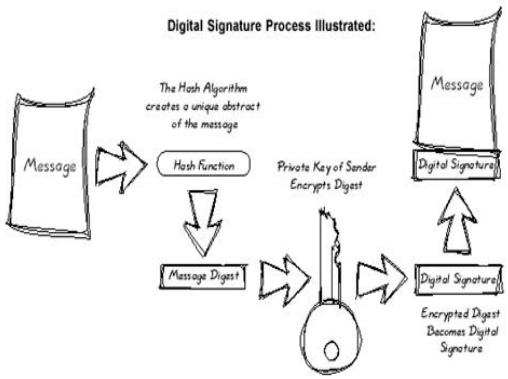
An example of Keyed Hash function is using the DES. The last three blocks of the cipher- text can be used as the checksum. However, this is not a very secure method, because of the weakness of the DES algorithm.

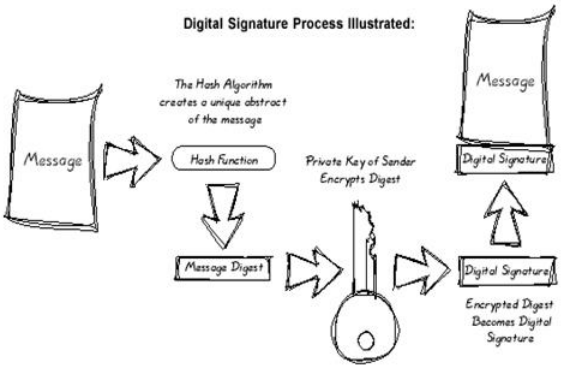
The two keyless Hash functions that are widely used are: MDS (Message Digest 5) and Secure Hash Algorithm-! {SHA-1). MDS produces 128-bit checksum and SHA-1 produces 160-bit checksum. Though many keyless Hash functions have been proposed in the literature, most of them proved to be insecure. MDS and SHA-1 provide a reasonably good message authentication.

Digital Signature:

A general misconception is that digital signature is the scanned version of the human beings signature. It is NOT. A digital signature is created by deriving the checksum from the message bits and then encrypting these checksum bits. This signature is unique for the message in the sense that even if one character in the message is changed, the signature will not match. Hence, this signature can be used to authenticate the contents of the message. The signature can also be encrypted with an encryption key known only to the sender and hence the originator of the message can also be authenticated.

A digital signature can be used by a third party (say, a judge in the court of law) to check whether a message and the origin are genuine. Hence, digital signature provides non-repudiation service.





Digital Certificate

A digital certificate is used to ensure that the public key of a person is really genuine. Digital certificate is a message that contains the public key of a person/organization (we will call it an entity, henceforth); information about the owner of the public key and also how long the certificate is valid. This message will also have a digital signature so that the recipient of this certificate can make sure that the certificate is genuine. Such digital certificates are issued by an authority which can be trusted . Such authorities, generally appointed by Governments, are called Certification Authorities.

Suppose A wants to communicate with B. A obtains B s certificate from the Certification Authority. The Certification Authority s public key is known to A and hence A decrypts the certificate. A also checks whether the certificate is genuine by verifying the signature in the certificate verifying the signature is nothing but checking whether the checksum is valid or not.

2.8. GOALS OF INFORMATION SECURITY:

The Goals

The goals can be broadly divided into:

- Prevention
- Detection
- Recovery

Prevention:

As we all know, prevention is better than cure. But then, it is not always possible to take enough measures to ensure that there will be no attacks. However, the security system should aim to ensure that a possible attack will fail. This is prevention. Some of the examples for preventive measures are: protecting the systems through passwords for preventing unauthorized access to systems or networks; installing anti-virus software on every system so that the files do not get corrupted by the virus that is spread through

emails or floppy disks etc. It needs to be emphasized that it is very difficult to foresee all possible attacks and devise preventive solutions.

Detection:

Another goal for security is detection. This goal is to devise mechanisms to find out that an attack is taking place or an attack has taken place. If the attack is discovered while it is taking place, the damage being done can be monitored and if possible the attack can be stopped. If the attack has already taken place, the damage that has been done should be detected. Detection is followed by working out possible preventive measures so that such types of attacks can be prevented in future.

An example of a detection mechanism is to keep a log of login attempts. If a user is able to login after say, 10 unsuccessful attempts, all the unsuccessful login attempts are recorded in a log file. This log file gives information as to whether the attacker was trying to guess the password. For example, if the user gives the passwords as HELLOl, hellol, hello then the user perhaps is genuine. If the user gives the passwords as johnl, maryl, trial2 etc., he is trying to guess the password and the user is likely to be an attacker. Note that detection mechanism does not prevent the damage being done.

Recovery:

The third goal of security is recovery i.e., to repair the damage done by an attack. An examples of recovery is: when a file is deleted through an attack, to restore that file from the backup. Of course, the underlying assumption is that you have a backup. So, the security system should work out a backup policy. Another example is: if some records in a database were modified by an attacker, to restore the database from a backup. However, it may not always be possible to restore a system to a state it was in before the attack. For example, the database backup may not contain all the latest modifications. However, a recovery mechanism has to be worked out in such a way that the damage is minimal and also the systems can be restored to the original status to the maximum possible extent in minimum possible time.

Chapter 3:

Computer Ethics

3. COMPUTER ETHICS

3.0. COMPUTER ETHICS:

Ethics are a set of moral principles that govern an individual or a group on what is acceptable behavior. This is also applied to computing practices which means computer ethics is set of moral principles to make the use of computers in a proper ethical manner. Duplicating the copyrighted content without the author's approval, accessing personal information of others are some of the examples that violate ethical principles.

3.1. What is the Ethical behavior of students/teachers?

Digital plagiarism:

Plagiarism is one of the major forms of academic dishonesty which has always existed in education, including higher education. For example, assignments submitted by students may turn out to be copied from fellow students or to be taken over, in part or in whole, from existing published works. The use of computers and Internet added to the means that students have at their disposal to commit plagiarism. However, they make it much easier to do and much harder to detect.

Breaking copyright and software theft:

Throughout the society, it is well known that the illegal copying of copyrighted media (texts, music works, movies and software programs) is widespread. Moreover, many people who engage in such activity do not consider themselves to be doing something that is immoral. This is certainly true for college students. And this attitude of students seems to match developments in the current information age, in which the Internet increasingly functions as the most important information medium that people use.

Improper use of computer resources:

Students and staff may have authorized access to computer resources, but then go on to use these resources improperly. They may have a school/library Internet account, or they may use computer system or computer network or computer software that is owned by the school, or they may use computerized services offered by the school, and do so in a way that does not meet the school's standards for proper use of that particular resource.

For example, students may use their student account to run their own Internet business, may open up a popular website or service that generates loads of traffic, downloads of MP3 files, staff members may use the school's server or computer systems to download or view or store content that is either illegal or against the school policies (e.g., racist or fascist materials or pornography) or members of the academic community may spread computer viruses or worms.

Securing informational privacy and confidentiality:

Personal information on public computers: While using publicly accessible computers, students or staff may unknowingly leave personal information on the public computers, such as cached web pages (accessed web pages that are left in temporary storage on the disk drive and may remain there even after a browser is closed) and cookies (small files that are put on a hard

disk by a web site to identify users and their preferences), that are then available for inspection by others.

File sharing: The computers that are used by Student or faculty may contain software that makes files on them accessible to other users on the campus network and outside without knowledge of the owner, or they may allow files to be stored on a central server that are then accessible to others without their permission. This could allow strangers to read these files that may contain personal information.

School web pages and bulletin boards: Web pages maintained by the school, by faculty or by students may contain personal information that may access the privacy of others. Likewise, postings and re-postings (forwarded messages) on bulletin boards or in other electronic forums may contain personal information of third parties for which no authorization has been given.

3.2. INTERNET ETHICS:

Internet ethics means acceptable behavior for using Internet. One should be honest, respect the rights and property of others on the Internet. One has to accept that Internet is not a value free-zone. It means World Wide Web is a place where values are considered in the broadest sense so we must take care while shaping content and services and we should recognize that Internet is not apart from universal society but it is a primary component of it.

It belongs to all and there are no boundaries of national and local cultures. It is used for multiple usages and is not subjected to a single set like local TV or a newspaper. The use of Internet is to help the knowledge grow and to do school work. Also in the virtual world the Internet is used for communication with family and friends. The IInternet is also used for listening the music, video, learning how to play instruments etc. The importance of copyrights and issues of copyright should be taken care while downloading or sharing the material on the Internet.

It is to be understood that everything exists on the Internet is not real, there might be false and fraud information even though people use the Internet. One has to verify the authenticity of the information and get reliable information. Internet is not a value-free zone and World Wide Web is not a just web where we can get the information from the world but it is a place where values are considered in a broadest sense.

3.3. CYBER BULLYING:

Cyberbullying is when the Internet and related technologies are used to bully other people, in a planned, repeated, and hostile manner. This could be done via:

- text messages or images,
- personal remarks posted online,
- hate speeches,
- making others to dislike and gang up on the target by making them the subject of ridicule in forums, and
- Posting false statements in order to humiliate or disturb another person.

Cyberbullies may also disclose victims' personal data (e.g. real name, address, or workplace/schools) on websites. Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a subject.

Under the Indian law, cyberbullying is covered by section 66A of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc." This section provides for imprisonment up to 3 years and fine. Section 66A penalizes the following being sent through email, sms etc:

(1) Information that is grossly offensive or has menacing character; or

(2) False information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.

This section also penalizes the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes:

(1) Causing annoyance, or

(2) Causing inconvenience, or

(3) To deceive or to mislead about the origin of the messages.

3.4. CYBER ETHICS:

Cyber ethics is a code of behaviour for moral, legal and social issues on the Internet or cyber technology. Cyber ethics also includes obeying laws that apply to online behaviour. By practising cyber ethics, one can have a safer and enjoyable Internet experience. Cyber bullying is the use of information technology to repeatedly harm or harass other people in a deliberate manner. With the increase in use of these technologies, cyber bullying has become increasingly common, especially among teenagers.

Cyber technology refers to a wide range of computing and communications devices from individual computers, to connected devices and communications technologies. Cyber ethics suggest the study of ethical issues limited to computing machines, or to computing professionals. It is more accurate than Internet ethics, which is limited only to ethical issues affecting computer networks.

We should not use the Internet chatting or communicating with strangers and forwarding the e-mails from strangers. And we must teach children on risks involved by chatting or forwarding e-mails to strangers.

3.5. CYBER SAFETY

Cyber safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviors protect personal information and reputation and include safe practices to minimize danger from behavioral-based, rather than hardware/software-based, problems.

3.6. CYBER SECURITY:

Whereas cyber safety focuses on acting safely and responsibly, cyber security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means.

3.7. SAFETY MEASURES FOR ETHICS:

There are four effective approaches who want to ensure they are doing the right thing online:

- Have a basic understanding of the technology
- Participate with your child online.
- Determine what standards have been established for in-school computer use.
- Create, with your child, a set of Rules relating to both ethics and safety.

As per the importance of information technology, and given the possibilities of unethical use of this technology by students and faculty, schools/colleges should ensure that they have policies regarding the use and management of information technology by students and staff.

Several ethical codes dealing with technology use exist and many schools have adopted Acceptable Use Policies that include rules for the proper use of information technologies. Teachers, students, and parents need to know and understand these codes.

For children, the major issues surrounding technology ethics can be categorized into three areas: privacy, property, and appropriate use. School related cases can be found in each of these areas.

Teachers need to develop learning objectives and activities that specifically address technology ethics. Proper use needs to be taught at the same time that other computer skills are taught. Students understanding of ethical concepts need to be assessed. Technology use privileges, especially those involving on-line use, should not be given to students until the assessments show that a student knows and can apply ethical standards and school policies.

In schools, one should have an Acceptable User Policy. An "Acceptable Use Policy" that describes the use of the Internet and other information technologies and networks in a school. The rules in these policies often apply to both staff and students. Everyone in the school, as well as parents, needs to know and understand these policies.

An Acceptable User Policy may contain:

- Not using the service as part of violating any law

- Not attempting to break the security of any computer network or user
- Not posting commercial messages to school groups without prior permission
- Not attempting to send junk e-mail or spam to anyone who doesn't want to receive it
- Not attempting to mail bomb a site with mass amounts of e-mail in order to flood their server
- Do not use computer technology to cause interference in other users' work.
- Do not use computer technology to steal information

3.8. THE TEN RULES OF COMPUTER ETHICS:

- One shall not use a computer to harm other people.
- One shall not interfere with other people's computer work.
- One shall not snoop around in other people's computer files.
- One shall not use a computer to steal.
- One shall not use a computer to bear false witness.
- One shall not copy or use proprietary software for which you have not paid.
- One shall not use other people's computer resources without authorization or proper compensation.
- One shall not appropriate other people's intellectual output.
- One shall think about the social consequences of the program you are writing or the system you are designing.
- One shall always use a computer in ways that insure consideration and respect for your fellow humans

CASE STUDIES ON COMPUTER ETHICS

CASE STUDY 1:

Chinna and Kanna are students of eighth class studying in District High School. They have a subject on computer course and daily practices in the computer lab. One day, Chinna has walked away from the computer lab without logging off. The next day many of their class told Chinna that they got some warning and abusive e-mails from Chinna's mail and also some inflammatory messages on the class forum.

DISCUSSION:

1) What might be the right and ethical way to do if someone walks away without logging off the computer?
2) What might be the steps that Chinna should have taken?
3) What might be the behavior of Kanna in case someone didn’t log off the computer?

CASE STUDY 2:

Santu is a bright and topper student studying tenth class in a school. She is the teacher’s favorite student and all the students are also fond of her and used to take help from her if they have any doubts.

As the annual exams are approaching, Santu has been receiving 4 or 5 anonymous insults daily over email. Because of the context of the notes, she has come to a conclusion that the sender is one among her in her class. She sends the entire class a warning not to do it again.

DISCUSSION:

1) What do you that has happened in case of Santu?
2) Do you think why the sender has sent that mails to Santu?
3) Is it a good way to send such mails at the time of exams?
4) What might be the method of Santu warning the students of her own class is right.

CASE STUDY 3:

Munni is a student of tenth standard studying in Convent High school. Her science teacher has given an essay topic to her as part of project submission for the annual exam. Munni submitted the project work as per the date. But after verifying her project work, her teacher to make changes in the project as she found that most of the content is copied from Internet.

DISCUSSION:

1) Is the way of copying others work without giving credits to the original author is ethical behaviour?
2) What might be the correct way to copy content or information from Internet?

CASE STUDY 4:

Chinna was the student from a class tenth and regularly goes to a library computer for studying the eBooks' from the Internet for their work and other project related activities. He also downloaded project related software and installed in his school library computer without taking permission from the concerned lab coordinator. The next day the school principal got a mail saying to buy the license for the particular software downloaded from the Internet.

DISCUSSION:

1) Do the school children are aware about the program or software which they are going to install and use?
2) What Library technician should do for blocking such software's from the Internet?
3) Does the Chinna read about the terms and condition during downloading a program?

CASE STUDY 5:

You are a computer Lab coordinator working for a small business that provides specialized financial services to local, mostly small businesses. You have been working for company X for about six months. Recently X has been occupied with re-engineering the inventory system of a local hardware chain, ABC Hardware. Your supervisor calls you into his office. "Do you know of any existing software products to help ABC keep better track of its inventory?"

You mention a particular product that you have worked with in another job and point out that ABC could use it without any modification. The only drawback, you point out, is that this software is somewhat expensive. Your supervisor leans back in his chair and says, "That's no problem. We have that software. Why don't you just install it on ABC's computers?" And ABC is a very important client. We need to do all we can to keep them happy."

DISCUSSION:

1) Go ahead and install the software on ABC's computers. After all, your supervisor is right: nobody will know what you have done?
2) Refuse to do it. Make it clear to your supervisor that he is putting you in a very difficult position, and you are not happy about it. It is illegal, and you don't have to do it
3) Establish the case that your supervisor is responsible for the act, and then send several people within the company copies of this memo, including your supervisor.
4) Go ahead and install the software. But be sure to cover yourself first by writing a memo that clearly states that this is illegal, and you are doing it because your supervisor has left you no choice.
5) Establish the case that your supervisor is responsible for the act, and then send several people within the company copies of this memo, including your supervisor.
6) Discuss the matter confidentially and informally with another colleague, preferably another supervisor, possibly someone over your supervisor's head.
7) If this person's reaction is good, then both of you can approach your supervisor and try to talk him out of this course of action.

CASE STUDY 6:

Ishaan spends most of the time in browsing his home computer and during holidays it increases because of the school and project related work. Ishaan's mother describes him as extremely good technically, very bright and very good at computer programming. His general certificate of secondary education homework has been good because most of the time he spends on his computer for school works.

Ishaan used to sit more on computers till mid night and writing the programming codes which made make difficulty in making new friends. His parents feel he views his computer as a "friend" and, therefore, tends to spend much of his time on the machine. He refused to do his normal household activities when requested, was generally embarrassed and difficult, and irritated and rude situations between him and other members of the family.

He spends time with the computer to the exclusion of family and friends. His parents had his general practitioner refer him to a psychiatrist for counseling and help. He is still getting the help of the local psychological services. His mother feels that much of his lack of confidence stems from the fact that he is content to spend his time in his room to the exclusion of others in his own world. Ishaan's own view is that he does not have a problem with his computer use and that he does not spend too much time on the computer.

DISCUSSION:

1) Did Ishaan consult about his addiction to Internet behavior to the parents?

2) Did Ishaan appear to use a computer as an "Electronic Friend?

3) Did Ishaan have any "Social isolation problem?

4) Did the PC used by Ishaan is kept in open Hall?

5) During the school holidays it increases even more, especially because he is in his room even as his parents at work.

6) His mother claims “he is computer mad, but not for computer games, rather for serious computing-programming etc.”

7) His general certificate of secondary education homework has been increasingly suffering because of the time he spends on his computer

CASE STUDY 7:

Vivaan has played on computer games since he was a small child. As an only child he got almost anything he wanted when he was younger, including all forms of electronic technology. He recalls that as a child he had a small computer on which he used to play games but used the computer for nothing else. He now believes that people can become better in using Internet via playing of fantasy role-playing games (such as Candy Crash and Farm Ville) and through the use of chat rooms and other online activities such as Wikipedia and school related projects.

Vivaan feels his whole life revolves around computers and he claims that using the Internet excessively helps him cope with everyday life as a university student. He spends an average 40– 50 hours a week on the Internet but has no financial problems because he accesses the Internet for free room his university.

DISCUSSION:

1) Did Vivaan is addicted to Internet?

2) Did Vivaan is having the Social life outside other than Internet world?

3) Did Vivaan uses Internet for motivation or socializing related activities?

4) Did Vivaan is addicted to computer games?

5) Did Vivaan studies have suffered considerably as he spends so much time on the Internet, which leaves him little time to get on with his degree work?

Chapter 4:

Cyber Crimes

4. CYBER CRIME

4.0. CYBER CRIMES:

Any attack on the information systems, that is against the law of the land, can be considered as cyber-crime. The attack can be on the confidentiality of information, on the integrity of information, or it can be a denial-of-service attack or a repudiation attack. The attack can be on an individual, an enterprise or on a government.

Here are some examples of cyber-crime: Intentionally sending a virus is a crime. Stealing the credit card information during an e-commerce transaction, impersonating a student in an e-learning portal, an employee sending the confidential information of an organization to an outsider through email etc., are cyber-crimes. However, the definition of what a crime is differs from country to country. In some countries, it is not a crime to visit adult sites, but in some countries, it is a crime, the punishment can be imprisonment. In some countries, it is OK to visit the adult sites, but the downloaded content cannot be sent to another person. Of course only if that person complains to the police, it will be a crime!

In many countries, there are no cyber-laws. Some countries do have cyber-laws, but the interpretations vary and it is difficult for the general public to know what is right and what is wrong. Many cyber-crimes go undetected as it is difficult to track and trace the criminal. Even if the criminal is caught, the punishment was not very strict. The person who released a computer worm that infected millions of computers was sentenced by a judge to pay 1000 dollars fine and to do community service for a few months.

Consider this case: a person created a mail account with a free mail service provider and then he sent a threatening mail to a lady. Again, the lady received another threatening mail, but now from a different mail address, but with the same email service provider. Perhaps this criminal was creating mail accounts and was using it only once. The email service provider is based in the US and the lady is in India. Think of it, how do you catch the criminal?

4.1. IT ACT 2000:

India has seen a sharp increase over the last few years in the commission of cybercrime and the loss has proven to be significant. In order to deal with such crimes, Information Technology Act 2000 was enacted to provide a legal framework to address issues of:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions in the cyber space

4.2. CYBER CRIMES AND SECTIONS:

Cyber Attacks/Crimes & Amendments	Sections Relevant in IT Act 2000
Cyber Stalking	43,66
Intellectual Property Crime	43,65,66
Salami Attack	43,66
Phishing	43,66,66C
Personal Data Theft	43,43A
Identity Theft	43
Spoofing	43,66
Data Theft	43,43A, 65,66
Worms, Trojan Horses, Virus,etc	43,66
Sabotage of computer	43,66
DoS, DDoS	43,66,66f
Money laundering on Web	43,66,66C,66D
Publishing or transmitting obscene material	67
Pornography	67A
Child Pornography	67B
Violation of Privacy	66E
Dishonestly receiving stolen computer/communication device	66B
Cyber Terrorism	66F

Hacking of Protected Systems	70
Offensive Messages	66A

4.3. CYBER CRIME SECTIONS AND DESCRIPTIONS:

SECTION NUMBER AND NAME	DESCRIPTION	COMPENSATION
Section 43: Penalty and Compensation for damage to computer, computer system, etc	If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network	The person shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Section 43A: Compensation for failure to protect data	Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages.	The person shall be liable to pay damages by way of compensation, to the person so affected.
Section 65: Tampering with Computer Source Documents	Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force shall be	The person shall be liable for imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

	punished.	
Section 66: Computer Related Offences	If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable.	The person shall be punished for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Section 66 A: Sending offensive messages through communication service, etc.	Any person who sends, by means of a computer resource or a communication device	The person shall be liable for imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
Section 66 B: Dishonestly receiving stolen computer resource or communication device	Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device shall be punished.	The person shall be punished for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Section 66 C:Identity Theft	Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person is liable for punishment.	The person shall be liable for imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
Section 66 D: Cheating by personation by using computer	Whoever, by means of any communication device or computer resource cheats by personation shall be liable for punishment?	The person shall be liable for a term which may extend to three years and fine which may extend to one lakh rupees
Section 66 E: Violation of Privacy	Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person	The person shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh

	without his or her consent, under circumstances violating the privacy of that person shall be punished.	rupees, or with both.
Section 66 F: Punishment for cyber terrorism	• With intent to threaten the unity, integrity, security or sovereignty of India or • To strike terror in the people or any section of the people and by means of such conduct causes • Is likely to cause death or injuries to persons or • Damage to or destruction of property or • Disrupts or knowing that it is likely to cause damage or • Disruption of supplies or services essential to the life of the community or • Adversely affect the critical information infrastructure specified under section70;	The person shall be punishable with imprisonment which may extend to imprisonment for life.
Section 67: Publishing or transmitting obscene material in electronic form	Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished.	The person shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
Section 67 A Publishing or transmitting of material containing sexually explicit act,	Whoever publishes or transmits or causes to be published or transmitted in the	The person shall be punished on first conviction with imprisonment of either

etc. in electronic form	electronic form any material which contains sexually explicit act or conduct shall be punished	description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Section 67 B: Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Whoever: • Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or • Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or	The person shall be punished on first conviction with imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment for a term which may extend to seven years and also with fine which may extend to ten lakh rupees
Section 68: Power of Controller to give directions	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.	Any person who intentionally or knowingly fails to comply with any order under this section shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both
Section 69 A: Power to issue directions for blocking for	Where the Central Government or any of its officer specially	The intermediary who fails to comply with the direction

public access of any information through any computer resource	authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.	issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.
Section 70: Protected System	• Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished. • The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. • Explanation: For the purposes of this section, "Critical Information Infrastructure" means the	Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under this section shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

	computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.	
Section 71: Penalty for misrepresentation	Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished.	The person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 73: Penalty for publishing electronic Signature Certificate false in certain particulars	No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that: ➢ The Certifying Authority listed in the certificate has not issued it; or ➢ The subscriber listed in the certificate has not accepted it; or ➢ The certificate has been revoked or suspended ➢ Unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation shall be punished.	The person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.
Section 74: Publication for fraudulent practices	Whoever knowingly creates publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished.	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Chapter 5:

Browser Security

5. BROWSER SECURITY

5.0. WHAT IS WEB BROWSER?

Web browser is used to gain an access the information and also resources on the World Wide Web. It is a software application used to trace and display the web pages .The main purpose of a web browser is to bring the information resources to the user. An information resource is identified by a Uniform Resource Identifier (URI/URL) and may be a web page, image, video or other piece of content. Web browser are used not only on the personal computers, laptops but are also used on mobile phones to access the information.

Uniform Resource Locator (URL)

The URL represents http://www.infosecawareness.in

Each URL is divided into different sections as shown below

http:// In short, http means the hypertext transfer protocol and the file is a web page and every time you don't needed to type the http, it is automatically inserted by the browser.

www – notation used for World Wide Web

infosecawareness – web site name

.in –It is one of the domains names, which is basically a country name.

Other domain names are .com (commercial organization), .net (network domain) etc.

(The organization address and location of the organization address are known as the domain name).

co.in –suffix or global domain name shows the type of organization address and the origin of the country like the suffix co.in indicates a company in India.

Generally a web browser connects to the web server and retrieves the information. Each web server contains the IP address, and once you are connected to the web server by using http, it reads the hyper text mark-up language (HTML) which is a language used to create document on World Wide Web and the same document is displayed in the web browser.

In short, a browser is an application that provides a way to look at and interact with all the information on the World Wide Web.

5.1. TYPES OF WEB BROWSERS

There are different types of web browsers available with different features.

SOME OF THE POPULAR WEB BROWSERS ARE:

Internet Explorer:
It is known as Microsoft Internet Explorer in short IE. It comes pre-installed on all Windows computers. It is one of the most popular web browsers and latest edition of IE 11 is available on the Internet. It can be installed with the following: windows operating system like Windows 7, Windows 8, Windows Vista and Windows Server's.

Mozilla Firefox:
It is a free, open source web browser developed by Mozilla Corporation. It has been said as being stable and safer, less prone to security breaches, viruses, and malware than Microsoft Internet Explorer. The browser can be used in different operating systems like Windows, Linux and Apple MAC operating system etc.

Google Chrome:
It is a web browser designed for windows operating system. This browser works on windows vista, windows 7 and windows 8 and. The chrome can be downloaded and installed for OS X or Linux operating system

Safari:
It is web browser developed by Apple Corporation. It is a default web browser of MAC OS X. This browser also works on all windows flavours. Apple maintains a plug-in blacklist that it can remotely update to prevent potentially dangerous or vulnerable plug-ins from running.

WHY TO SECURE YOUR BROWSER

Today, web browsers such as Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari are installed on almost all computers. And it is easy to notice the increasing threat coming from online criminals that try to take advantage of web browsers and their vulnerabilities. Because web browsers are used so frequently, it is very important to configure them securely. Often, the web browser that comes with an operating system in a default settings which is not set up in a secure configuration.

Securing browser is the first step that needs to be taken in order to assure online protection and there is an increase in number of threats taking advantage of vulnerabilities present in the web browsers and through use of malicious websites. This problem is made worse by a number of factors, including the following:

- Many computer users are not aware of the click on the web links.
- Software and third party software packages installed combined increases the number of vulnerabilities
- Many websites require that users enable features or install more software, third-party software which doesn't get security updates putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.

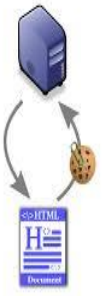
5.2. WEB BROWSER RISKS AND CASE STUDIES

Browsers are used to access various web pages to have a complete online experience. The browsers are enabled by default with some of the features to improve our online sessions, but at the same time these options create a big security risk for our operating systems and databases. The online criminals use available vulnerabilities in our browser and in its additional features to control operating systems, retrieve private data, damage important system files or install data stealing software.

Some of the features are important for browser's functionality and the user should understand their importance and should enable or disable for securing the browser.

Browser Cookies:

A cookie is used to identify a website user. A cookie is a small piece of text sent to a browser by a website that is visited from it. It contains information about that visit like remembering the website visited preferred language and other settings. The browser stores this data and uses it in accessing the features of the website or the next time the same site is visited to make the access more personalized. If a website uses cookies for authentication, then an attacker may be able to obtain unauthorized access to that site by obtaining the cookie.



Case 1:

Shania visited a movie website and indicated that she is interested in comedies. The cookies sent by the website remembered her choice and when she visited the same website next time, she sees comedies are displayed on the website.

Case 2:

When users log in to a Web site, they enter their username and password into a login page and, if they are authenticated, a cookie is saved that allows the Web site to know the users are already logged in as they navigate around the site. This permits them access to any functionality that may be available only to logged-in users, probably the primary use of cookies at this time.

Case 3:

Online shopping carts also use cookies. As you browse for DVDs on that movie shopping site, for instance, you may notice that you can add them to your shopping cart without logging in. Your shopping cart doesn't "forget" the DVDs, even as you hop around from page to page on the shopping site, because they're preserved through browser cookies. Cookies can be used in online advertising as well, to remember your interests and show you related ads as you surf the web.

Pop-ups:

Pop ups are a small windowpane that opens automatically on your browser. Generally, they show advertising, which can be from legitimate company, but also may be scams or dangerous software. It works when certain websites are opened. Pop-up ads can be part of a phishing scam designed to trap you into revealing your personal or financial information as you visit web sites. Sometimes pop-ups mislead you like when ever pop-ups come you click on close or cancel on the window. But sometimes advertisers create a pop-up window that look similar to a close or cancel option so whenever user choose such options the button performs an unexpected action like opening another pop-up window, performing unauthorized commands on your system.

Not all pop-ups are bad some web sites use pop-up windows for particular tasks. You might have to view the window in order to complete that task.

Case 4:

Sarah was listening music online from XYZ@music.com, after some couple of hours later I came across a Pop-up which tells to download the latest songs with only one click. I filled the form displayed in my browser download section. After a month I saw my credit card bill information which is showing some unauthorized charges. I was very upset and surprise and called repeatedly to that particular website where I have downloaded the songs but it was no use.

Scripts:

Scripts are used to create websites more interactive. It is most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. There are specifications in the JavaScript standard that limit certain features such as accessing local files.

The same script can be used for inclusion of malicious code which takes control of the web browser there in by allowing to access the files of the system. It may cause damage to the system by accessing the vulnerabilities in the browser.

Case 5:

Chintu used to visit at Internet for regular updates for his school work and playing games and listening music. When playing the games I found some news popping about Lady Gaga found dead. When I click on the BBC site a survey dialog is pop out and prompt user to complete a survey form. In the respective survey form it was written "If you are true fan on Lady Gaga" Click for Like Button. As soon as survey completed I returned back to my account homepage and posted the same link for the news to be known for my family and friends.

Plug-ins:

Plug ins is the in-built applications for use in the web browser and Netscape web browser has developed the NPAPI standard for developing plug-ins. But later this standard is used by many web browsers. Plug-ins are same to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in inside the web browser.

Case:

For example, users may download and install a plug-in like Adobe Flash Player to view a web page which contains a video or an interactive game. But the plugin may be installed with a key logger which captures all the key strokes of the user typing in the browser and send it to the attacker.

Browser Extensions let you add new features to your browser exactly like extending your browser for customising your browser with the features that are mainly important to you. In the other words you can say adding new superpowers to the browser. For example, you may install a currency converter extension that shows up as a new key next to your browser's address bar. Click the button and it converts all the prices on your present web page into any currency that you give.

Adding more code to the browser also added to security concerns, as it gave attackers more chances to exploit the browser. Because the code was sometimes hidden, extensions were notorious for causing browser crashes as well.

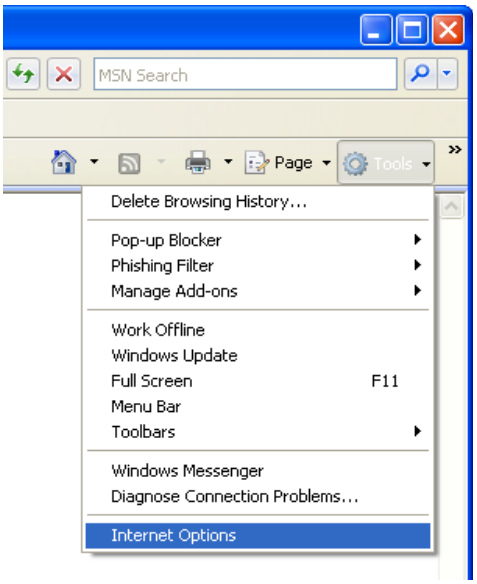
5.3. HOW TO SECURE YOUR WEB BROWSER

By default web browser comes with an operating system and it is setup with default configuration which doesn't have all secure features enabled in it. Not securing web browser leads to problems caused by anything like spyware, malware, viruses, worms etc being installed in to a computer and this may cause intruders to take control over your computer.

There is a raise of threat from software attacks this may take advantage of vulnerable web browsers. Some software's of a web browser like java script, Active X etc may also cause the

vulnerabilities to the computer system. So it is important to enable security features in the web browser you use this may minimize the risk to the computer.

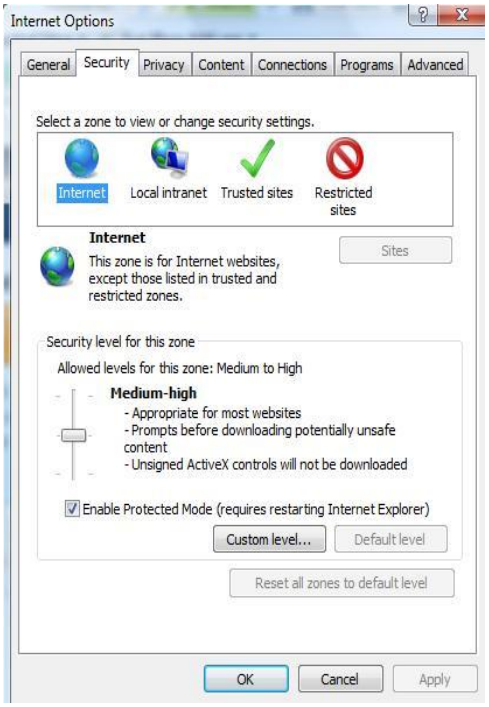
Security zone



Security zone in an Internet web browser lets you to secure the browser and offer to trust the people, companies on the Internet. This helps to decide and adds which sites to be allowed to run the application, scripts, add-ons, install plug-in on your computer .Security zone also contains other features like adding address of web sites under restricted sites this feature is available in Internet explorer and block the untrusted sites or attack sites this feature is available in Firefox, this varies with different web browser.

Trusted site

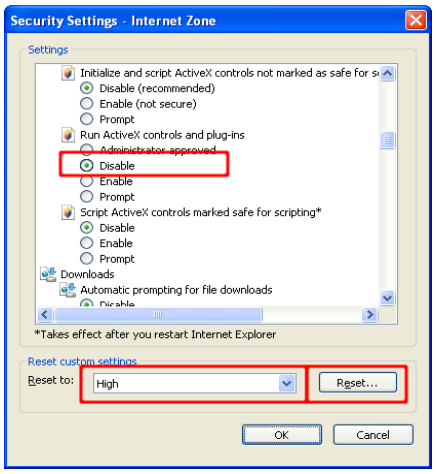
As Internet is a network of people, with all kinds of stuff with different kind of people. Generally you don't trust everyone around you so why to trust all the web sites? Also why do you allow everyone to come into your computer without your authorization? So use the feature of trusted sites in your web browser to decide whom to trust



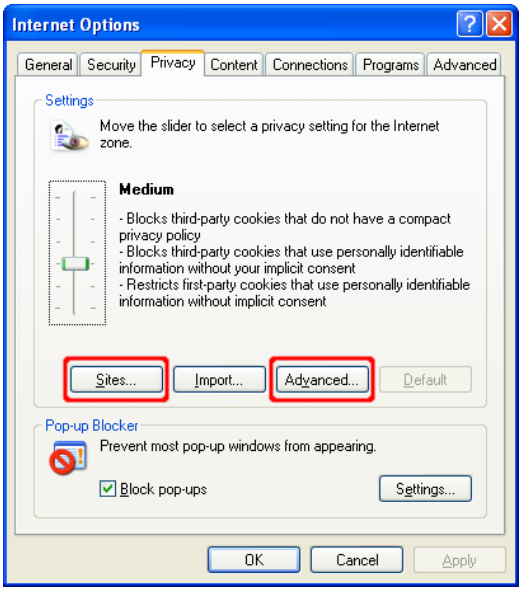
Internet explorer

The following are the some of the features and their settings of Internet explorer

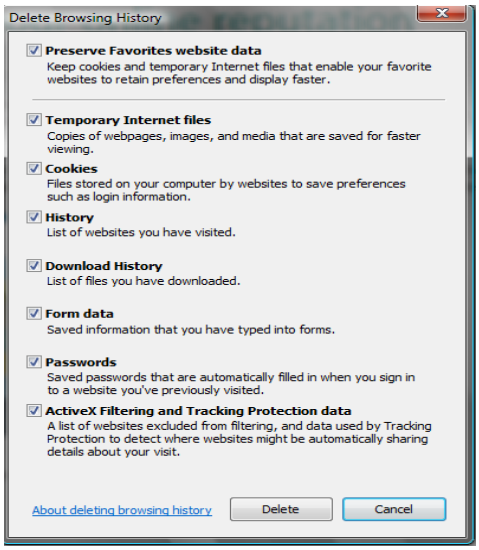
- In order to change settings for Internet Explorer, select Tools then Internet Options
- From the tools menu of Internet explorer select the Internet options and then click on the security tab and check the current security settings and change the settings of security zone as per the necessary
- To change the security setting under security level move the slider up to increase the security level to, medium, medium and high level
- For more settings and controls click on the custom level and then select the options you want
- From the tools menu option if required there is an option for: Delete browsing history which deletes all the cookies, temp files, history, active x filtering and more as shown in the figure



- To add or remove trusted or restricted web sites ,click on the sites option and then click on the add or remove button and enter your list of sites for the selected zone



- The Privacy button contains settings for cookies. Cookies are text files placed on your computer browser by various sites that you visit either directly or indirectly through third party web sites.
- From the Advanced button and select override automatic cookie handling. Then select Prompt for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your machine.
- From the menu select tools and choose the smart screen filter and click on the turn on smart screen filter and enable the smart screen filter which is recommended, this option is used to “Avoid phishing scams and malware”



- From the tools menu select the option in private filtering settings, this option is used for “Browse privately” which doesn’t store any browsing history

- In the tools menu there is an option called tracking protection which protect your information like if some websites try to track your visits to those websites or any of your personal information such information would be stopped. This feature works based on the add-ons we install.

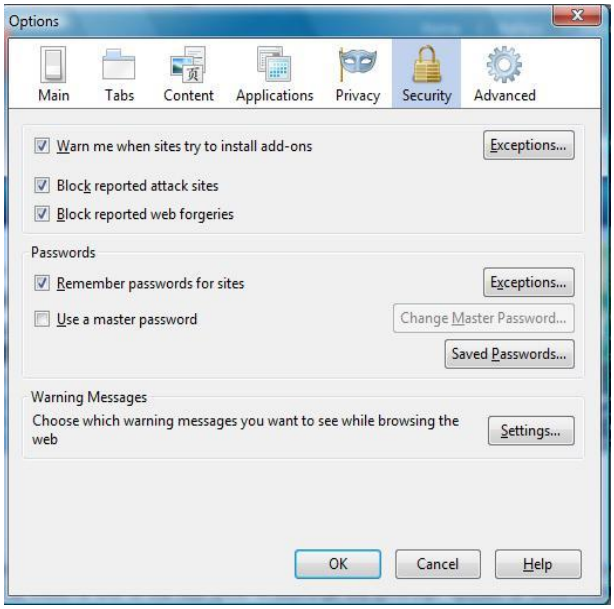
- Enable the protected mode by this option all the web sites are opened in protected mode.

- Select the advanced tab and select the options as you want like enable " Use SSL 3.0, Use TLS 1.0 "

Mozilla Firefox

The following are the features and their setting of Mozilla Firefox web browser.

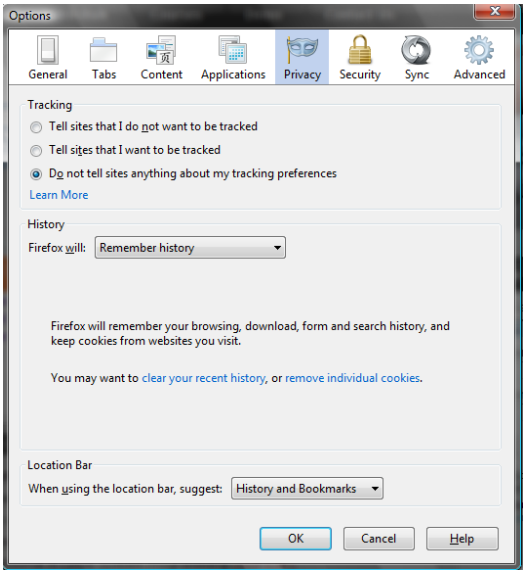
Security settings in a Firefox control the level of examination you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for passwords, cookies, loading images and installing add-ons for a fully empowered Web experience as shown below



- From the tools menu of the Firefox browser select the options and then click on the security tab

- Under security tab enable the options like warn me when sites try to install the add-ons in and to add or remove the sites click on the exception tab and add or remove the sites you want
- Enable the option tell me if the site I'm visiting is a suspected attack site
- Enable the option tell me if the site I am using is a suspected forgery Firefox gets a fresh update of web forgery sites 48 times in a day, so if you try to visit a fraudulent site that's pretending to be a site you trust a browser prompts you message and will stop you

- Disable the option remember passwords for sites Firefox integrated the feature into your surfing experience. Choose to "remember" site passwords without intrusive pop-ups.
- Select the advanced tab and enable the encryption tab in order to have a secure data transfer and use SSL 3.0
- The other feature is automated updates this lets us to find the security issues and fix updates and make the safe surfing and receive automatic notification or wait until you are ready
- One more feature is tracking which is under options privacy it stops the activities you do from the browser and we can choose the option do not tell sites anything about my tracking preferences



which will not track and don't share the information to other websites.

Google chrome

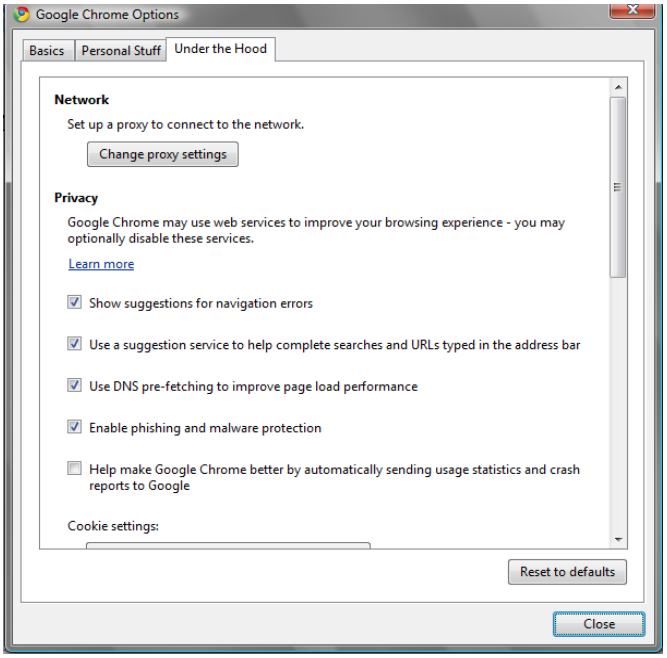
From the setting menu select the **Incognito window** a new window appears and pages you view from this window won't appear in your web browser history or search history and they won't leave any traces like cookies after you close the incognito window any files you download or bookmarks will be preserved.

Chrome there is a new feature that it has an own **Task Manager** that shows you how much memory and CPU usage each tab and plug-in is using.

The **safe browsing** feature in the Google Chrome displays the warning if the web address listed in the certificate doesn't match the address of the website .The following are the steps for a safe browsing setting in Google Chrome.

From the settings tab select the options and click on the under the hood

- Enable the option use a suggestion service to help complete searches and URLS typed in the address bar
- Enable DNS pre-fetching to improve page load performance
- Enable the phishing and malware protection
- Under cookies select the "Restrict how third party cookies can be used" only first-party cookie information is sent to the website.
- Under minor tweaks enable the enable the never save passwords
- Under computer wide SSL settings enable the option use SSL 2.0



Apple safari:

The following are the features of Apple safari secure web browser

Phishing Protection

Safari protects you from fraudulent Internet sites. When you visit a suspicious site, Safari warns you about its suspect nature and prevents the page from loading.

Malware Protection
Safari recognizes websites that harbour malware before you visit them. If Safari identifies a dangerous page, it warns you about the suspect nature of the site.

Antivirus Integration
Thanks to support for Windows Attachment Monitor, Safari notifies your antivirus software whenever you download a file, image, application, or other item. This allows the antivirus software to scan each download for viruses and malware.

Secure Encryption
To prevent eavesdropping, forgery, and digital tampering, Safari uses encryption technology to secure your web communications. Safari supports the very latest security standards, including SSL versions 2 and 3, Transport Layer Security (TLS), 40- and 128-bit SSL encryption, and signed Java applications.

Automatic Updates
Get quick, easy access to the latest security updates. Safari takes advantage of Apple Software Update, which checks for the latest versions of Safari when you're on the Internet.

Pop-Up Blocking
By default, Safari intelligently blocks all unprompted pop-up and pop-under windows, so you can avoid distracting advertisements while you browse.

Cookie Blocking
Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from your current domain.

TIPS

Always use the secured web browser to avoid the risks .Using secure browser we can gain access the information and resources that are available on the Internet and can have safe browsing over Internet.

To avoid your PC being compromised and becoming a weapon to attack other machines, web browser and the Internet users are advised to: ensure that your operating system and key system components such as the web browser is fully patched and up to date.

Install a personal firewall along with anti-virus software with the latest virus signatures that can detect malware such as key loggers.

Regularly change your passwords with the combinations of letters, numbers and special case characters in critical web applications if a one-time password system is not supported.

Turn off all JavaScript or ActiveX support in your web browser before you visit any unknown websites.

Most vendors give you the option to download their browsers directly from their websites. Make sure to verify the authenticity of the site before downloading any files.

To additional minimize risk; follow the latest good security practices, like using a personal firewall, Updating to the latest browser with security patches installed and keeping anti-virus software up to date with regular scanning the entire system.

REFERENCES

https://www.us-cert.gov/publications/securing-your-web-browser

http://www.kb.cert.org/vuls/id/680526

http://www.20thingsilearned.com/en-GB/conclusion/2

http://www.infosec.gov.hk/english/technical/files/attacks.pdf

Chapter 6:

Email Security

6. EMAIL SECURITY

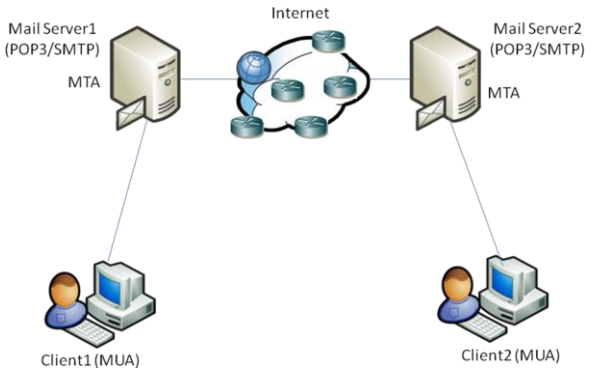
6.0. INTRODUCTION:

E-mail is a short form of electronic mail which is widely used services on the Internet. E-mail is used for transmission of messages in a text format over the Internet by using the receiver E-mail address and vice versa. E-mail can be sent to any number of users at a time it takes only few minutes to reach the destination. E-mail consists of two components; the message header contains control information, and another receiver addresses with message body, which is the e-mail content.

Some E-mail systems are confined to a single computer system or to a small network, and they are connected to the other E-mail systems through the gateway, which enables the users to connect to anywhere in the world. MAPI is a Mail Application Programming Interface, system built in Windows, which allow different mail applications working together for distributing mails. Until MAPI is enabled on both the application's the users can share mails with each other.

6.1. HOW AN E-MAIL WORKS?

Each mail server consists of two different servers running on a single machine. One is POP3 (Post Office Protocol) or IMAP (Internet Mail Access Protocol) server which holds the incoming mails and the other SMTP (Simple Message Transfer Protocol) server which holds the outgoing mails. SMTP works on the port number 25 and POP works on the port number 110 and IMAP works on the port number 143.



The working of e-Mail is as shown in the figure below. Each mail server consists of two different servers running on a single machine. One is POP3 (Post Office Protocol) or IMAP (Internet Mail Access Protocol) server which holds the incoming mails and the other SMTP (Simple Message Transfer Protocol) server which holds the outgoing mails. SMTP works on the port number 25 and POP works on the port number 110 and IMAP works on the port number 143.

- In the figure shown above, Client 1 has an account in the mail server 1 and Client 2 has an account in mail server 2.
- When Client 1 sends a mail to Client 2, first the mail goes to the SMTP server of mail server 1. Here the SMTP server divides the receiver address into two parts username and domain name.
- For example, if SMTP server receives user1@example.com as the receiver's address. It will separate into user1, which is a mail account in destination mail server and example.com which is the domain name of destination mail server.

- Now with the help of the domain name it will request particular IP address of the recipient's mail server, and then it will send the message to mail server 2 by connecting to its SMTP server.
- Than SMTP server of Mail Server 2 stores the message in Client2 mailbox with the help of POP3 in mail server 2. When the client 2 opens his mailbox, he can view the mail sent by client 1.

AN EMAIL CLIENT

If you make use of e-mails for online communication then you would certainly be using an e-mail client which provides the following capabilities:

- Provides a list of messages that people have sent to you which consists of the name of sender, a subject, a message body and the time/date on which it was received.
- Provides the capacity to read a total message, reply to it or forward it to other people.
- Provides the ability to compose a new message and send it to the chosen receiver and also gives an option to delete a message (or) messages etc.

The e-mail clients could be Microsoft Outlook, Mozilla Thunderbird etc or could be web based (like Gmail, yahoo, BING etc). There could be a lot of advanced features that e-mail clients may provide but whatever the type of e-mail client is, the core abilities described above are provided by all type of clients.

AN EMAIL SERVER

Whenever you like you send a message from your e-mail client, it goes to an e-mail server first. The e-mail server then manages the messages received by it and forwards the message to a POP or IMAP service else it follows the standard method to send the message over Internet to the destined person.

An e-mail server comes into the scenario twice if e-mail is sent over Internet to a remote destination. First it's the sender's e-mail server that sends the e-mail over the Internet and second is the receiver's e-mail server that receives the e-mail and it makes sure that it is delivered to the receiver end or the system. SMTP servers are generally used as e-mail servers all over the Internet which is also known as Mail Transfer Agent (MTA).

POP3 SERVER

- POP3 server contains a collection of text files one for each mail account. When a message has arrived to a particular user it will append that message at the bottom of that particular user account text file.
- When a user connects to the mail server for checking his mails, he connects to POP3 server of that mail server through port 110. Here it requires username and password to view his mailbox on the mail server.

IMAP SERVER

As previously explained, these servers come into the picture when a message is received by SMTP server and it wants to be forwarded to the real recipient.

IMAP stands for Internet message access protocol which is used to access e-mails but it is distant more capable than POP. One of the most important features an IMAP server provides is the central access to e-mails. Unlike POP server, an IMAP server keeps the e-mails on the server itself and so you can access e-mails from any machine or device.
This server moreover provides easy administration of e-mails like searching, categorizing the e-mails and placing them into various sub-folders etc. The only problem that one can imagine with IMAP server is that you all the time needs an Internet connection so that the e-mail client is able to obtain e-mails from the IMAP server. But today, almost all of the e-mail clients have the capability to cache the e-mails so that you can even view them when you are offline.
To interact with IMAP server, the e-mail client connects to server machine on port 143. As with POP, IMAP server also understands a set of commands which the e-mail client uses to connect with the server.

6.2. POSSIBLE THREATS THROUGH E-MAIL

E-Mails are just like a postcard from which the information can be viewed by anyone. When a mail is transferred from one mail server to another mail server there are various stops at which there is a possibility of unauthorized users trying to view the information or modify it.

Since a backup is maintained for an e-Mail server all the messages will be stored in the form of clear text though it has been deleted from your mailbox. Hence there is a chance of viewing the information by the people who are maintaining backups. Hence it is not advisable to send the personal information through e-Mails.

Say you have won a lottery of million dollars, getting or receiving such kind of mails is a great thing, and really it's the happiest thing. However these mails may not be true. By responding to such kind of mails many people lost huge amount of money. So ignore such kind of e-Mails without your participation in it and consider it as a scam. Sometimes e-Mails are received from unknown address by offering free gifts and asking for personal information it is one way to trap your personal information.

- One way of stealing the password is standing behind an individual and looking over their password while they are typing it or searching for the papers where they have written the password.
- Another way of stealing the password is through guesses. Hackers try all possible combinations with the help of personal information of an individual.
- When there are large numbers of combinations of passwords the hackers use fast processors and some software tools to crack the password. This method of cracking password is known as "Brute force attack".
- Hackers also try all the possible words in a dictionary to crack the password with the help of some software tools. This is called a "dictionary attack".
- Generally spammers or hackers try to steal e-Mail address and send malicious software or code through attachments, fake e-Mails, and spam and also try to collect your personal information.

- Generally attackers continuously monitors on the computers or networks through which your information is travelling to capture the sensitive information like username, passwords and proprietary information that travels over the network in clear text and read it.
- If someone can obtain the username and password that you use to access your email servers, they can read your email and send false email messages as you
- Anyone who has system administrator permission on any of the SMTP Servers that your message visits cannot only read your message, but they can delete or change the message before it continues on to its destination.
- When email is sent, the receiver may be able to know the IP address of the sender's computer. This information may be used to tell in what city you are located, their name and address to find out in some cases.

ATTACHMENTS

Sometimes attachments come with e-mail and may contain executable code like macros, ".exe" files and ZIPPED files. Sometimes attachments come with double extension like "attachment.exe.doc". By opening or executing such attachments malicious code may download into your system and can infect your system.

FAKE E-MAILS

Sometimes e-Mails are received with the fake e-mail address like services@facebook.com by an attachment named, "Facebook_Password_4cf91.zip and includes the file Facebook_Password_4cf91exe" that, the e-mail claims, contains the user's new Facebook password. When a user downloads the file, it could cause a mess on their computer and which can be infected with malicious software.

E-MAILS

Spam messages may trouble you by filling you're in-box or your e-mail database. Spam involves identical messages sent to various recipients by e-Mail. Sometimes spam e-mails come with advertisements and may contain a virus. By opening such a type e-Mails, your system can be infected with virus and your e-Mail ID is listed in spammers list.

E-MAILS OFFERING FREE GIFTS

Sometimes e-Mails are targeted to you, unknown users by offering gifts, lottery, prizes, which might be free of cost, and this may ask your personal information for accepting the free gift or may ask money to claim lottery and prizes it is one way to trap your personal information.

HOAXES

Hoax is an attempt to make the person believe something which is false as true. It is also defined as an attempt to deliberately spread fear, doubt among the users.

6.3. HOW TO PREVENT AND GUIDELINES FOR HANDLING E-MAILS SAFELY

USING FILTERING SOFTWARE'S

Use e-Mail filtering software to avoid Spam so that only messages from authorized users are received. Most email providers offer filtering services.

IGNORE E-MAILS FROM *STRANGERS*

Avoid opening attachments coming from strangers, since they may contain a virus along with the received message. Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.

GUIDELINES FOR USING E-MAIL SAFELY

- Since the e-Mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt email messages before sending, so that it can be decrypted only by the specified recipient only.
- Use Email filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated anti-virus software before saving it.
- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- Avoid sending personal information through e-Mails.
- Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-Mail.
- Do not click on the e-Mails that you receive from untrusted users as clicking itself may execute some malicious code and spread into your system.

6.4. WHY YOU SHOULD ENCRYPT YOUR MAIL

The majority of the emails you send might not be mostly private, but you know there are some times when you want to make sure only you and your receiver sees the information. Think of credit card details, passport numbers, addresses as to where you're hiding the house keys before going on holiday. Even though emails can take seconds to be sent and received, they in fact go through all sorts of networks and servers before reaching their target.

And at those way ways they leave a copy. Which means there are plenty of places from where anybody can access and read what you've written? Encrypting or authenticating your mail can

make sure only you and your receiver can see the contents of the message. It's also a great way of reducing the flow of spam using your own email address.

6.5. HOW EMAIL ENCRYPTION WORKS

Email encryption works with public-key cryptography also known as digitally signed certificates, the three most familiar standards being PGP, S/MIME and GnuPG. What you're doing is digitally signing your mail, for which only the message's recipient has the key. This means anyone as well trying to get a preview at your mail just sees twisted garbage of letters.

So how does it work? You first create a public key, which you issue to your contacts. When somebody wants to send you a private email they'll encrypt it using your public key. To read it you'll have to unencrypted it using your private key, which you are the only one to know. The public key can be made public because it is only used to encrypt, the private key being the one that authenticates messages.

In modern browsers, web site identification information may appear when users however over the address bar. They can also click the closed padlock icon. An SSL certificate serves as a credential in the online world. Each SSL certificate exclusively identifies an exact domain and a web server. Trust of a credential depends on confidence in the organization that issued it. Certificate authorities have a variety of methods to validate information provided by individuals or organizations.

6.6. WHERE TO GET AN EMAIL CERTIFICATE

Email certificates, also known as SMIME certificates, are digital certificates that can be used to sign and encrypt email messages. When you sign an email using an email certificate, only the person that you sent it to can decrypt and read the email. The receiver can also be confident that the email hasn't been changed in any way. The method of getting an email certificate is very simple. You simply apply for one from an SSL Certificate Authority and then verify that you own your email address. You'll normally respond to an email that the certificate provider sends to your address. They will then send you the certificate file that you can install to your email client.

An SSL certificate is a bit of code on your web server that provides security for online communications. When a web browser contacts your secured web site, the SSL certificate enables an encrypted connection. It's kind of similar to sealing a letter in a cover before sending it through the mail. SSL certificates also inspire trust because each SSL certificate contains identification information. When you request an SSL certificate, a third party verifies your organization's information and issues a unique certificate to you with that information. This is known as the authentication process.

SSL certificates keep online communications confidential even though the data pass through across the public Internet and they help clients to achieve the confidence to carry out with your web site. If you ask users of your web site to sign in, if they enter personal data such as credit card numbers online, or if they view confidential information such as health benefits or

financial accounts, you need to keep the data private. You also need to help them confirm that your web site is authentic.

An SSL certificate serves as a credential in the online world. Each SSL certificate uniquely identifies a specific domain and a web server. Trust of a credential depends on confidence in the organization that issued it. Certificate authorities have a variety of methods to verify information provided by individuals or organizations. Established certificate authorities, are well known and trusted by browser vendors. Browsers extend that trust to digital certificates that are verified by certification Authorities (CA)

6.7. WAYS TO ENCRYPT YOUR EMAILS

Encryption is a numerical process of coding and decoding information. The number of bits (40-bit, 56-bit, 128-bit, 256-bit) tells you the size of the key. Like a longer password, a larger key has more possible combinations. In fact, 128-bit encryption is one trillion times stronger than 40-bit encryption. When an encrypted session is established, the strength is determined by the capability of the web browser, SSL certificate, web server, and client computer operating system.

An SSL certificate contains verified information about the web site it secures to help users confirm that they are communicating web site in a secure manner. Extended Validation is the industry's highest standard of verification and provides the most visible guarantee to users: the address bar turns green in high-security browsers. When you display the Certification Authority Trusted Site Seal, users can click the trust mark to view web site identification information, the third party that verified it, and the expiration date of the SSL certificate.

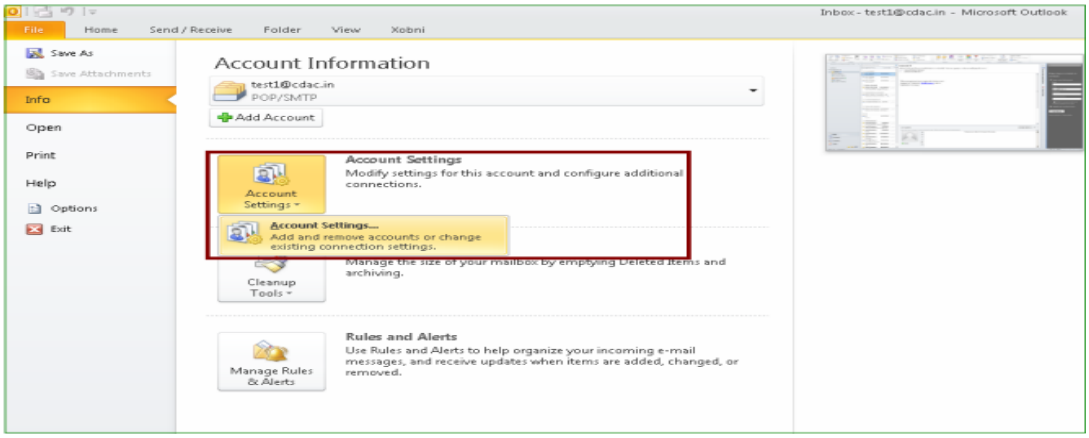
AN EXAMPLE HOW IT WORKS

- Bob sends Alice a signed e-mail. A signed -email includes the person's public key.
- Alice saves Bob's public key into her address book.
- Alice uses Bob's public key to send Bob an encrypted e-mail.
- Bob decrypts this e-mail using his private key.

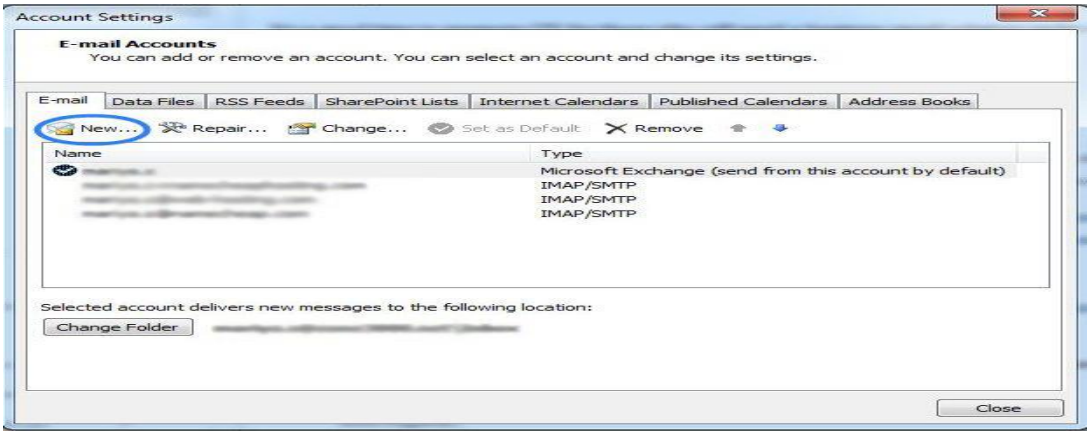
If you want to send a private message to a group of people you can use passphrase encryption that is long passwords, normally around 20 to 30 with numbers, letters and special case characters. It's easier to send to a group than with a public key and the catchphrase can be easier to remember. But you need to avoid transmitting the passphrase online and if somebody leaves the group you'll need to create a new passphrase all over again. Also, passphrase encryption isn't always available.

CONFIGURE SMTP-AUTHENTICATION IN MICROSOFT OUTLOOK

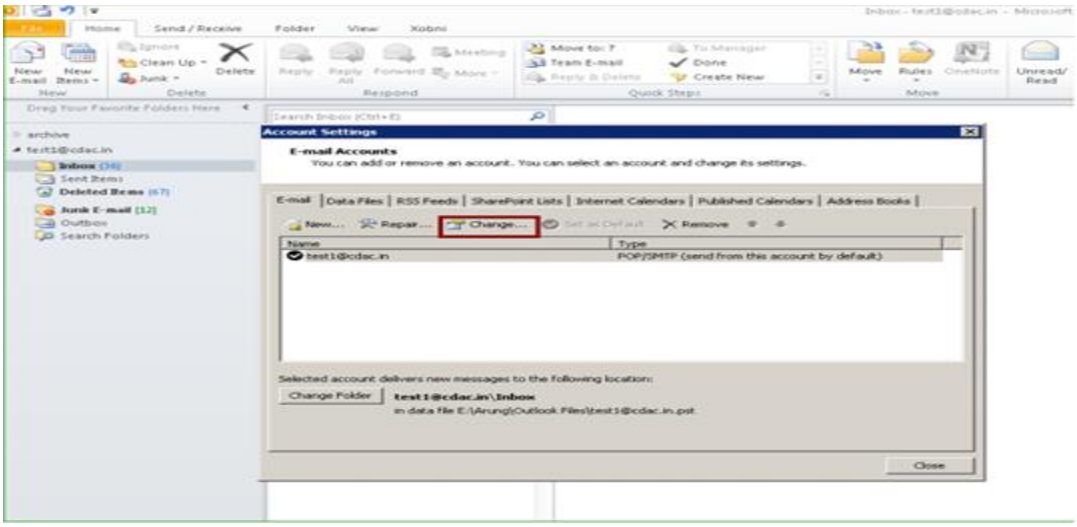
Step 1: Open MS Outlook & on the Tools/File menu, click Account Settings as shown



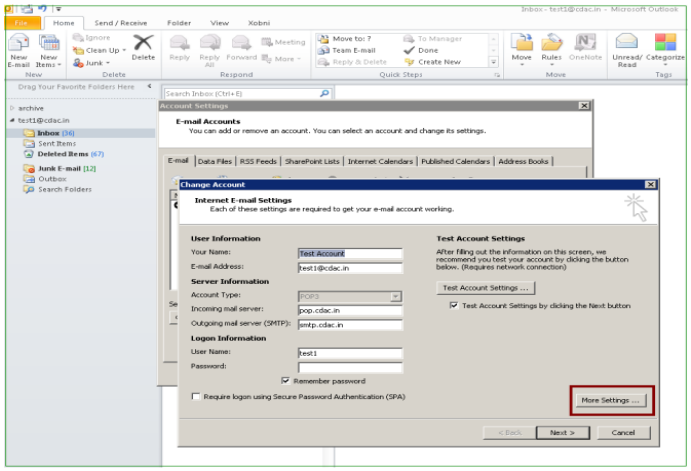
Step 2: Click 'New' in the new window



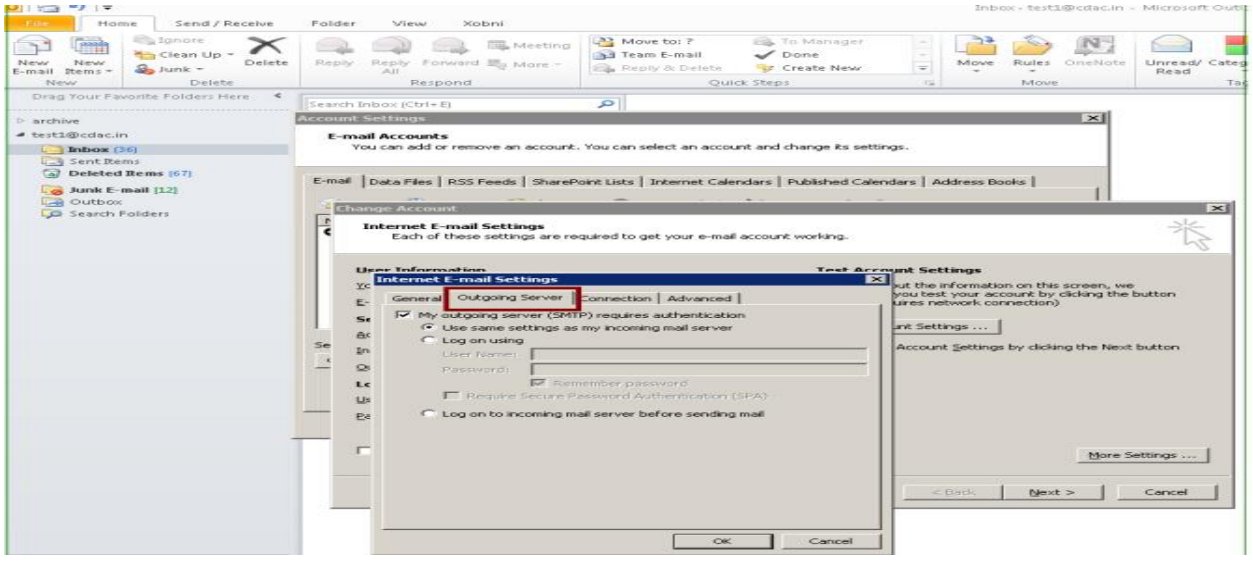
Step 3: Click on the "change" tab as shown in the below figure



Step 3: Click on “More Settings”

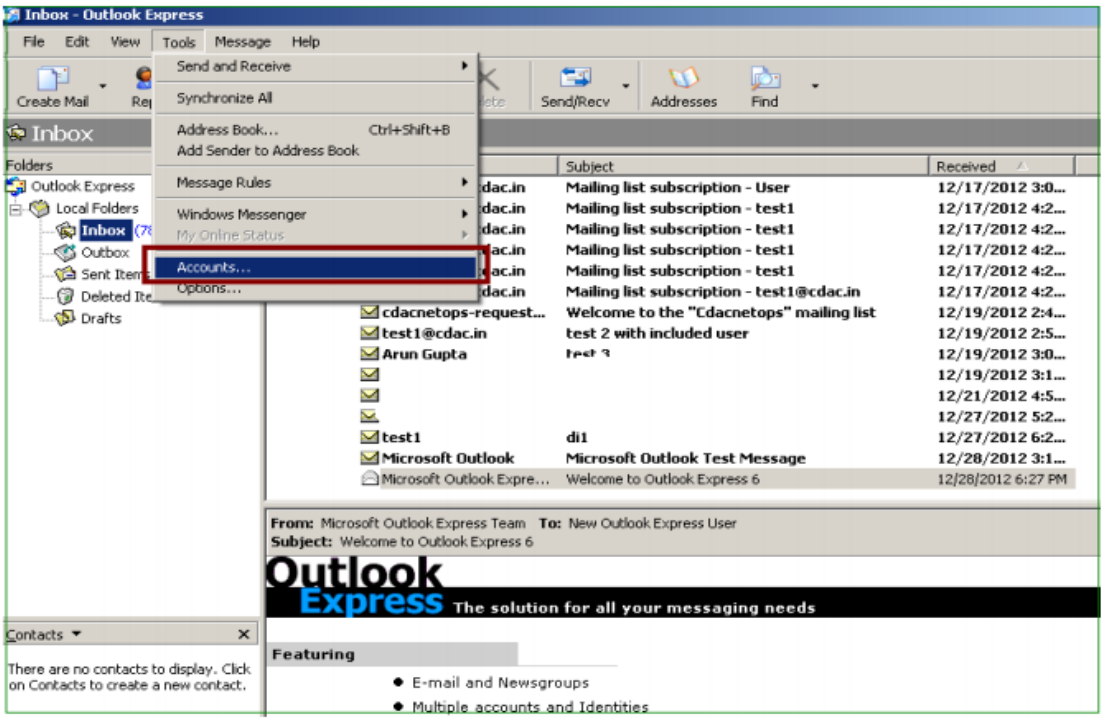


Step 4: Click on “Outgoing Server” tab and select 'Use same settings as my incoming mail server' as shown in the below figure

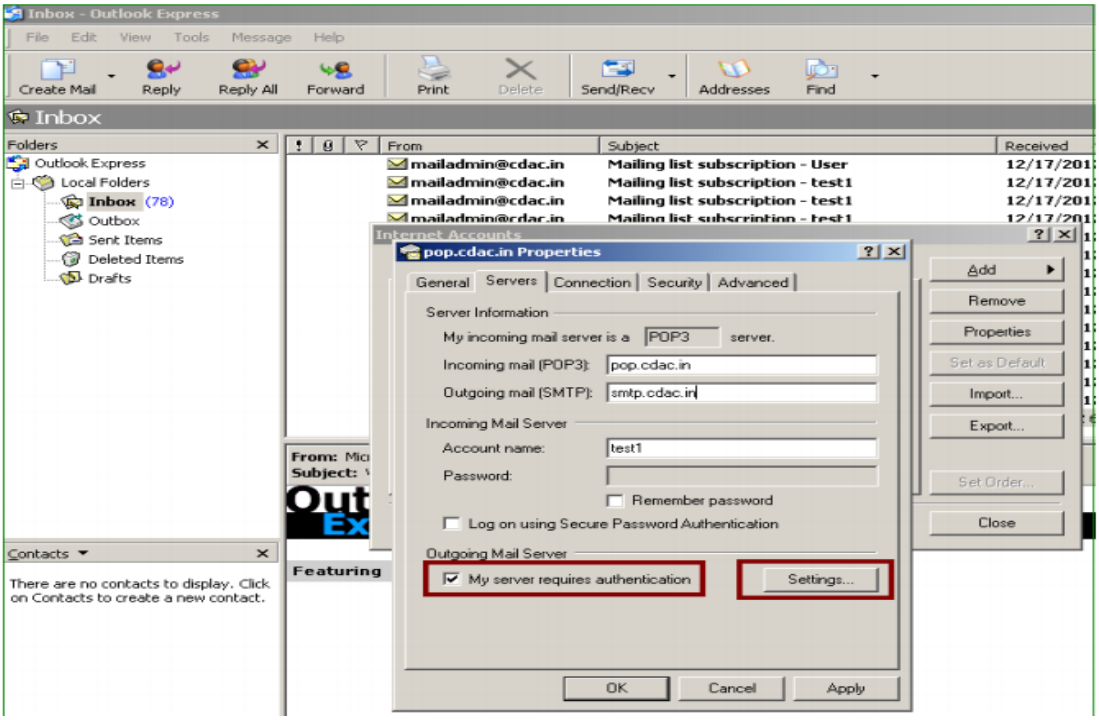


CONFIGURE SMTP - AUTH – OUTLOOK EXPRESS

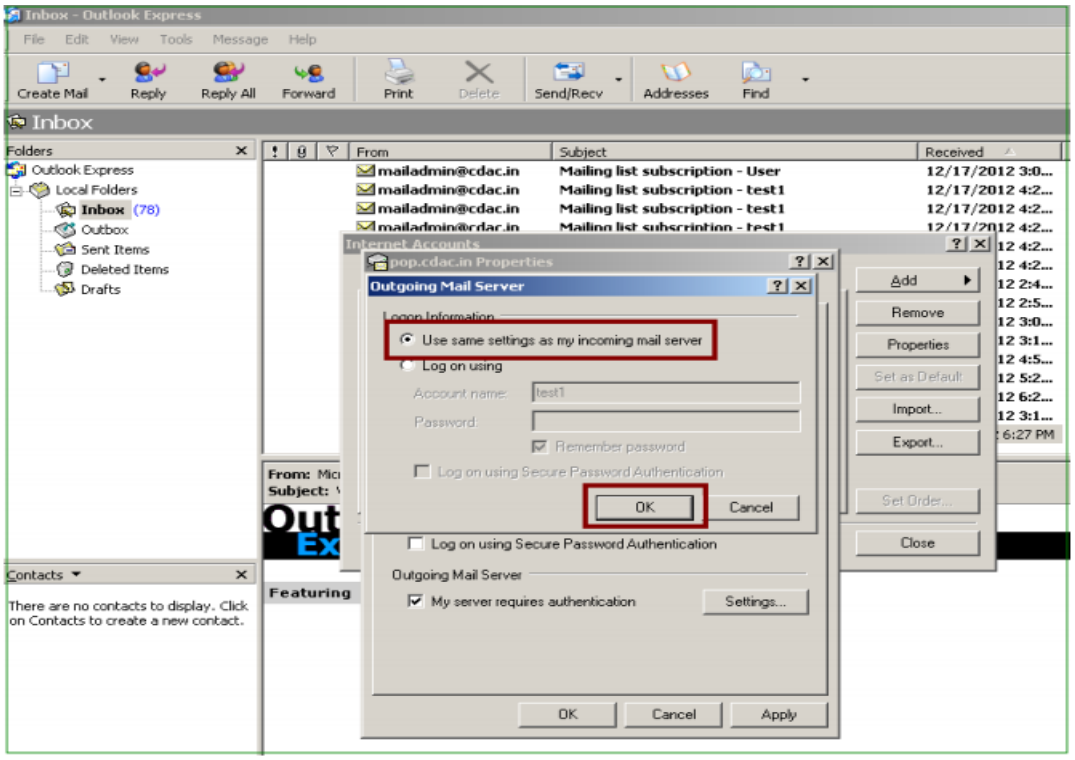
Step 1: Open Outlook Express & on the Tools menu, click Accounts as shown in the below figure



Step 2: Click on 'Servers' tab & select 'My Server requires authentication' then go to 'settings' as show in the below figure

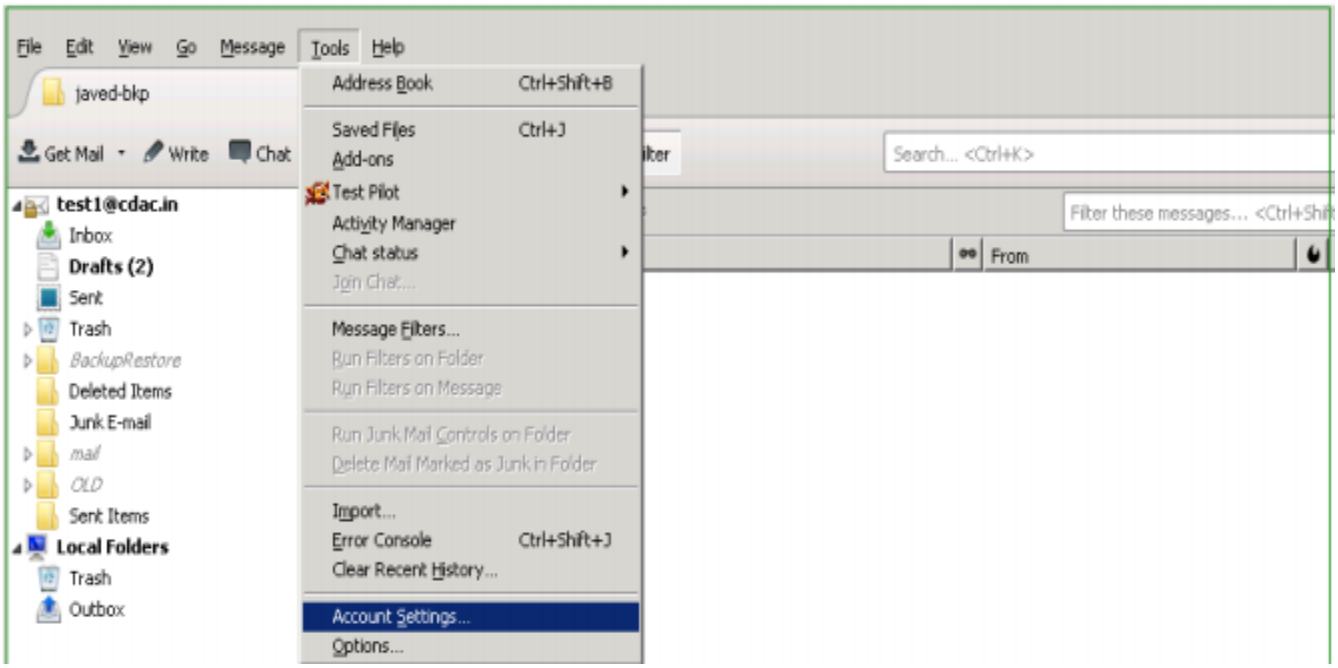


Step 3: Click on 'Use same settings as my incoming mail server' then OK

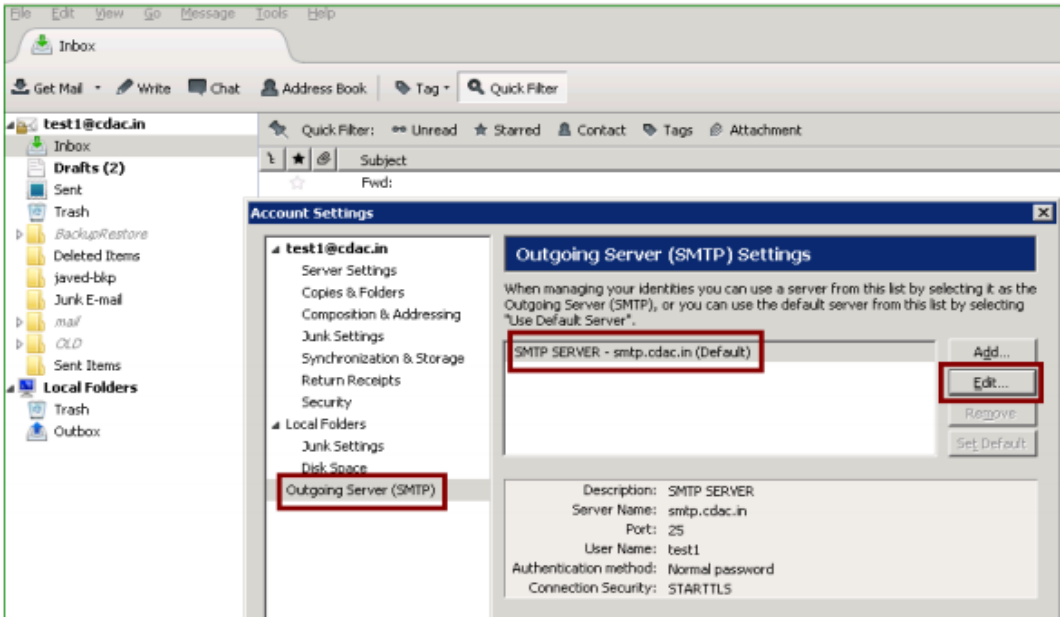


CONFIGURE SMTP AUTHENTICATION IN MOZILLA THUNDERBIRD

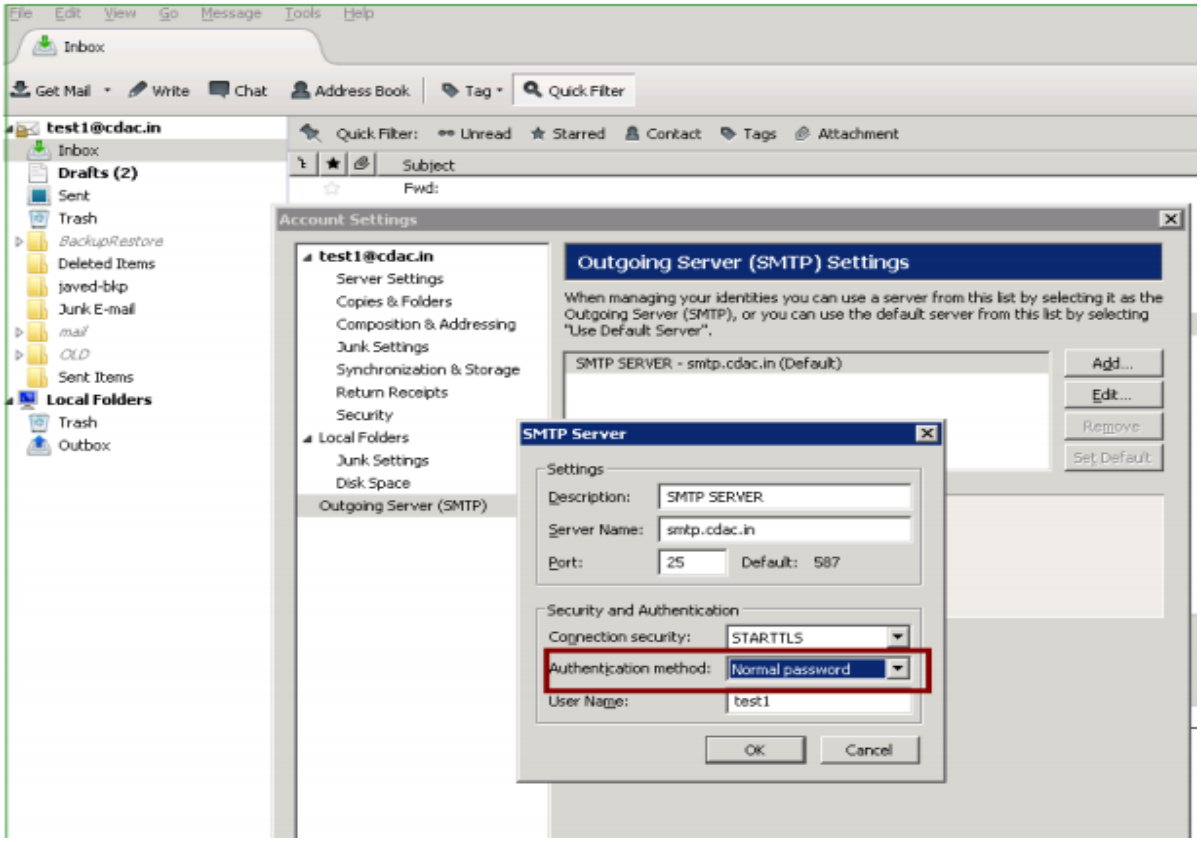
Step 1: Open Thunderbird & On the Tools menu, click Account Settings as shown in the below figure



Step 2: Click on 'Outgoing Server' and go to 'edit' tab as shown in the below figure



Step 3: Click on 'Authentication Method' & choose 'Normal Password' as shown in the below figure



6.8. INSTANT MESSAGING

Instant messaging (IM) is a real time text based communication between two or more people connected over the network like Internet. Instant message became most popular with this you can interact with people in a real time and you can keep the list of family and friends on your contact list and can communicate until the person is online .There are many instant service providers like AOL, Yahoo messenger, Google Talk and many more.

6.9. HOW DOES IM WORK

Instant messaging delivers the user's message to his desired contact directly. The message delivery is direct provided users contact person is online. The client software allows user to maintain a list of contacts that he wants to communicate. Such list is referred to as a buddy list or contact list. This contact list is nothing but e-mail ID of a contact. The user and his contact can send instant messages to each other provided both of them are on each other's contact list. The contact list can be managed by adding, deleting or editing the contacts e-mail ID and other related information.

Also a group can be formed of different ID. Creating groups helps when sending group communications. User can also block a particular contact or everyone who is not on his contact list from sending an instant message using privacy settings. User can send a message, file, graphics, image and voice to his contact. Messages can be printed, saved and archived. Nowadays use of web camera makes this communication even more exciting.

Now a day's all type of messenger service user can send an offline message to the other user on his contact list added in his account. When the other user logs on his messenger, message window pops up and makes user aware of the offline message. This makes it much more convenient than e-mail.

6.10. RISKS INVOLVED IN INSTANT MESSAGING

Hackers will be constantly accessing the instant messages and try to deliver malicious code through the instant message and the code may contain a virus, Trojan, and spyware and if you click on the file the code will enter your system and within a seconds it infects the system.

PUBLIC NETWORKS

Instant Messaging user's in the world utilizes public networks and IM provider's servers which are referred to as public IM or external IM. These servers are not secured by any firewalls. On the other hand IM in the private network also called as private or internal IM can be secured by firewall.

EAVESDROPPING

The sensitive information exchanged during an IM session is often stored in unsecured systems. As mentioned earlier Public IM provider's servers are not protected by any firewalls. It is very easy for someone to listen in on IM user's private chat

SPIM

Spim is a short form of spam over instant messaging; it uses IM platforms to send spam messages over IM. Like e-mail spam messages, a spim message also contains advertisements. It generally contains web links, by clicking to those links malicious code enters into your PC. Generally, it happens in real time and we need to stop the work and deal with spim as the IM window pop-ups, in the e-mail we have time to delete and we can delete all spam at a time, or we can scan before opening any attachments. This cannot be done in IM.

LACK OF ENCRYPTION

The IM session conducted using public network is like an open book to the entire Internet community. Communication via IM cannot be monitored or logged in order to maintain security with respect to confidential information.

6.11. RISKS INVOLVED IN EMAIL SECURITY AND CASE STUDIES

ATTACHMENTS

Sometimes attachments come with e-mail and may contain executable code like macros, ".exe" files and ZIPPED files. Sometimes attachments come with double extension like "attachment.exe.doc". By opening or executing such attachments malicious code may download into your system and can infect your system.

ILLUSTRATION 1:

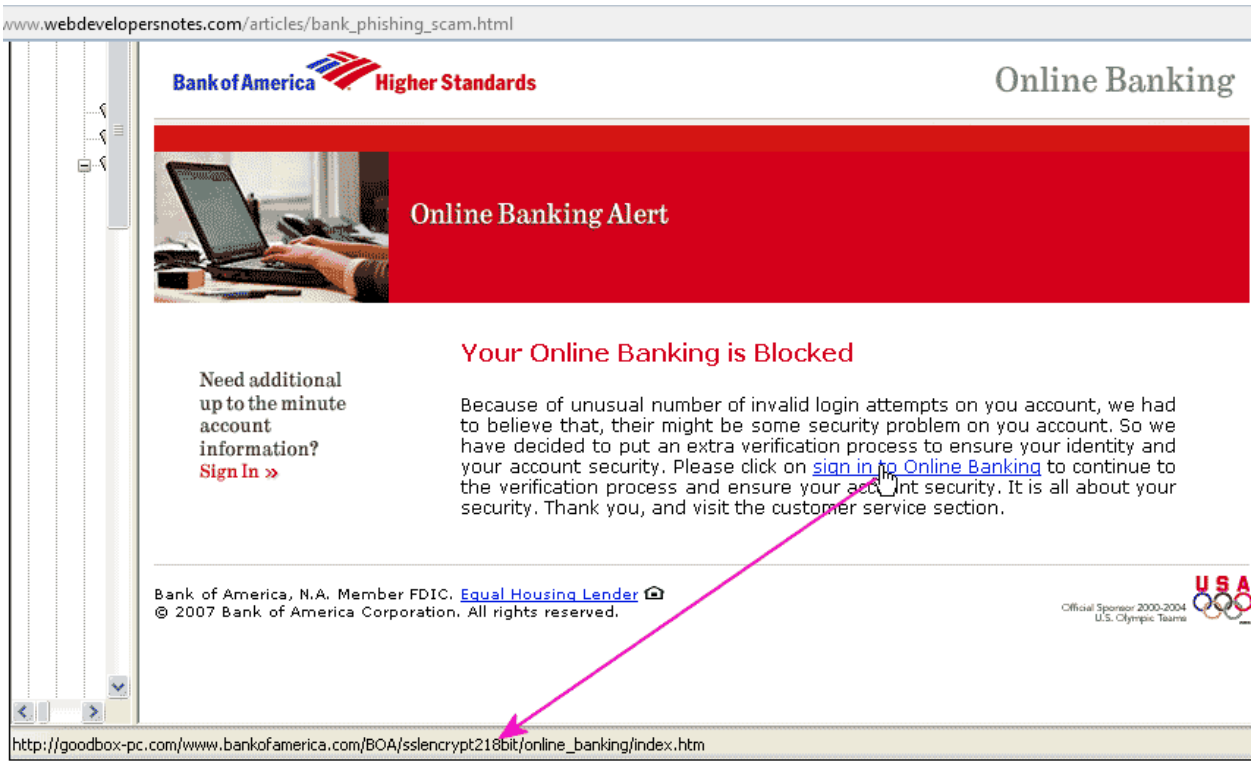
Raju received an notification attachment email from unknown recipient with the subject "Wow exclusive offer on gadgets offer valid for a limited period", Raju felt happy and clicked and downloaded the attached email to see more about the email after few minutes his system went into blue of death screen.

Example: http://fakebsod.com/

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

ILLUSTRATION 2:

Ajay received an attachment from xyz@abcbank.com website for updating the personal information. He filled the same and submitted the same to the same bank. After a week by checking his bank credit statement statements, he found some strange things of buying some products with his bank credit card. After contacting the bank officials they confirmed as a phishing attack. It is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means e-mail attachment.



For More:

http://security.arizona.edu/phishingexample

http://www.phishing.org/scams/credit-card-phishing/

http://www.webdevelopersnotes.com/articles/bank_phishing_scams.php

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

ILLUSTRATION 3:

Last month, Rahul wanted to purchase 10 Nokia phones for my newly-opened store so I contacted a supplier who could provide high quality, low-priced phones. Rahul was a bit suspicious at first because the prices were very much lower than those in the market. About the same time, I received an email attachment claiming to be from **xyz.com**. The email says that the supplier that I contacted is a verified supplier. The email further states that the supplier paid an Rs.600, 000 deposits to xyz.com and that xyz.com will protect my benefits should any dispute occur.

Rahul felt confident enough to trade with the supplier after receiving the email. I ordered and paid Rs.160, 000 worth of goods. After payment, Rahul waited for the goods, but nothing appeared. I tried contacting the supplier, but they did not reply. I turned to xyz.com for a refund, but they told me that they did not send any email to me.

EMAIL SPOOFING

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g. Siddharth has an e-mail address siddharth@xyz.org. He sends fake mails to his entire friend's contact list. Siddharth spoofs his e-mail and sends obscene messages to all her contacts. Since the e-mails appear to have originated from Ajay, his friends may take offence and friends ship relationships may be spoiled for life.

Generally to send an email the sender has to enter the following information:

- email address of the receiver of the email
- email addresses of the persons who will receive a copy of the email also referred to as CC for carbon copy
- email address of the persons who will receive a blind carbon copy but whose identities will not be known to the other recipients of the e-mail
- A short title / description of the message

Certain web-based email services like www.sendfakemail.com, offer a facility wherein in addition to the above, a sender can also enter the email address of the purported sender of the email.

IILUSTRATION 1:

Consider Mr. Siddharth whose email address is siddharth@hotmail.com. His friend Ajay's email address is ajay@yahoo.com. Using SendFakeMail, Siddharth can send emails claiming to be sent from Ajay's email account. All he has to do is enter ajay@yahoo.com in the space provided for sender's email address. Ajay's friends would trust such emails, as they would suppose that they have come from Ajay whom they trust. Siddharth can use this misplaced trust to send viruses, Trojans, worms etc. to Ajay's friends, who would unknowingly download them.

Example: http://www.sendfakemail.com/

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

ILLUSTRATION 2:

Arnav received an email from his friend Ajay with subject best offers in the market, Arnav opened the email and clicked on the link which redirected to the interesting page and he started browsing and opening some other pages and he continued the same after few days his email was not accessible and his friends received the emails with inappropriate content.

SPREADING TROJANS, VIRUSES AND WORMS

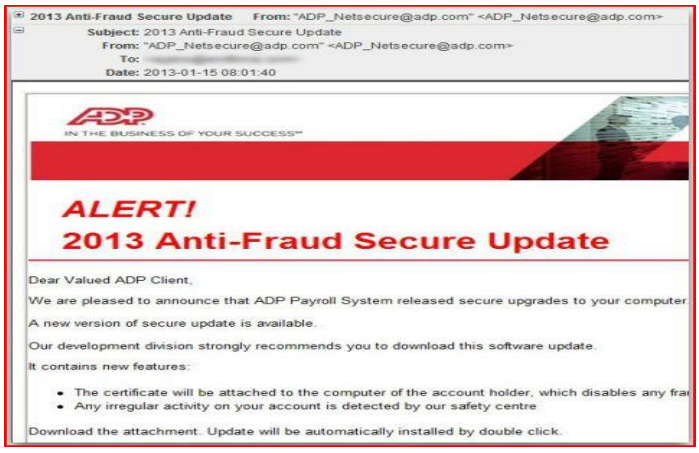
A computer virus is a program which can replicate and attach itself to a program or files infecting the system without its knowledge. A Computer virus can be spread from one host to another by sharing infected file or by downloading infected files from un-trusted sources .All computer viruses are man-made, they spread only with human assistance and support. Virus can be installed in a computer by downloading applications from un-trusted sites, by a removable medium like USB, CD, DVD's and sharing files from one infected computer to another also virus comes through attachments with e-mails.

ILLUSTRATION 1:

Aarav receives malicious link information@mcaffee.com which is a spoofed email but the Aarav does not know much about this. The email informs him that the attachment contained with the email is a security patch that must be downloaded to detect a certain new virus. Most unsuspecting Aarav would submit to such an email if they are using a registered copy of the McAffee anti-virus software and would download the attachment, which actually could be a Trojan or a virus itself!

Example: https://nakedsecurity.sophos.com/2013/01/15/bogus-adp-anti-fraud-update-emails/

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser



For More Refer:

http://www.firetrust.com/products/benign/support/about_email_viruses_and_worms

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

ILLUSTRATION 2:

Ronith used to get 100 or more than 100 emails per day to his personal email ID which is used for personal purpose as well as official purpose so most of the time his official emails used to be received in spam/junk folder so he opened one email received in spam folder after some finishing his work he signed out and carried with some other works. Next day when he was trying to login into his email ID he couldn't login and got error message "user name or password in incorrect".

ILLUSTRATION 3:

Atul received the pop-up message that claims your computer is infected with dozens of viruses, and that will offer to clean your system for a fee. If you provide your credit card or banking information and the scammers will then have access to your funds and will steal even more of your money.

EMAIL BOMBING

Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account or in case of an individual or company email or web servers crashing. A simple way of achieving this would be to give to the victim's email address to a large number of mailing lists. Mailing lists are very popular and can generate a lot of daily email traffic depending upon the mailing list. All that one has to do is compose a message, enter the email address of the victim multiple times in the "To" field, and press the "Send" button many times.

ILLUSTRATION 1:

Vivaan writing the email address 25 times and pressing the "Send" button just 50 times (it will take less than a minute) will send 1250 email messages to the victim! If a group of 10 people do this for an hour, the result would be 750,000 emails. These tools send multiple emails from many different email servers, which make it very difficult, for the victim to protect himself with such type of effects.

ILLUSTRATION 2:

In one case, a foreigner who had been residing in Ooty, India for almost thirty years wanted to avail of a scheme introduced by the Ooty Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Ooty Housing Board and repeatedly kept sending e-mails till their servers crashed.

THREATENING EMAILS

Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.

ILLUSTRATION 1:

In a recent case, Sophia received an e-mail message from someone who called him or herself 'your friend'. The attachment with the e-mail contained morphed pornographic photographs of Sophia. The mail message said that if Sophia were not to pay Rs. 10,000 at a specified place every month, the photographs would be uploaded to the Internet and then a copy sent to her fiancé.

Scared, Sophia at first fulfilled with the wishes of the blackmailer and paid the first Rs. 10, 000. Next month, she knew she would have to approach her parents. Then, trusting the reasonableness of her fiancé she told him the truth. Together they approached the police. Investigation turned up the culprit - Sophia's supposed friend who wanted that Sophia and her fiancé should break up so that she would get her chance with him.

Florida Man Cyberstalked Teen Girl For Five Years

By Ashley Helms | Oct 16, 2014 01:27 PM EDT Email Print

For More Examples:

http://www.hngn.com/articles/46102/20141016/florida-man-cyberstalked-teen-girl-for-five-years.htm

http://www.dailymail.co.uk/news/article-2876503/Sony-hackers-latest-chilling-warning-threatens-9-11-like-attacks-theaters-showing-Interview.html

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

ILLUSTRATION 2:

A 16 year old student from ABC City who threatened to blow up XYZ Railway station in an email message was found guilty by the Juvenile court in ABC city. A private news channel received an email on 18 Sep 2014 claiming sender as ADDA gang saying a bomb would be planted on an unspecified train to blow it up.

The case was registered in ABC Police station under section 506 of IPC and transferred to cyber crime investigation cell. During Investigation CCIC traced the cyber cafe from which the email account was created and threatening email was sent.

Cafe owner told police about friends which had come that day to surf the net. Police summoned them and found that the system which was used to send email was accessed by only one customer. On 22nd Dec 14, police arrested the boy a Class XII science student who during interrogation said that he sent the email for fun of having his prank flashed as "breaking news'' on television.

EMAIL FRAUDS

Email fraud is the intentional fraud made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to take advantage of people.

ILLUSTRATION 1:

It is very often used to commit financial crimes. It becomes a simple thing not just to imagine someone else's identity but also to hide one's own. The person committing the crime understands that there is very little chance of his actually being identified. In a recently reported case, a Pune based businessman received an email from the Vice President of the ABC Development Bank (AbcDB) offering him a profitable contract in return for Rs 10 lakh. The businessman verified the email address of the Vice President from the web site of the AbcDB and subsequently transferred the money to the bank account mentioned in the email. It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

ILLUSTRATION 2:

In another famous case, one Mr. Yash sent himself spoofed e-mails, which were supposedly from the Lulu Lottery Company. These mails informed him that he had won the largest lottery. He also created a website in the name of the Lulu Lottery Company, announced n it that he had won the Lulu Lottery and uploaded it on to the Internet. He then approached the Income Tax authorities in India and procured a clearance certificate from them for receiving the lottery amount. In order to let people know about the lottery, he approached many newspapers and magazines.

The media seeing this as a story that would curiosity a lot of readers hyped it up and played a vital role in spreading this misinformation. Mr. Yash then went to many banks and individuals

and told them that having won such a large sum of money he was afraid for his safety. He also wanted to move into a better house. He wheedled money out of these institutions and people by telling them that since the lottery prize money would take some time to come to him, he would like to borrow money from them. He assured them that the loan amount would be returned as soon as the lottery money came into his control.

It was only when he did not pay backing the loan amounts to the banks that they became suspicious. A countercheck by the authorities revealed the entire scheme. Mr. Yash was arrested. Later, it was found that some of the money had been donated for charitable causes and also to political parties!

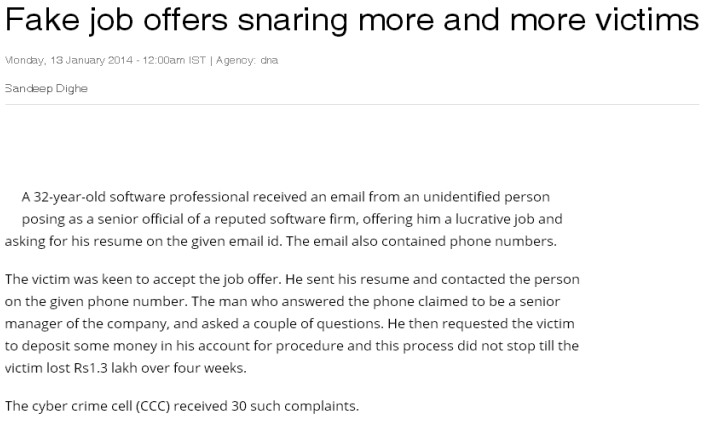
EMPLOYMENT SCAMS

This scam targets people who have posted their resumes on e.g. job sites. The scammer sends a letter with a inaccurate company logo. The job offer usually indicates exceptional salary and benefits and requests that the victim needs for working in the country and includes the address of a fake government official to contact which are fake. A variant of the job scam recruits freelancers seeking legitimate gigs such as in editing or translation, then offers pre-payment for their work. The scammer contacts the victim to interest them in a work-at-home opportunity or asks them to cash a check or money order that for some reason cannot be redeemed locally.

ILLUSTRATION 1:

Mr. Abhijeet posted his resume on a website. Later, he received a job offer from a European trading company looking for US personnel to intermediate marketing transactions overseas. This company claimed to be a broker company through testabc.com. They also claimed that the job was to help their company collect payment in the US and that they would pay 10% commission to Mr. Abhijeet.

The company sent him a business cheque, which Mr. Abhijeet deposited into his account. The European company then instructed him to purchase Western Union money orders, and send them to the UK and other locations in Europe. Sometime later, Mr. Abhijeet's bank contacted him to inform him that the business cheque he had deposited was a fake. Unfortunately, Mr. Abhijeet had already paid the Western Union money order expenses and lost his money.



Fake job offers snaring more and more victims

Monday, 13 January 2014 - 12:00am IST | Agency: dna

Sandeep Dighe

A 32-year-old software professional received an email from an unidentified person posing as a senior official of a reputed software firm, offering him a lucrative job and asking for his resume on the given email id. The email also contained phone numbers.

The victim was keen to accept the job offer. He sent his resume and contacted the person on the given phone number. The man who answered the phone claimed to be a senior manager of the company, and asked a couple of questions. He then requested the victim to deposit some money in his account for procedure and this process did not stop till the victim lost Rs1.3 lakh over four weeks.

The cyber crime cell (CCC) received 30 such complaints.

Example:

For More Reference:

http://www.ndtv.com/article/cities/delhi-two-men-arrested-for-duping-people-with-fake-job-promise-568667

Reference:

http://www.dnaindia.com/pune/report-fake-job-offers-snaring-more-and-more-victims-1949862

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

LOTTERY SCAM:

In a typical lottery scam, the victim receives official-looking communication in the mail that tells them they have won lakhs in a lottery. In order to collect their winnings, they need to send money to cover the taxes and administrative fees. Those who do send money are placed on lists and receive further mail and phone calls telling them to send more money. To keep the victims quiet while the scam is in progress, the fraudsters tell them not to discuss their "good fortune" with anyone until the official announcement. Before long, the victims are drained dry of their money and in most instances, the money is never recovered.

ILLUSTRATION 1:

Twenty-two year old Aishwarya loved her mother Amisha enormously. Theirs was a close relationship however in recent months, Aishwarya sensed that something was troubling Amisha. She was unusually withdrawn, secretive, and appeared depressed. Her mother also appeared to be getting a lot of mail, most of it spotted about the lottery. Aishwarya remembered how only a few months earlier Amisha appeared thrilled and happy.

The phone call from Amisha's bank manager came out of the blue and shook Aishwarya to her core. Amisha had withdrawn almost all of her savings in a very short period of time and the manager was concerned. Her mother was convinced that she had won fifty lakhs in a lottery and had been sending thousands of rupees to "collect" her significant winnings in the form of tax. Of course, the lottery was a scam and her mother was out of money.

TIP: Remember, if it seems to be too good to be true, it is. Legitimate winners of lotteries never have to send money to claim their winnings.

7 February 2014 Last updated at 01:00

Share

Man travels 1,000 miles to claim bogus prize

By Geeta Pandey
BBC News, Delhi

Ratan Kumar Malbisoi travelled more than a thousand miles to claim a bogus prize

An Indian villager recently travelled more than a thousand miles to the BBC office in Delhi in an unusual quest - to claim millions of rupees he believed he had won in a "BBC lottery".

In today's Magazine

The day the Pintupi

Ratan Kumar Malbisoi, a 41-year-old unemployed Indian villager, fell for a

Example: http://www.bbc.com/news/world-asia-india-26012779

http://www.moneylife.in/article/beware-of-lottery-spam-scam-on-rbis-name/37316.html

https://www.scamwarners.com/forum/viewtopic.php?f=34&p=231702

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

WORK-AT-HOME-E-MAIL FRAUD:

A work-at-home method is a get-rich-quick scam in which a victim is lured by an offer to be employed at home; very often doing some simple task in a minimal amount of time with a large amount of income that far exceeds the market rate for the type of work. The true purpose of such an offer is for the person behind to obtain money from the victim, either by charging a fee to join the scheme, or requiring the victim to invest in products.

ILLUSTRATION 1:

Ajay was trying hard to buy a car but he doesn't have for extra money to afford it. His friends told him regarding such work from home concept, so during browsing from Internet he came across some contact numbers and email ids for help regarding the work from home. Ajay

immediately mailed he requires such type of work and paid initial some amount in the form of registration or confirming the same for job. After waiting for a week an email came to me offering me a job that I could work from home.

The job was to receive cashier checks and money orders and cash them at my bank and transfer the money to another country. I took the checks to my bank and deposited them and the bank called me and told me that they were fakes and I was shocked. I told the people that emailed about the checks that they were fake and I never heard from again. A few months later I was arrested in the case of cheque bounce.

Tip: It's better to consult the head office or supporting team. If you're considering a work-at-home opportunity, ask questions and do some research before committing any money.

ILLUSTRATION 2:

A work from home fraud which could run into a whopping Rs 1 crore has been to bring to public notice at leading multinational company at Gurgaon. Gurgaon Police Commissioner Abhinav Chawal said an FIR was made under sections of cheating and forgery against a bank employee and three others has been lodged and 18 accounts having close to Rs 1 crore have been made into public. Sources said funds amounting to Rs 1 crore of 20 high networth customers have been fraud. The fraud is said to be a work of Shivraj Rahul, the employee of **XYZ** MNC Company who is alleged to have sold investment products to high networth clients, claiming that they would generate unusually high returns. He is also accused of claiming that these products were authorized by the bank's investment product committee.

Sources said Rahul allegedly sought deposits from customers in profitable schemes but transferred the funds to some pretended accounts. It is also alleged that Rahul, who is named in the FIR, showed a forged notification of market controller Securities and Exchange Board of India for obtaining funds from customers.

Reference:

http://www.forbes.com/sites/groupthink/2011/12/13/16-work-at-home-scams-to-avoid/

http://career-advice.monster.com/job-search/getting-started/avoid-work-from-home-job-scams/article.aspx

MEDICAL ALERT SCAM

This is a telemarketing scam that promises a free medical alert system, that scam targeted seniors and caretakers. The fake calls claimed to be offering the medical alert devices and system free of charge because a family member or friend had already paid for it.

ILLUSTRATION 1:

Akshay received an email saying free medical service and free offers that require your personal information to be needed. Secondly it was asked to provide their bank account or credit

information to 'verify' their identity and, as a result, was charged the monthly of Rs 2000 /- service fee. The system of course, never arrived and the akshay was left with a charge they had trouble getting refunded.

Tip: Always verify with the supposed friend or family member that the caller says paid for the service.

Reference: http://timesofindia.indiatimes.com/city/patna/Medicine-scarcity-in-Bihar-post-scam-Modi/articleshow/42291554.cms

PAY A FEE TO RECEIVE MILLIONS SCAM

Sometimes you receive an email like “you won a lottery of million dollars” receiving such a kind of mails is a great thing, and really it’s a happiest thing. By responding to such a kind of mails huge amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money.

ILLUSTRATION 1:

I have received various e-mails from people overseas asking me to be the party to receive payment of money Mr. Adarsh has left in a bank in Korea. I have also received overseas e-mails informing me that my e-mail address was chosen as a winner and that I am to send Rs 50,000 to pay for transferring service fees & taxes. I almost sent my money and all my information. After a month I came to now that I was trapped by scammers and e-Mails with a subject line you won Rs 50 Lakhs rupees

Tip: Don’t get trapped by scammers and e-Mails with a subject line you won some $10000 just think why only you received the email without your participation**.**

BETTER BUSINESS BUREAU SCAM

The Better Business Bureau Scam look like legitimate email and cheat with respect to your banking and financial information. And they won’t mind destroying your computer to get it. Attackers sending emails that appear to come from your trusted Better Business Bureau. They’ll tell you that a complaint has been registered against your business. It doesn’t matter that you might not even OWN a business.

ILLUSTRATION 1:

One fine morning Atul received an email asking you to download and complete an attached form and respond to the consumer posting. After filling up the attached form he got the message telling that we have updated your personal information. After a month when he got the credit card bill he surprise to see un-usual bills from the strange locations and he immediately called the bank. The bank officials clearly told it is an act of email fraud where the “attached form” is actually an executable file that will drop a malicious virus onto your system.

The links in the bogus email are dangerous, as well. They look like a link to a Better Business Bureau page, but the code behind the link will actually method your browser to a website where malware is dropped onto your computer. The malware is written in such a way that it usually passes by anti-virus programs undetected. Once the malware is in place, the scammer can sniff for your banking information including user names and passwords, and can use your system to send more scam emails out to your contacts under your name.

IRS SCAMS

A fake tech support caller claims he needs access to your computer to fix a non-existent bug. But a new twist involves the caller actually installing a virus on victims' computers. You get a telephone call from someone claiming to be with tech support from a well-known software company. The scammers may know your name and other personal information, which they get from publicly available phone directories. They might even guess what computer operating system you're using.

ILLUSTRATION 1:

Aadarsh receives a phone call on Thursday April 24th approximately 7:34 am claiming to be a Microsoft tech he went on saying and pointing out all errors and asked me to go into my computer step by step so he can show me what was wrong being it was early and caught me off guard I fell for it, and very upset by it! He actually was into my computer asking me what I do most on my computer, online shopping, banking executive! Then proceeded to tell me I needed to fix my computer or it will eventually crash! Afterwards he told me there was a onetime fee of around 1000 Rs to replace infected software's and fix security issues.

I told him I am not interested, he questioned me by saying, "you don't want to fix your computer. And you want it to crash, why? Finally he gave up and said goodbye! Is my computer now infected and how is it so easy for these criminals to get your information?

ILLUSTRATION 2:

I just received a call that came in as Skype from a name Anurag Mishra with a heavy foreign accent. It sounded Indian. He said he was calling for Microsoft support and that Microsoft was receiving error messages from our computer. He said Microsoft would not work on our computer any more. I found this very suspicious. He told me he worked for a company named Support Plaaza, which Microsoft used to fix software problems. He had me hold down the Windows key on my keyboard + the R key, which brings up a box for RUN. Then he wanted me to type in "eventvwr". At this point I asked for a number where I could call him back. He gave 1-866-856-4811. I'm sure they were getting ready to install a virus.

INVITATION LETTER FRAUD

Some fraudsters use an export & import company to run illegal immigration rackets. The company will pretend to be buyers and ask to visit the supplier' factory to negotiate more business or inspect production facilities. For this, they will ask for an official invitation letter

from the manufacturer. When they receive the invitation letter, it will then be used to apply for a visa for an illegal immigrant.

ILLUSTRATION 1:

A few days ago, I met a buyer who asked about the prices of our products. After working out the prices, I replied to the inquiry. The buyer accepted the quoted prices and told me they would like to visit our company for further cooperation. They asked for an invitation letter so they could get the required business visa.

I sent an invitation letter and was surprised when the buyer said a company-issued invitation letter was not accepted in their country. The buyer asked for an invitation letter from my local government instead. After spending a lot of time preparing documents for my local government offices in ABC country, I finally got an invitation letter issued by the ABC government and sent it to my client. Once they received the invitation letter, they stopped replying to my emails.

5.13. CONCLUSION

Email is not secure. Email encryption is very critical for a variety of reasons, including compliance with regulatory obligations to protect the integrity of sensitive data and best practices focused on maintaining the confidentiality of corporate data. Simply using encryption is not enough: you need to know how to use the encryption system properly, because improperly used encryption offers little more protection or sometimes none at all.

Organizations should put policies and make sure they are kept up-to-date to ensure compliance. Individuals should have anti-virus software on their computers and also backup their emails on their personal computers and as well as from the Email server. Organizations and individual should focus on encryption across applications, i.e. use systems that are interoperable. If you use one system and the person you want to send/receive message to/from is on another, and the two are not well-matched, then you will not be able to send each other encrypted messages.

Pretty Good Protocol and S/MIME resolve many problems but also create some compatible issue. The first one is interoperability issue where PGP and S/MIME are completely incompatible. If you are using PGP and your friend is using S/MIME, you will not be able to send each other secure messages.

PGP and S/MIME keys use asymmetric key encryption to protect the contents of your messages all over their total journeys. They provide:

- Protection against eavesdropping and unwanted backups
- Message Digests to detect whether messages have been altered in journey
- Signatures to prove sender authenticity

Public key cryptography systems have one problem. Such systems are computationally intensive and thus are extremely slow to use. Many companies are using SSL to encrypt

communications with their email servers. Do not set your IM client to automatically accept file transfers. If you do, you put yourself at very high risk of automatically accepting virus- infected files unintentionally.

Before opening any file received via IM, you should always verify with the sender that he or she did really send that file to you. In addition, make sure the file has been scanned by latest and updated anti- virus software before opening it. Never click URL links within an IM that is sent from unknown or suspicious contacts. There might be chances of viruses being spread when users clicking on an IM URL. Never send personal or sensitive information by IM. Even you really want to send, make sure your sensitive information is encrypted.

13. REFERENCE

http://www.thegeekstuff.com/2013/05/how-email-works

http://features.en.softonic.com/email-encryption-how-it-works-and-how-to-use-it

http://www.thawte.com/resources/getting-started/ssl-faq/

https://www.sslshopper.com/email-certificates-smime-certificates.html

http://lifehacker.com/180878/how-to-encrypt-your-email

http://www.ibm.com/developerworks/lotus/library/ls-SMIME/

Chapter 6:
Social Networking Security

6. SOCIAL NETWORKING

6.0. INTRODUCTION

The use of Social Networking Services has become a common and important part of everyday communication in India. Young people in India are particularly passionate users: the vast differences are engaging on a daily basis with SNS via a computer or mobile phone. Research in this area is a growing field and studies identifying the negative impacts have been likely to control the popular media and much policy development. However, there is considerable proof of the benefits associated with SNS use, which has been largely ignored in public debate. The following report summarizes how the school teachers teaches the current evidence concerning the enabling effects of SNS in the context of young people's and school students in everyday lives.

The School teachers should aware the benefits of SNS use which directly or indirectly dependent on moral Internet and media knowledge: having the skills to critically understand, analyze and create media comfortable. Maximizing the benefits of SNS and promoting Internet and media literacy may help protect young people and students from many of the risks of online interaction, such as cyber - bullying, privacy breaches and predation.

For example, understanding how to produce creative content and manage the distribution of this content supports fully informed decision making and assessment of one's own, and others, privacy. Policy currently focuses primarily on regulating the negative effects of SNS and social media, frequently framing digital citizenship within an online risk - management example.

6.1. WHAT IS SOCAIL NETWORKING

A social network is a social structure made of nodes which are generally individuals or organizations that are tied by one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friendship, dislike, conflict or trade. Most of the students use social networking sites for fun, Employee find suitable and helpful for job hunting, and teachers great for keeping in touch with friends, business contacts and relatives etc.

A Social Network Service focuses on building online communities of school children's and teachers and people who share interests and/or activities, or who are interested in exploring the interests and activities of others. The other side of Social Network is security and privacy issues and is entirely treated as two different issues. As security issue is a hacker gains unauthorized access to sites protected resources and the privacy issues is someone can gain access to confidential information by simply watching you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user.

The reason social network security and privacy lapses exist results simply from the astronomical amounts of information the sites process each and every day that end up making it much easier to exploit a single flaw in the system. Features that invite user participation -- messages, invitations, photos, open platform applications, etc. are often the avenues used to gain access to private information.

Now a day's most of the school children's are using social Networking sites in their mobile phones as a third party application program interface (API) if not used properly or aware of the such social networking goods and bad allows for easy theft of private information and it gave developers access to more information like addresses, pictures than needed to test the applications.

Social networking means grouping of individuals into specific groups, like small communities. Social networking is used to meet Internet users, to gather and share information or experiences about any number of topics, developing friendships, or to start a professional relationship. A simple Social Networking site is where different people keeping different information related to any particular thing at one place. For example Twitter, Facebook, etc.

Through social networking there are many advantages like we can get into any kind of groups based on our hobbies, business, schools and many more, it is a different communication tool to keep in touch with friends and colleagues. Apart from all these advantages there are disadvantages like based on these communication tools, sites can be trapped by scammers or any hackers so it is very important to protect yourself.

These social networking sites are very popular with young people. They expose them to risks they have always faced online but in a new forum: online bullying, disclosure of private information, cyber-stalking, access to age-inappropriate content and, at the most extreme, online grooming and child abuse. For adults, who are also using these sites in greater numbers, there are serious risks too. They include loss of privacy and identity theft. Adults too can be victims of cyber-bullying and stalking.

6.2. SOCIAL NETWORKING RISKS

Harassment and bullying

Cyber bullying can be carried out through an Internet service such as email, chat rooms, discussion groups, instant messaging or web pages. It can also include bullying through mobile phone technologies such as SMS. Cyber bullying can include teasing and being made fun of, spreading rumors online, sending unwanted messages and defamation.

Cyber bullying can be done in the following ways

Forwarding a private IM communication to others

A kid/teen may create a screen name that is very similar to another kid's name. The name may have an additional "I" or one less "e". They may use this name to say inappropriate things to

other users while posing as the other person. Children may forward the above private communication so others to spread their private communication.

Impersonating to spread rumor's

Forwarding gossip mails or spoofed mails to spread rumors or hurt another kid or teen. They may post a provocative message in a hate group's chat room posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier.

Posting embarrassing photos or video

A picture or video of someone in a locker room, bathroom or dressing room may be taken and post it online or send it to others on cell phones.

By using web sites or blogs

Children used to tease each other in the playground; now they do it on Web sites. Kids sometimes create Web sites or blogs which may insult or endanger another child. They create pages specifically designed to insult another kid or group of people.

Humiliating text sent over cell phones

Text wars or text attacks are when kids gang up on the victim, sending thousands of text-messages related to hatred messages to the victim's cell phone or other mobile phones.

Threatening e-mails and sending pictures through e-mail or mobile to hurt another

Children may send hateful or threatening messages to other kids, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.

Insulting other user in Interactive online games

Kids/Teens verbally abuse the other kids/teens, using threats and foul language while playing online games or interactive games.

Stealing Passwords

A kid may steal another child's password and begin to chat with other people, pretending to be the other kid or changes actual user profile.

6.3. SOCIAL NETWORKING SITES CASE STUDIES:

CYBERBULLYING:

Cyber bullying can be carried out through an Internet service such as email, chat rooms, discussion groups, instant messaging or web pages. It can also include bullying through mobile phone technologies such as SMS. Cyber bullying can include teasing and being made fun of, spreading rumors online, sending unwanted messages and defamation.

ILLUSTRATION 1:

Because her daughter loved performing, Anupama felt she was being supportive by giving Aishwarya a camcorder for her 13th birthday. The days and weeks following her birthday Aishwarya recorded everything, from the family dog playing to her mom cooking and, of course, herself, singing and acting out her favorite movie scenes. Her home videos became so popular that her family from out of state asked to see them.

When Aishwarya asked her if she could open a facebook account for video-sharing, her mother anupama was doubtful at first. However, she agreed after Aishwarya promised not to reveal personal details such as her real name, where she lived and went to school, and also that her videos didn't have footage that would accidentally release this information.

After a while, her mother noticed Aishwarya had lost her passion for making videos. She checked in on Aishwarya's Facebook account to find that strangers were leaving hateful and inappropriate comments on the videos.

Her mother explained to her daughter that the bullies were wrong for posting the messages. She sat with her daughter Aishwarya to review her privacy settings and made sure that the settings allowed only her Facebook friends to view her videos. After some research on the website, she found a new feature called "safe mode" that filtered offensive content, both from a user's session and permanently on an account. She set safe mode for Aishwarya's account, as well as on all the browsers on the home computer, in order to filter search content even if someone browsed Facebook without logging in.

Tips:

- Be careful about the information you post online, like if you put your photo or video or your account details Anirudh stay for a long time and who ever connected Anirudh see it.
- Remember don’t put anything personal like sensitive information about your family details, addresses, personal photographs.
- Most of the sites and services provide options for privacy settings and use them to prevent attackers to view your information. You can also set the privacy settings according to whom you want to allow seeing your information.

For More Refer:

http://www.dnaindia.com/bangalore/report-social-media-abetting-cyber-bullying-doctors-1953605

http://www.firstpost.com/world/monica-lewinsky-gives-public-speech-13-years-joins-twitter-1766401.html

http://zeenews.india.com/entertainment/red-hot/rihanna-accused-of-cyber-bullying-teen-fan_155130.html

http://zeenews.india.com/entertainment/and-more/how-to-handle-cyber-bullying-sexting_69299.html

http://zeenews.india.com/news/net-news/cyber-bullying-cases-put-heat-on-google-facebook_609727.html

PLAYING ONLINE GAMES RISKS ON SOCIAL NETWORKING SITES

Online games involve the technology risks to your computer system or system of gamers with whom you interact. If the software on the game server as been compromised, computers that connect to it also compromised. Exploited Vulnerabilities codes in games makes attackers to get into your system and read the files from a gamer computer, crash the games during online play in order to get the full control of the exploited computer.

ILLUSTRATION:

Anirudh had been a casual poker player since high school, but he had since lost touch with all his poker buddies. While surfing the Internet one night, he came across an online poker site and decided to give it a try. Soon he was playing nearly every night and winning good money. This went on for about a year, until a promotion at work led to long hours at the office. Anirudh never had time to play anymore, so he withdrew his money and closed his accounts.

A few weeks later though, Anirudh got a notice from his bank that his checking account was overdrawn. When he checked his account statement, there was thousands of dollars worth of purchases from websites for items he had never ordered. It turned out that somebody had stolen Anirudh's bank account details from one of the gambling sites he frequented. Even after clearing up those charges, Anirudh continued to have trouble. Credit card accounts had been opened in his name and left criminal, which seriously damaged his credit.

Tips:

- Always checked out the sites you are using to make sure they had good security practices in the form of SSL
- Use antivirus and antispyware programs
- Be cautious about opening files attached to email messages or instant messages.
- Configure your web browsers securely.
- Beware of clicking links, images and pop ups in the web sites as they may contain a virus and harm the computer.
- Never give personal information over the Internet while downloading games.
- Some free games may contain a virus, so be cautious and refer elders while downloading them.
- Create and use strong passwords
- Patch and update your application software

ONLINE IDENTITY:

An online identity is a social identity that network users establish in online communities. To protect their privacy, most Internet users prefer to identify themselves by means of pseudonyms. In some online contexts, including Internet forums, instant messaging, and massively multiplayer online games, an online identity might include an image called an avatar. As other users interact with an established online identity, it acquires a reputation, which enables them to decide whether the identity is worthy of trust.

ILLUSTRATION 1:

Ananth's family got a computer when he was 13 years old so that he could use it for homework. His parents installed monitoring software on the computer, so they felt safe letting Ananth keep the computer in his bedroom, and they were fine with him using it for other things besides homework. "I loved being online; I couldn't wait to get home from school every day so I could get on the computer," says Ananth.

However, when Ananth got his school progress report card several months later, his grades had gone down. Ananth's parents had also noticed a change in his mood; while he used to be a happy child, he was now irritable and tired most of the time. To find out what was going on, they looked at the monitoring software's log of how much time Ananth was spending on the Internet and what he was doing. It turned out that he was spending up to six hours a day - often late into the night - surfing the Web, instant messaging his friends, and playing online games.

Ananth's parents immediately took the computer out of his bedroom to the hall. He was no longer allowed to be online when they were not home, and they used a timer to gradually limit the time he spent online to one hour a day. Ananth's grades started to pick up since he was actually doing his homework, and he became much more pleasant to be around. I sometimes miss hanging out on the Internet all day," Ananth said, but it is good to have my old life back.

For More Refer:

http://www.hawaiinewsnow.com/story/6694946/teens-are-latest-victims-of-online-identity-theft

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-Internet-credentials.html?_r=0

ILLUSTRATION 2:

Eighteen months after moving in with his fiancée Mrs. Anita Rao received a collection letter about a past due credit card account that had been assigned to a collection agency. “I was confused,” said Mrs. Anita Rao, who always pays his bills on time. “I have only one credit card—an ABC Express card that I pay in full every month. The letter referred to a Visa card with a Rs 50,000 balance.”

Mrs. Anita Rao immediately called both the collection agency and the original creditor. After hours of detective work, Mrs. Anita Rao discovered that an identity thief forged a credit card application sent to Mrs. Anita Rao at his previous address. Mrs. Anita Rao explained the situation to the collection company as well as the Visa card representatives. Trouble was, the creditors had no way of knowing whether Mrs. Anita Rao was telling the truth.

Twelve months later, Mrs. Anita Rao still answers calls from creditors trying to collect the debt. Though Mrs. Anita Rao wants to buy a house, the collection account wreaked havoc on his credit score. He wonders whether he should keep fighting to have the collection account removed from his credit report; sometimes he thinks he should pay the entire Rs 50,000 bill and be done with it. Either way, he knows he must delay the purchase of a home for his new family because his credit score is too low to receive the best interest rates.

Tips:

- Always check credit & debit card statements thoroughly and regularly
- Always follows almost all of the rules of identity fraud prevention
- Always shreds important documents, never uses roadside mailboxes to send important information
- Never uses roadside mailboxes to send important information, and keeps his PIN number securely

Reference:

http://www.protectmyid.com/identity-theft-protection-resources/identity-recovery/one-victims-story.aspx

http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud

http://www.reviewjournal.com/news/22-year-old-guilty-racketeering-online-identity-theft-scheme

CHANSLASH - STORIES THAT FANS HAD WRITTEN AND POSTED ONLINE

Chanslash is a divide of fan fiction in which people write their own stories using characters from popular television shows, movies, and books. Chanslash is any such story that involves underage characters in a romantic pairing. While fan fiction can be a great creative outlet for children, a young Harry Potter fan could accidentally run across chanslash in her search for more stories about her favorite characters. While this can be disturbing for the child and the parent, most chanslash is clearly labeled as such and can thus be avoided.

ILLUSTRATION:

Anita is a working mother of two young girls. Her oldest, Sara, is 11 years old and a huge Harry Potter fan. After completing all of the school related homework and school books reading, she started reading stories that fans had written and posted online. Anita says, “I try to control her

Internet usage using parental control software, so for a while I checked all of the stories that she was reading. They were all pretty much like the books, so after a while when she told me she was reading Harry Potter stories I just let her read what she wanted."

Sara became more and more involved in the fan fiction community. She got to know some of the people who wrote stories, and they encouraged her to write her own tales. Her mother was thrilled. "I thought it was great. Instead of just reading, she was being creative and coming up with her own plots and story lines. It seemed that she had finally found her talent." Sara started sharing the stories with her friends, and one day Anita got a call from the mother of one of Sara's friends.

"This woman was very upset about a story Sara had written and given to her daughter," Anita recalls. "It involved a very 'adult' relationship between two of the novel's young characters. I couldn't believe what she had written. It even made me blush!" Anita asked Sara where she had come up with the ideas for her story. It turned out that Sara had stumbled onto a genre of fan fiction called chanslash, which depicts sexual relationships between popular characters. I have no problem with adults reading and writing this kind of material, but Sara is just a young girl. I should have been more involved; I should have checked all of the stories she was reading.

Tips:

- Monitor your child's Internet activity regularly
- Use popular tools like Parental control software to limit the Internet and content used while browsing
- Always use updated antispyware and antivirus program in your system
- Always run the antivirus scan once in a week

INSTANT MESSAGING – MALWARE

Chat rooms, forums and instant messaging are all great ways to communicate online, but when using them you have to watch out for the threat of malware. Malware short for "malicious software" is any software designed to harm your computer, such as viruses, worms, Trojan horses and rootkits.

ILLUSTRATION:

Every day after school, Swetha would talk to his friends online with instant messenger. His parents often checked his buddy list to make sure he only talked to people he knew in real life. They also set up the program so he could only download files from people in his buddy list. While they were chatting, Swetha and his friends would send each other links to cool Web sites, pictures from school events, and music files. Sometimes though, Swetha would get links that opened up blank pages, pictures that looked confused, or music files that wouldn't play.

When he asked his friends about it later, they didn't know what he was talking about. It turns out that Swetha's friends had never sent those links. The strange messages were actually coming from hackers who faked his friends' screen names, and the files and links were installing

malware on his machine. Eventually, there was so much malware on Swetha's computer that it slowed the machine, eventually Internet also and became unusable.

Tips:

- Always check and be careful while downloading any attachments or links from social networking sites.
- Always scan an attachment while you get through instant messaging or chatting
- Conduct regular anti-virus scans
- Only communicate with trusted sources
- Conduct manual malware removal scans
- Set your anti-virus package for "Real-time Protection
- Set your anti-virus package for the types of files you want it to check
- Set your anti-virus software to make scheduled automatic scans
- Disconnect from the network if you have any security concerns
- Always enable the system firewall and install root kit detection software

For More Refer:

http://tech.firstpost.com/news-analysis/malware-infects-yahoo-im-spreads-through-fake-browser-455.html

INCORRECT INFORMATION ON SOCIAL NETWORKING SITES

The Internet provides us with a wealth of information that we can access at any time. Unfortunately, mixed in with all that information is a lot of misinformation. Because anybody can publish on the Web, it is important to evaluate Web sites yourself to determine if the information they give is reliable, accurate, and unbiased. Filling any personal information may lead to loss of your money.

ILLUSTRATION:

Aruna after her retirement planned to visit every place she wanted to see in the form of some money and stocks left in her account. Aruna began looking for ways to increase her investments, and she began researching inexpensive stocks that might grow quickly. In her research, Aruna signed up for a few online newsletters claiming to offer the best stock advice, one of which talked a lot about new bio-tech companies on the cutting edge. Aruna put a thousand dollars in one of the stocks touted by the newsletter.

A few weeks later, she invested more money in a different company that the newsletter recommended. At first, the prices of her new stocks rose. But before Aruna thought to sell the stocks for profit, these prices fell significantly, leaving her with a little under half the money she had invested. Later, Aruna attended an investment workshop where she learned about pump-and-dump scams. She realized she had been a victim to this type of scam, where newsletter writers are paid to promote a stock, inflating its worth, for the profit of only a handful of dishonest investors.

Tips:

- Be cautious to research a new company before investing.
- Always Check the authority of the site
- Always check the accuracy and coverage of the site
- Check the objectivity of the site and information on the site is current
- Install Pre-Screened Web directories that have been evaluated and approved by subject-matter experts.

For More Refer:

http://timesofindia.indiatimes.com/tech/social/Indian-Army-has-a-new-challenge-Misinformation-on-social-media/articleshow/45469074.cms

ONLINE DATING SCAMS

Fake profiles of scammers posing as attractive men and women, and then claiming they need money to help in an emergency, typically when they claim to be out of the country on a business trip. If you are active on online dating websites, or via classifieds, chat rooms and forums, beware. Some reports indicate that as much as 30% of the personalities are scams. That beautiful woman or handsome guy may be in love with your wallet or purse, not you.

ILLUSTRATION 1:

Sheena met a guy on a dating site. We chatted for a while. He claimed to be fairly wealthy don't know what business he was in because. I believed he was just better and larger. Well. Because it was the holiday weekend. He said he was going to add me to his corporate account. And to call a number so they could set me up for him to be able to transfer money directly from his account to me. He said he was in Delhi. For the weekend. So he wanted me to take the money he sent me and get a plane ticket and come sending me. But the minimum amount the could send would be Rs 50000 as per the bank norms.

So when I called the number. The lady said for me to get a money Pak card for 5000 rupees. And call her back and give her the number. For security damage they can't load money on a card with a zero balance and there had to be 10000 for every 100000 rupees trying to be loaded. That did not make sense because I know if I purchase money Pak whoever I give the confirmation number to can remove the money and load it onto a card themselves. So I Google searched the number. And it came to be a virtual assistant number I was dialing.

When I called the 877 number back to ask more questions. The operator. Got very upset at my questions. About it not making sense to me and noticed it was the same person I had talked to before even though she gave a different name. When I questioned him. He got very belligerent. All I have are the two phone numbers. But. I know these two are probably scamming all over the Internet.

ILLUSTRATION 2:

Rimy have been chatting to a man who contacted me from the website www.isingles.I believed he was an American living in England. He then said he was away on business in West Africa. We have been chatting for several weeks and he was very believable. However, when he said he was returning to the India he said he had run out of cash and could I send him some, asking initially for Rs 50,000 and when I said no asked how much could I send. I led him to believe that I would send 5000 and these are the details that he gave me:

Western Union Money Transfer

Agent name - Olusesan Ashaye

City - Ikorodu

State - Lagos

Country - Nigeria

Zipcode - 23401

Text question - best color

Answer - blue

His email address is littleman4075@yahoo.com

ILLUSTRATION 3:

Recently Anand joined a dating site by the name of xyz@test.com, it cost me in total Rs 850 to join and there is a fixed fee of Rs 350 a month. I have recently discovered that many of the profiles with pictures on them are taken from other sites on the net and not just dating sites. Also when I tried to communicate with someone I always got a one line answer, almost as if it was automatic. This aroused my worries and I investigated the matter and found many complaints of hard done by consumers who were doped by this scam, People were saying that they never met anyone and that there was always some excuse, one person even said that he had a lot of difficulty cancelling his account, so to avoid this problem I changed my credit card PIN number.

Now, I just want to highlight this in the hope something can be done about it, the company is based in Belgium, well that's what they promote, and I believe they have a team of people who are pretending to be the person that is in the profile, responding to emails from unsuspecting customers, keeping them on a string as to extract money from them, It even says that when you cancel the account the membership will terminate immediately even if you have paid until a certain time that has yet to expire.

TIPS:

- Never send money to someone you met online
- Let friends or relatives know where you are going and when you expect to return when you meet someone from a dating website.
- Especially, never, ever send money via Western Union

Reference:

http://www.consumerfraudreporting.org/datingscams.php

ILLUSTRATION 4:

Amrita had been married for 25 years when her husband suddenly died of a heart attack. After several years her children started pushing her to date again, but she didn't know where to meet any single older men in the small town she lived in. Her daughter eventually suggested she try one of the many online dating sites on the Internet. Amrita was skeptical, but she decided she had nothing to lose by trying it out.

Amrita posted a profile and soon received emails from several men who all seemed very nice. One fellow in particular, Sharma, always said just the right thing in his emails. He was smart, romantic, charming, and, judging from his picture, quite handsome. He finally persuaded her to come visit him where he lived, in a city 600 miles away.

A few months later Amrita was waiting at the airport for Sharma to pick her up. It took her a while to recognize him, since he appeared to weigh about 50 pounds more than he had in his photo and had half as much hair. Amrita was willing to forgive this, though, since he seemed like such a nice guy. But then Sharma told Amrita that he had to drop her off at her hotel and meet her later his wife was expecting him at home.

CHATTING WITH STARANGERS IN FACEBOOK

Chat rooms are the place where people who want to have online conversations can get together electronically and broadcast messages to everybody in real time. By giving out personal information, you increase your chances of falling victim to identity theft. It is highly recommended that you keep this information private, or at least only for trusted friends to view. Most social networking sites allow you to control who can view what on your profile page. Your friend may have malware running on his machine.

These messages contain links and are sent automatically without your friend's knowledge. Just by clicking on them, worms or viruses can load on your machine. Before clicking, verify with your friend if he really sent it.

ILLUSTRATION:

When Sreedhar was in high school, he used instant messaging all the time to talk to his friends. Sreedhar was a friendly kid, and occasionally he would even IM with people he didn't know if

they started a conversation with him. Whenever Sreedhar had to go out, he would leave his cell phone number in his IM away message so his friends could get in touch with him.

One day Sreedhar got an IM from somebody who claimed to be a kid from his school. They talked for a little while, but the other kid started asking a lot of questions that made Sreedhar uncomfortable. Sreedhar closed the conversation and the other kid never tried to IM him again. But a couple of days later, Sreedhar got a disturbing phone call on his cell phone. The number on the call was blocked so he couldn't find out where it was coming from. However, he knew the person must have gotten his number from his IM away message since he only ever gave his number out to friends and family.

The strange calls kept coming, until Sreedhar finally had to change his cell phone number. He changed his Facebook account away message too so that it didn't give out any information about him, and he removed any personal information from his Facebook profile.

TIPS:

- Never reveal your personal information to online strangers in any of the social networking sites.
- Always avoid opening links and attachment through social networking sites
- Always enable Antivirus program in your machine for more security
- Always enable your system firewall for secure and filtered communications from outside world

BLOGGING IN FACEBOOK:

Blogs are report in popularity among both adults and kids. While blogging used to be limited to a technologically-savvy few, there are now many sites that allow you to set up a blog with only a few clicks of the mouse. Many give out personal information about themselves - where they go to school, phone numbers, addresses, where they hang out. Some even post pictures of themselves at their office desks on their blogs. While there have been no reported instances of predators finding victims on blogs, the potential is certainly there, and kids need to be careful about what information they give out.

ILLUSTRATION:

Ayushman majored in creative writing in college, but after graduation he found himself working for an insurance company, and he didn't have much time for writing anymore. He decided to start a blog as a way to flex his writing muscles again and keep in touch with friends and family. He was pretty open about his life and wrote about all the stuff that happened to him at work, at the gym, or while out on the town. When he got a cell phone that took pictures, he started posting photos to go with his blog posts.

One day Ayushman was called into his boss' office at work. His boss pulled Ayushman's blog up on his computer and showed him posts that included pictures of the company's facilities and

employees. He reminded Ayushman that this was a violation of company rules and suggested that he start looking for work elsewhere.

MY COMPUTER WAS HACKED THROUGH SOCIAL NETWORKING:

A keylogger is a tool that captures and records a user's keystrokes. It can record instant messages, email, passwords and any other information you type at any time using your keyboard. Keyloggers can be hardware or software.

One common example of keylogging hardware is a small, battery-sized device that connects between the keyboard and the computer. Since the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device in plain sight. As the user a type, the device collects each keystroke and saves it as text in its own miniature hard drive.

A software keylogger can be downloaded and installed as a program running in the background. Software keyloggers may also be embedded in spyware, allowing your information to be transmitted to an unknown third party over the Internet.

ILLUSTRATION:

Swathi regularly used popular social networking sites, and she considered herself a careful user. However, one day she received a message at work from her friend Anita with a link to view pictures from his recent vacation. Swathi didn't recognize the linked website, but she wanted to see Anita's photos, so she clicked the link. When a new page didn't open, Swathi Sharma replied to Anita saying his link was broken, but he never responded.

Several weeks later, Swathi Sharma was called into her boss's office at work. Inside, her company's IT technician told her he had investigated an increase in the company's network traffic, and he had found that a hacker was receiving hourly reports of Swathi Sharma's keyboard activity.

When Swathi had clicked the link in Anita's message, a type of malware called a keylogger had been installed on her company computer. Through the keylogger, the hacker learned Swathi logon to the company's network, which he used to access confidential information. Additionally, the hacker broke into Swathi social networking account and sent malicious messages to her friends, just like the message from Anita.

Fortunately, Swathi Company caught the hacker before any lasting damage occurred, but Swathi almost lost her job. She changed all of her Internet account information, and she is now much more careful when using social networking sites.

TIPS:

- Never click the links received in the social networking sites, instead type the same URL in the browser
- Always enable the desktop firewall and allow only selected services or port

- Always enable the Antivirus program and update the same for every two days
- Always keep the operating system patches with the latest security database

MY PHOTO WAS SPREAD AROUND THE INTERNET:

Webcams pose a serious risk to children because they provide a visual link with online predators. Predators scan webcam sites to find children and teenagers with webcams and then try to convince the children to expose themselves. Webcams are being used on social networks sites in dangerous ways. At worst they can connect children to sexual predators and child molesters. It lets teenager's video chat with random strangers all over the globe, which is a very scary prospect.

ILLUSTRATION 1:

When Anupama was 15 her mother got a new job, and she and her family moved to a new city all the way across the India. Anupama was lonely in her new school, so her parents bought her a webcam so she could send video messages to her friends back home. Every day after school, Anupama would get on the computer and talk to her friends online, especially her friend from her old school. On her friend's birthday, she even surprised him with some strange video she had taken of herself.

Months later, Anupama was settling into life at her new school. She had made a lot of new friends. When she told her old friend about this, he got upset, but she figured he would get over it in time. One day, though, Anupama received an email from her old friend that contained a link to a website. She went to the website and saw her pictures and videos splashed all over it, with comments from all the people who had visited the site and seen the videos. Soon some kids at her school saw the video on another website, and she became the laughing store of the school.

ILLUSTRATION 2:

Ishanth was a shy, quiet 15 year old who didn't get along very well with the kids at his school. However, he did have many online friends whom he chatted with regularly. Some of Ishanth's online friends had webcams, and Ishanth eventually got a webcam of his own to help him meet new people. Setting up the webcam was easy - all he had to do was plug it in, install the software, and post his picture and contact information on an online directory of webcam users. Soon he started hearing from all sorts of people, although none of them were the teenagers he had hoped to meet.

One day Ishanth got an email from somebody who said he would pay Ishanth Rs 5000 to take off his shirt on camera. Ishanth had been looking to upgrade the video card on his computer, so he was tempted. Figuring that he already took his shirt off in public whenever he went swimming, Ishanth agreed to do what the man asked. The man told Ishanth how to set up a PayPal account to receive the money, and indeed, Rs 5000 showed up in Ishanth's account when he took off his shirt on camera.

Soon more requests were coming in to Ishanth's email, and not just from the first man who had contacted him. Men were offering large amounts of money for Ishanth to expose himself on camera, and each request asked Ishanth to go just a little bit farther than before. Ishanth was making lots of money, but he wasn't feeling very good about himself, and some of the people who were contacting him scared him. Eventually, Ishanth unplugged his webcam and changed his email address. "It all seemed so innocent at first," says Ishanth, "but after a while I was doing things I was really uncomfortable with. Unfortunately, all those pictures are still out there on the Internet."

TIPS:

- If you have a computer with a webcam, keep it in a common room, not in a child's bedroom.
- Teach your children to use webcams only to communicate with people they know
- Make sure children understand that what they do on a webcam is not necessarily private. Teach them to never do anything in front of a webcam that they wouldn't want the entire world to see.
- Don't post your webcam URL on the Web
- Teach children about the dangers of posting personal information and pictures online.
- Teach children to not respond to instant messages or emails from strangers

AGE-INAPPROPRIATE CONTENT RISKS:

There are the risks of your child accessing inappropriate information. This includes access to information that may be inappropriate for children generally, sites that sell contraband or advocate illegal activities, and sites that pose risks to their privacy. There are also sites which show graphic and inappropriate pornography and sexual content which our children can easily access. And there are sites with tobacco and alcohol advertisements, bomb-building sites, sites that advocate taking drugs, as well as sites that contain violence and gore, misinformation, and hate literature.

ILLUSTRATION:

When Rahul turned eleven years old, his parents decided that he was old enough to use their computer to get on the Internet. Rahul had a lot of fun surfing the Net, playing games, and chatting with his friends. But one day Rahul came across a Web site that really disturbed him. On it, there were violent pictures and instructions for building bombs. He switched to another site right away, but he couldn't forget what he had seen.

Rahul thought maybe he had done something wrong and he didn't want to lose his right to use the computer, so he didn't tell his parents about what he had found. But soon he started having awful nightmares and eventually he asked his parents about the pictures he had seen.

Rahul's parents were horrified that their son had found these things online, but they knew there was a lot of good content on the Internet that he should still have access to. To protect Rahul they installed filtering software that only let him visit approved sites that had no adult

content. They also made sure that Rahul understood he could talk to them about anything he saw online.

TIPS:

- Set up a content filter tool through the browser to block inappropriate sites
- Kid-safe search engines and Internet Filters
- All-in-one parental control software

SPAMMERS TOOK MY MONEY

E-commerce (also called e-business) is just another term for conducting business over the Internet. However, you can run into some dangers. Online advertisements in the form of banner ads and pop-up ads commonly appear while you access e-commerce sites. These advertisements can lead users to untrustworthy Web sites and install cookies and spyware on computers. It is best to just ignore online advertisements and do not click on them.

ILLUSTRATION:

At the age of 40, Kapil Sharma found he newly divorced and back on the dating scene. After a few rejections from younger women, Kapil Sharma became convinced that his receding hairline was to blame. Thinking that he might have more luck with the ladies if he had a full head of hair, Kapil Sharma investigated hair replacement options. Unfortunately, hair growth drugs were expensive, and between alimony payments and child support he didn't have the money to spare.

Then Kapil Sharma found an email in his inbox claiming he could buy the latest hair growth drugs for much less than what they cost at the pharmacy. Figuring he had nothing to lose except some more hair down the drain, Kapil Sharma went to the advertised Web site, ordered a six-month supply, and waited for his drugs to arrive.

He was in for a long wait. After four months had gone by and he still hadn't received his pills. I've tried getting my money back, but the company is based in a foreign country, and I have no way to track them down. Their Web site isn't even up anymore.

TIPS:

- I should have checked out the site more and made sure it was a legitimate company.
- Always check the genuineity of the website form where you are buying the product
- Always check for the Secure Socket layer padlock at the top and bottom most layer of the website

NEVER REVEAL TOO MUCH INFORMATION ABOUT YOU ON SOCIAL NETWORKING SITES

Chat rooms are online forums where people who want to have online conversations can get together electronically and broadcast messages to everybody in real time. By giving out personal information, you increase your chances of falling victim to identity theft. It is highly

recommended that you keep this information private, or at least only for trusted friends to view. Most social networking sites allow you to control who can view what on your profile page.

ILLUSTRATION:

A respected doctor, Anadh held a stressful job at a large hospital, so when time allowed for vacation, he and his wife Sumitra splurged on lengthy Indian trips. When they became comfortable with the Web, finding plane tickets and investigative worthwhile destinations only got easier. One travel Web site, in particular, provided excellent information, as well as a large forum where hundreds of travelers posted questions and comments and discussed travel with each other online.

Before taking a long trip to Kashmir, Anadh visited their favorite travel Web site for information. As usual, Anadh worked out many details of their trip using recommendations from the Web site's forum. While planning this trip, he was pleasantly surprised to meet and trade information with a Web site visitor who went by the name PlaceFan. PlaceFan was especially polite and helpful, and Anadh was amazed to learn that he and the man were from the same local area. In addition to sharing information about London, they chatted about other local interests they shared. Later that month, Anadh and Sumitra enjoyed another trip overseas.

The couple's homecoming, however, was far from restful. While they were gone, someone broke into their home. Their new television set, stereo, jewelry and other valuable items were gone. A police investigation couldn't find the culprits, but it revealed that the burglars pulled a moving truck up to the house in broad daylight and helped themselves to the couple's belongings. Police concluded that information available about Anadh online had helped the culprits to plan the perfect robbery.

TIPS:

- Never reveal your personal information to online strangers in any of the social networking sites.
- Always avoid opening links and attachment through social networking sites
- Always enable Antivirus program in your machine for more security
- Always enable your system firewall for secure and filtered communications from outside world

6.4. DO SOCIAL NETWORKING SITES IMPROVE YOUR ABILITY TO NETWORK IN REAL LIFE?

Every teacher should understand firstly how both our online and offline social networks benefit us; it helps to understand the meaning of social capital. We all know what our physical capital is. It's the measure of our belongings and our money -- our stuff. Social capital, on the other hand, is the measure of our connections with others, suppose school children’s with the strangers -- our networks.

The main concept of social capital is that social networks are valuable. Having a social network provides you with benefits like trust, cooperation and information. Your social capital, then, is the collective value of the social networks with which you are connected. For example, when your neighbors are out of town, do you keep an eye on their house just to make sure everything's OK? That's social capital -- your network of neighbors looking out for each other. Have you ever gone to an Internet board in search of a support group? That's social capital in action.

However, research shows that the social capital of communities has declined considerably over the past few decades. Experts attribute it to metropolitan city spread out. People don't all live in close proximity to each other anymore. They also blame television, busier lives and, sadly, a decline in our overall trust in each other.

Some people may also blame the decline of community social capital on the popularity of the Internet. However, the Internet actually helps to build social capital -- just in different ways. Studies show that the Internet doesn't conflict with people's connection to the community. The Web actually helps people to maintain active contact within their network because they're not limited to geographically-restricted face-to-face interactions.

PROFESSIONAL NETWORKING

Teachers should learn their students about the today's job market; social networking sites offer users with outer limits with the domain knowledge expertise. The site LinkedIn targets the professional, white-collar employee. As you create a profile, the site suggests possible contacts -- people you may have known in previous jobs or through college and university. You can search for specific people, research companies you'd like to work for and reach out to the right people without having to navigate through a telephone network.

Teachers also should teach their student how a LinkedIn even lets you write recommendations for people you know, and allows them to return the favor. There's an old adage that states, "It's not what you know; it's who you know," and social networking sites prove that to be true. Social networking and the job market is such a great match that some colleges even offer seminars on how to network online for the various technical study materials.

*6.*5. GUIDELINES TO AVOID RISKS BY SOCIAL NETWORKING

- Be careful about the information you post online , like if you put your photo or video or your account details will stay for a long time and whoever connected will see it.
- Generally, business people will see as part of hiring process to know about everyone views and interests. However hackers will use these sites to collect the personal information and may misuse them.
- Remember don’t put anything personal like sensitive information about your family details, addresses, personal photographs.
- Most of the sites and services provide options for privacy settings and use them to prevent attackers to view your information. You can also set the privacy settings according to whom you want to allow seeing your information.

- Be careful if you want to meet social networking friends in person, it may not be true identity posted on a web site. Think before you meet. If you are going to meet then do it in a public place during the day.

- In real life, you may follow some rules for interacting with people. The same should be applying for Internet. Convey the message to all known people, how Cyber Bullying can be harm and causes pain in the real world as well as in the cyber world.

- The observations or monitoring online activity can be done informally by participation and supervision of your child online experience.
- You may also monitor formally with software tools and use discretion when covertly spying on your kids. This may cause more damage than good if your child feels privacy and may go completely underground.
- Always frame rules for Internet accessing and share the information how cyber bullying can affect the family and educate Internet based behavior, and etiquette.
- Moreover teach and reinforce moral values about how others should be treated with respect and dignity.
- Use Parental Control Bars, Desktop Firewalls, Browser Filters to avoid or preventing children from cyber bullying other or accessing inappropriate content.
- You may request school authorities to teach or guide students about how to prevent and respond to online peer harassment, interact wisely through social networking sites and responsible online users.
- Specify clear rules, Guidelines and policies regarding the use of the Internet, Computers and Other Devices such as USB, CDROM at School for Cyber Bullying.
- Teach students that all types of bullying are unacceptable and the behaviors' are subject to discipline.
- Teachers need to mentor or establishment mentorship with senior students to guide information security awareness and monitoring through peer students.
- Use Desktop Firewalls, Browser Filters to avoid or preventing children from cyber bullying other or accessing inappropriate content. In addition use monitoring with software tools for students online activity.
- Educate students by conducting various workshops from an internal or external expert to discuss related issues in cyber bullying, good online behavior and other information security issues. Moreover keeping related posters in school.

Chapter 7:
Social Engineering Security

7. SOCIAL ENIGNEERING SECURITY

7.0. INTRODUCTION

Typically, many organizations have information that has value that justifies expensive protection mechanisms. Critical information may include patient records, corporate financial data, electronic funds transfers, access to financial assets, and personal information about clients or employees. The compromise of critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and the collapse of the organization. To respond to the threats, organizations implement Information Security Plans to establish control of information assets.

Information Security Plans specify protection mechanisms for organizational information. There is usually a heavy reliance upon technical security mechanisms, such as firewalls, user passwords, closed networks, and operating system protection mechanisms. There appears to be a belief within the computer and information security profession that everyone understands the Operational Security requirements for protecting information.

The disclosure of information through non-technical means can and will occur. This type of disclosure can bypass millions of dollars of technical protection mechanisms. In many cases, if an impending attacker wants to gain access to a computer system, all they have to do is ask for it. Users have disclosed a variety of sensitive information, including the names of employees, organizational costing information, telephone numbers to organizational modems, and customer data. Surprisingly, user identifiers and passwords are extremely easy to obtain.

7.1. WHAT IS SOCIAL ENGINEERING?

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Some emails entice the recipient into opening an attachment that activates a virus or malicious program in to your computer.

- Careless talking is one of the reasons for social engineering
- Careless talking about business, the office, home, personal and the people and discussing with those who not authorized to talk
- Carelessly giving the sensitive information indirectly to someone who may use it for a specific reason such as breaking into your computer, your organization details etc

7.2. WHY SOCIAL ENGINEERING?

Social Engineering uses human mistake or weakness to get access to any organization in spite of the layers of defensive security controls that may have been implemented. A hacker may have to spend a lot of time & effort in breaking an access control system, but he or she will find it much easier in persuading a person to allow entry to a secure area or even to disclose confidential information.

In spite of the automation of machines and networks today, there is no computer system in the world that is not dependent on human operators at one point in time or another. Human interfaces will always be there to provide information and perform maintenance of the system.

7.3. HOW DO THEY DO THIS?

- A Social Engineer may approach you either a telephone or e-mail and pose as a person from your Information Technology Department or Help Desk and may ask for user id, password and other details like systems and network information.
- A Social Engineer may meet you outside of your work place or organization and may ask you about your work or how your organization does the things.
- A Social Engineer may come to your organization to present business needs and may ask for network connectivity to know about network information or any sensitive information.
- A Social engineer may ask your identity card to know about your personal information about your School, organization etc.
- The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information to commit fraud, network intrusion, identity theft or simply disrupt the system and network.

7.4. SOCIAL ENGINEERING CAN BE DONE IN MANY WAYS:

Public Places

Social Engineering can be done through public places like cafes, pubs, movie theatres. You may release or give some sensitive information to the public or a social engineer or someone may overhear you.

Gossips:

You may talk about some gossip with colleague and may give some information to other colleague who might be a social engineer.

Personal Pride or Confidence:

You may give sensitive information of your family or organization to boast your achievements, pride, and confidence to unknown persons.

Online:

Social engineers may obtain information on-line by pretending to be the Network Administrator, sending e-mail through the network and asking for a user's password or any sensitive information indirectly.

Vishing:

It is one of the methods of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.

The term is a combination of "voice" and phishing. Don't give any financial information to unknown people over phone, confirm to whom you are speaking and cross check with the Concern Company or bank before giving any information.

Phishing:

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data and or other information. The attackers have become more sophisticated and also their phishing e-mail messages and pop-up windows. They often include official looking logos from real organizations and other identifying information taken directly from legitimate Web sites.

If you think you've received a phishing email message, do not respond to it. And don't even click on the links you received from the unknown users.

Instant messaging/Internet Relay Chat:

Users are intended for to sites that claim to offer help or more information but are actually intended to place Trojan horse programs on their computers which the hackers afterward use to gain access to their

computers and the networks to which they are connected.

E-mail attachments:

Programs can be hidden in email attachments that can spread viruses or cause damage to computer networks. This includes malicious software such as viruses, worms and Trojan horses. In order to attract users to open the attachments, they are given names that raise curiosity and interest.

Email scams:

Email scams are becoming more common. One recent example claims that you have won a trip to the Bahamas and requests "basic information" from the user so that the prize can be awarded.

At first they request quite harmless information such as name, address and phone number; however, in a succeeding email, credit card information is requested in order to hold your spot on the "free" trip.

Chain Letters and Hoaxes:

These trouble emails rely on Social Engineering to continue their spread. While they do not typically cause any physical damage or loss of information, they cause a loss of productivity and also use an organization's valuable network resources.

Websites:

A common trick is to offer something free or a chance to win prizes on a Website. To win the user must enter a valid email address and a password. Many employees will enter the same password that they use at work, so the Social Engineer now has a valid user name and password to enter an organization's network.

Use User Authentication:

In this type of attack, attacker gain physical access by pretending to be a employee etc means in this type of attacker use others identity to gain access the system and then gathers the information.

Posing as an Important User:

In this type of attack, the hacker pretends to be an important user such as an executive or high-level manager who needs immediate assistance to gain access to a computer system or files.

The hacker uses intimidation so that a lower-level employee such as a help-desk worker will assist them in gaining access to the system. Most low-level employees won't question someone who appears to be in a position of authority.

Using a third person:

Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or can't be contacted for verification.

Calling technical support:

Calling tech support for assistance is a classic social-engineering technique. Help-desk and technical support personnel are trained to help users, which makes them good pray for social-engineering attacks.

Shoulder Surfing:

Shoulder Surfing is very most popular techniques, in this technique we gather passwords by watching over a person's shoulder while they log in to the system. The watch valid user login and then use that password to gain access to the system.

Impersonation

It is one of the most common social engineering techniques and it takes many forms. Impersonation can occur in person, over the phone or on-line.

Ex: The overly helpful help desk, Third-party Authorization, Tech Support.

7.5 OTHER TECHNIQUES:

Baiting

It is one of the methods of social engineering which uses physical media and relies on the curiosity or greed of the victim.

Here the attacker leaves the malware inserted or infected USB or pen Drive, CD/DVD ROM in a location that to be found and gives a legitimate looking and makes victim curiosity and waits for them to use the device.

Don't get tempted in accessing the devices which left unattended or found at sidewalk, elevator, parking lot etc.

Persuasion:

Influence someone to give you confidential information either by convincing them you are someone who can be trusted or by just asking for it. Be suspicious don't get influenced by the unknown person and don't give away the confidential information to them.

Dumpster diving:

Dumpster diving, also known as trashing is another popular method of Social Engineering. A huge amount of information can be collected through company dumpsters or wastage from home.

Don't dump any confidential papers into trash, before dumping make sure you don't have any important information in it.

Hoaxing:

A Hoax is an attempt to trap people into believing that something false is real. This is usually aimed at a single victim and is made for illicit financial or material gain a hoax is often perpetrated as a practical joke, to cause embarrassment. Beware don't believe the e-mails received from unknown and don't ever give the financial information.

Pretexting:

Pretexting is the act of creating and using an imaginary scenario to engage a targeted victim in a manner that increases the chance the victim will reveal information or do actions that would be unlikely in ordinary circumstances. It is more than a simple lie.

Be cautious because strangers try to fool you by creating false situation and make you to believe in order to collect the confidential information.

7.6 CASE STUDIES:

Case Study 1:

Mr. Rahul: Hello?

Caller: Hello, Mr. Rahul. This is Rohan in tech support. Due to some disk space constraints, we're going to be moving some user's home directories to another disk at 8:00 this evening. Your account will be part of this move, and will be unavailable temporarily.

Mr. Rahul: Uh, okay. I'll be home by then, anyway.

Caller: Good. Be sure to log off before you leave. I just need to check a couple of things. What was your username again, Rahul?

Mr. Rahul: Yes. It's Rahul. None of my files will be lost in the move, will they?

Caller: No sir. But I'll check your account just to make sure. What was the password on that account, so I can get in to check your files?

Mr. Rahul: My password is Tuesday, in lower case letters.

Caller: Okay, Mr. Rahul, thank you for your help. I'll make sure to check your account and verify all the files are there.

Mr. Rahul: Thank you. Bye

Case Study 2:

Three weeks ago **XYZ Middle School** was hacked. The computer hacker posed as a system administrator for the central corporation and called an administrative assistant in the principal's office. The conversation went something like this:

Hacker: "Hi, this is Shyam with tech support. We have had some individuals in your office report slowdowns in logging in lately. Is this true?"

Clerk: "Yes, it has seemed slow lately."

Hacker: "Well, we have moved you to a new server, so your service should be much better. If you want to give me your password, I can check your service. Things should be better for you now."

Unfortunately, Shyam did not really work in the central office at XYZ Middle School. Shyam hacked into the school's system; from there he found the financial system. Within one week, over 30 per cent of the teachers reported that their bank accounts had been stolen and used.

Case Study 3: Using Names

"Hello, can I speak with Yash from R&D please?" "I'm sorry; he'll be on vacation until next Monday" "OK, who's in charge until he gets back?" "Deepak Kumar" So we speak to Deepak Kumar instead. A hacker, however, can leverage this information when contacting R&D later. After some small talk with an R&D employee, the hacker claims:

"By the way Michael, just before Yash went on vacation, he asked me to review the new design. I talked with Deepak Kumar and he said you should just fax/mail/send it to me. My number is 123-1234. Could you do it as soon as possible? Thanks."

Case Study 4: Vendor Impersonation

Hi, I'm calling from Applied Technology Corporation. We have a special offer on routers. Could you tell me if you're satisfied with the hardware you're using at the moment?"

During an afterhours Internet chat session, you are asked for a picture of yourself. Although you don't have one available, you are obligingly asked if you would like one of the other parties. After a bit of additional encouragement, the other party sends an attachment that, in all respects, resembled a JPEG file. Upon accessing the attachment the hard drive starts spinning, and of course, there is no photo.

Understand the danger of a Trojan horse being enclosed, and immediately alert the IT department. The Internet connection needs to be closed down and checked. Eventually, the computer could be reinstalled and rolled back to the day before with a backup tape, (losing a full day of production and possible additional days overall).

Case Study 5: Online Fraud

The director of a small Scottish company received a call from a man purporting to be from his bank advising him that there were some suspicious transactions on the company bank account. The man (hereafter "fraudster") purporting to be from the bank was able to describe recent authorized transactions which made the director think it was a genuine employee of the bank's fraud team.

The director was asked for his log-in details for the online bank account and the PIN which the fraudster said he required to access the account and take any action should the transactions be fraudulent. Once the details had been provided to the fraudster, he advised the director he would call back later to confirm everything had been resolved.

Later that evening the director checked his bank account and saw that several large transactions had been made. He called his bank who advised that nobody had called from the fraud team earlier and that he had probably been the victim of a scam. The bank investigated and advised the director a few weeks later that due to the director's gross negligence they would not refund the money lost to the fraudster.

Case Study 6: Enthusiasm Of Fun

As for this attack, first we gather information like we used the person whom we know. We gathered the information like he uses the Operating system as Linux; He is fond of Linux shell script programming. Second stage is relationship development which is already established as we choose person who trust us. We sent it to friend who uses Linux as desktop operating system in mail. Subject line of the mail was "Shell Script for Fun". As frequently you got mail from your friend having attachment, you open it as it pretend to be from friend and safe.

You get trapped because even you can send mail with any fake name using open mail relay SMTP servers. This is psychological strategy and it is customized attack, as we have chosen the individual. Some parasite writers use customize approach for some specific victim while some uses general approach to trap unknown victims and if that technique get successful then many people will get trap in it.

Case Study 7: Eagerness To Know Great Thing

Second case we gone for same principal first information gathering, relation establishment and then deception. We choose persons who are fond of hacking and cracking activity. It targets such user who loves hacking and cracking. Even on Internet, if you search for free tools for hacking and cracking, you will get it for free.

But many of such software itself hack your system. On Internet: I have put link of this shell script with Name “Tool to hack in Windows” to friend. And they clicked on it, downloaded it and ran it.

Case Study 8: Hoaxing

As people think, Linux is secure than windows but don’t know by what percentage and they want information on this aspect. So fake Linux report containing the Shell Script as the case. As a news to friend – Linux security report. As people normally follows the link as it is report on Linux. As all this techniques uses social engineering, human get trapped. Our spyware requires the root privileged.

7.7. HOW DO YOU AVOID BEING A VICTIM?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. Take advantage of any anti-phishing features offered by your email client and web browser.
- A well-documented and open Security Policy, connected with standards and guidelines and acceptable usage policy for business usage of email, computer systems, telephone, network etc.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. Information classification and handling for identifying critical information assets and related handling instructions.

- Personnel security – screening prospective employees, contractors to ensure that they do not pose a security threat to the organization, if employed.
- Physical security – to secure the facility from unauthorized physical access with the help of sign in procedures, electronic and biometric security devices etc.
- Information access control – password usage and guidelines for generating secure passwords, access authorization and accountability procedures, securing remote access via modems etc.
- Automated password reset and synchronization tools can raise the responsibility of managing passwords from tech support and the help desk.
- Information security awareness training – to ensure that employees are kept informed of threats and counter measures and their responsibilities in securing company's assets

7.8. WHAT DO YOU DO IF YOU THINK YOU ARE A VICTIM?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft.
- If you feel you have been victimized by an attempt at social engineering, report the incident to your manager and to security personnel immediately.

7.9. CONCLUSION

Even the best technical mechanisms could not have prevented the attack. Only the use of one-time password mechanisms could have minimized the effects of the Social Engineering attacks. The attackers exploited poor security awareness, from both an information and operational security perspective. Even if the attackers were unable to "obtain" computer passwords, they successfully obtained sensitive personal and company information.

A Social Engineering attack reveals vulnerabilities in security policies and awareness that cannot be detected through other means. In general, Social Engineering attacks will uncover similar problems in many organizations. However, each attack will yield problems that are specific to the organization being examined. It is for this reason that every threat assessment should include a thorough Social Engineering effort performed by qualified and trusted individuals.

Chapter 8:

Malicious Applications

8. MALICIOUS APPLICATIONS

8.0. MALWARE:

Malware is short known for malicious software. It is software designed to infiltrate a computer system without the owner's informed consent. Malware includes computer viruses, worms, Trojan horses, rootkits, spyware, dishonest adware, crime ware and other malicious and unwanted software. Around 80% of malware today is designed to find and steal confidential information stored on your computer. This type of malware is sometimes called “crime ware. Malware can invade your machine through infected email attachments, “bots” that crawl the Internet looking for unprotected computers, and visits to “hostile” Web sites.

8.1. FORMS OF MALWARE:

Malware has become the utmost external threat to most hosts, causing damage and requiring extensive recovery efforts within most organizations. The following are the typical categories of malware:

8.1.1 Viruses: A computer virus is a program which is able to replicate and attach itself to a program or files infecting the system without our knowledge. The software programs that hide on your computer and cause mischief or damage. Viruses can be divided into the following two subcategories:

8.1.1.a Compiled Viruses: A compiled virus is executed by an operating system. Types of compiled viruses include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media; and multipartite viruses, which combine the characteristics of file infector and boot sector viruses.

8.1.1.b Interpreted Viruses. Interpreted viruses are executed by an application. Within this subcategory, macro viruses take advantage of the capabilities of applications’ macro programming language to infect application documents and document templates, while scripting viruses infect scripts that are understood by scripting languages processed by services on the OS.

8.1.2 Sign of Viruses:

- Computer runs more slowly than normal
- Computer stops responding or locks up often
- Computer crashes and restarts every few minutes
- Computer restarts on its own and then fails to run normally
- Applications on your computer don't work correctly
- Disks or disk drives are inaccessible
- Can't print correctly
- See unusual error messages
- See distorted menus and dialog boxes

8.1.2 Spyware

Spyware is a generic term for malicious software which ends up on your computer, and is used to gather information about you and other files on your computer and passes it over Internet to others. Generally speaking, spyware is software that hides on your computer, tracks what you're doing online, and then sends that information over the Internet. Some types of spyware, called "keystroke loggers" actually record and send everything you type on your computer. Spyware software can sneak onto your computer when you download unsafe software and files—or even visit a hostile Web page. One major source of spyware is the peer-to-peer file sharing software commonly used to share music and videos online.

8.1.3 Worms:

A worm is a self-replicating, self-contained program that usually executes itself without user intervention. Worms are divided into two categories:

– **Network Service Worms**. A network service worm takes advantage of vulnerability in a network service to propagate itself and infect other hosts.

– **Mass Mailing Worms**. A mass mailing worm is similar to an email-borne virus but is self-contained, rather than infecting an existing file

8.1.4 Trojan Horses:

A Trojan horse is a self-contained, non-replicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts.

8.1.5 Malicious Mobile Code:

Malicious mobile code is software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.

8.1.6 Blended Attacks:

A blended attack uses multiple infection or transmission methods. For example, a blended attack could combine the propagation methods of viruses and worms.

Many, if not most, instances of malware today are blended attacks. Current malware also relies heavily on social engineering, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. Because so many instances of malware have a variety of malware characteristics, the classic malware categories listed above (virus, worm, etc.) are considerably less useful than they used to be for malware incident handling.

At one time, there were largely different procedures for handling incidents of each malware category; now there is largely one set of procedures for handling all malware incidents, thus nullifying the primary need for having categories.

Another problem with the classic categories is that newer forms of malware do not neatly fit into them. For example, in the growing trend of web-based malware, also known as drive-by-download, a user's web browsing is redirected to an infected website, often with little or no use of social engineering techniques. The infected website then attempts to exploit vulnerabilities on the user's host and ultimately to install rootkits or other attacker tools onto the host, thus compromising the host.

Although the website is infected, its malware does not infect the user's host; rather, it functions as an attacker tool and installs other attacker tools on the host. Web-based malware is a blended attack of sorts, but its components do not map to the other malware categories.

The classic malware categories do not include phishing, which refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information.

To perform a phishing attack, an attacker creates a website or email that looks as if it is from a well-known organization, such as an online business, credit card company, or financial institution. The fraudulent emails and websites are intended to deceive users into disclosing personal data, usually financial information. For example, phishers might seek usernames and passwords for online banking sites, as well as bank account numbers.

Some phishing attacks overlap with web-based malware, because they install keystroke loggers or other attacker tools onto hosts to gather additional personal information. Organizations should avoid expending substantial time and resources in categorizing each malware incident based on the types of categories expressed above.

8.2. ATTACKER TOOLS

Various types of attacker tools might be delivered to a host by malware. These tools allow attackers to have unauthorized access to or use of infected hosts and their data, or to launch additional attacks.

8.2.1 Popular types of attacker tools:

Backdoors: A backdoor is a malicious program that listens for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a host, such as administration tools, which are installed on a host to enable a remote attacker to gain access to the host's functions and data as needed.

Keystroke Loggers:A keystroke logger monitors and records keyboard use. Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means.

Rootkits: A rootkit is a collection of files that is installed on a host to alter its standard functionality in a malicious and stealthy way. A rootkit typically makes many changes to a host to hide the rootkit's existence, making it very difficult to determine that the rootkit is present and to identify what the rootkit has changed.

Web Browser Plug-Ins: A web browser plug-in provides a way for certain types of content to be displayed or executed through a web browser. Malicious web browser plug-ins can monitor all use of a browser.

E-Mail Generators: An email generating program can be used to create and send large quantities of email, such as malware and spam, to other hosts without the user's permission or knowledge.

Attacker Toolkits: Many attackers use toolkits containing several different types of utilities and scripts that can be used to probe and attack hosts, such as packet sniffers, port scanners, vulnerability scanners, password crackers, and attack programs and scripts.

Because attacker tools can be detected by antivirus software, some people think of them as forms of malware. However, attacker tools have no infections capability on their own; they rely on malware or other attack mechanisms to install them onto target hosts. Strictly speaking, attacker tools are not malware, but because they are so closely tied to malware and often detected and removed using the same tools.

8.3. THE NATURE OF TODAY'S MALWARE

The characteristic of today's malware that most distinguishes it from previous generations of malware is its degree of customization. It has become trivial for attackers to create their own malware by acquiring malware toolkits, such as Zeus, SpyEye, and Poison Ivy, and customizing the malware produced by those toolkits to meet their individual needs. Many of these toolkits are available for purchase, while others are open source, and most have user-friendly interfaces that make it simple for unskilled attackers to create customized, high-capability malware.

8.3.1. EXAMPLE:

Here's an example of what a malware toolkit can do, illustrated by how the resulting attack works.

1. The toolkit sends spam to users, attempting to trick them into visiting a particular website.

2. Users visit the website, which has malicious content provided by the toolkit.

3. The website infects the users' computers with Trojan horses (provided by the toolkit) by exploiting vulnerabilities in the computers' operating systems.

4. The Trojan horses install attacker tools, such as keystroke loggers and rootkits (provided by the toolkit).

Many attackers further customize their malware by tailoring each instance of malware to a particular person or small group of people. For example, many attackers harvest information through social networks, and then use that affiliation and relationship information to craft superior social engineering attacks.

Other examples are the frequent use of spear phishing attacks, which are targeted phishing attacks, and whaling attacks, which are spear phishing attacks targeted at executives and other individuals with access to information of particular interest or value.

Malware customization causes significant problems for malware detection, because it greatly increases the variety of malware that antivirus software and other security controls need to detect and block. When attackers are capable of sending a unique attack to each potential victim, it should not be surprising that largely signature-based security controls, such as antivirus software, cannot keep up with them.

Mitigation involves a defense in depth approach, using several different detection techniques to increase the odds that at least one of them can detect the malicious behavior of the customized malware

8.4 CASE STUDIES:

Case Study 1. POPUP RISKS

Pop-up ads or pop-ups attacks are often forms of online advertising on the World Wide Web planned to capture email addresses and the personal information.

ILLUSTRATION 1:

Ankush was a pretty savvy Internet user and know to not open email attachments from unknown sources or automatically click on links that could download viruses onto his machine. However, one day while browsing the Internet, an icon popped up at the bottom of his screen that said "Your computer is infected! Click here to protect your computer from virus!" The icon looked like it came from his Windows system, so Ankush clicked on the link. He was confused when nothing happened, but he didn't give it much thought after that.

Within days Ankush noticed serious problems with his computer. Files showed up on his computer that he didn't put there, other files were disappearing, and pop-up windows for adult websites were appearing on his desktop. It turned out that Ankush had been a victim of a malware exploiting on his machines. This vulnerability gave the hacker full control of his computer. It took lots of time and effort for Ankush to get his computer back to normal, and he lost a lot of his data.

ILLUSTRATION 2:

Anuj and his friend Anup kept in touch regularly through email. Even though they lived on opposite ends of the country, One day, Anuj received an email from Anup that simply said "check out my pics!" "Such a short email felt strange," he tells us, "but I opened it anyway because I remembered her mentioning something about a family vacation." The email didn't

contain any pictures, but it did install a nasty virus onto Anuj's computer. Soon after, Anuj's other friends were getting similar emails from him. Some of them got tricked, just like Anuj did, and the virus continued to spread.

Tip: Update your browser with the latest software updates and security patches. Install and update genuine and latest Anti-virus software with patches.

ILLUSTRATION 3: FREE PIZZA – IT'S MALWARE

Recently during browsing for my project related article I have visited one website where it was written - its Pizza Hut's 55th anniversary, the email says, and you can join in the celebration by getting a free pizza at any of its restaurants. Just click on the "Get Free Pizza Coupon" button. When I clicked it displays repeated error messages. Seeing this I restarted my machine after that I found that many new and unexpected toolbars have created and shortcut icons created on my desktop.

An example

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

Case Study 2: SPYWARE RISKS

Spyware is a generic term for malicious software which ends up on your computer, and is used to gather information about you and other files on your computer and passes it over Internet to others.

ILLUSTRATION 1:

Akhilesh and Arpita got their first cellular phone so they could keep in touch with their grandchildren, who were off traveling around the world. Since international calls weren't

cheap, they often used SMS to send quick messages back and forth. Akhilesh and Arpita's plan allowed them to receive a limited number of messages each month for free, with a small fee for additional messages.

One of their grandchildren introduced them to a Web site that allowed users to send group messages. Akhilesh decided to sign up so their grandchildren could add them to their groups. As a part of the registration process, Akhilesh entered their cell phone number. Since all of their grandchildren's friends used the site, she assumed it was ok, and did not bother to read the privacy policy.

After signing up for the site, Akhilesh and Arpita began getting advertisements through SMS. It started as a trickle, and then became a flood. The mobile spam quickly used up their free incoming messages, and charges began piling up. Akhilesh went back to the Web site, whose privacy policy allowed her to opt out of getting future advertisements. The phone company would not refund the charges they had already accumulated though, so they still got stuck with a hefty bill.

ILLUSTRATION 2:

Adarsh Kumar has been fast climbing the ranks at a small, fashionable clothing company. A recent promotion required him to relocate, which, combined with longer work hours, made meeting people difficult. One day an old friend convinced him to try out online dating, but the dating sites he found all required an email address to register and receive messages. Without reading any of the site's privacy policies, he signed up with his work email address.

"The next day I came into work, and was really stoked to see 17 new messages. I thought the sites had really worked!" Adarsh Kumar said. But as it turns out, most of the new messages were junk, and the spam only got worse. By the next week, Adarsh Kumar was getting around 300 messages a day. "It became hard to keep up with clients, because of number of spam mails arriving.

Eventually, the volume of spam to Adarsh Kumar's account began to slow down the entire company's email system. This caught the attention of the company's IT department. They had to change Adarsh Kumar's email address and install expensive anti-spam software on the main mail servers. When upper management found out about the trouble Adarsh Kumar had caused, he was lucky to keep his job. In hindsight, Adarsh Kumar says that he has learned his lesson. Not only did I seriously hurt my chances for getting another promotion any time soon, I lost a lot of respect among my co-workers and clients. I guess this will teach me to be more careful about whom I give my email address to.

Tip:

- Protect your email address when filling out registration or subscription information.
- Don't reply to unsolicited email.
- Don't use the spam unsubscribe option
- Don't forward chain letters

- Read the terms and conditions while filling the form

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

Case Study 3: EMAIL PHISHING

Online scammers send you an e-mail and ask your account information or credit card details along with a link to provide your information. Generally, the links sent will be similar to legitimate websites. So whenever you post your details in the link then the details will be received by scammers and information given by you is misused.

A phishing attempt usually starts with an email urging you to click on a Web link in order to check something about your bank account or another on-line account. These emails often appear to be from popular online institutions such as eBay, AOL, PayPal, or MSN. When you click on the link you go to a page where you are asked for information. The page appears genuine, but is in fact counterfeit. Phishers may then use the personal information you give on the page to steal your identity or your

ILLUSTRATION 1:

Priyanka Rani had been at her new job for only a few days when she got an email from the IT department telling her there might be a problem with her account. A link in the email sent her to a Web page where she could enter her corporate username and password to maintain her computer access. "It looked official, so I went ahead and gave them my information," she says.

A few hours later, she got another email stating that hackers had forged the IT department's email address. It said that anyone who visited the fake Web page from the email should change his or her password and report the incident immediately.

Priyanka Rani changed her password right away, but the damage had already been done. It had only taken a few minutes for the hacker to log into the company's computer system and install a program that gave him full control of the system. The hacker had control of the network for months and used it to launch attacks against other networks, relay massive amounts of spam, and distribute illegal software.

Tips:

- Use common sense when giving out personal information
- For sites requiring personal information, type in the Web link yourself
- Check your bank and credit card statements for purchases that you did not make
- Check your bank and credit card statements for purchases that you did not make
- Use Anti-phishing tools

Note: Directly don't click on the link received in e-Mail and Cross check the link by typing it in the web browser

Case Study 4: DATA THEFT

One of the reasons we are so computer-dependent these days is our confidence on digital documents. These days we store everything in our computers from important letters and personal financial information to digital pictures and music files. Almost every company operation is stored in digital form: memos, financial information, projections, customer records, etc.

That's why it is so important to make sure the documents on your computer are safe from attackers. There are many ways an attacker can get to your personal documents, including getting into your computer's hard drive or intercepting email attachments. A direct intrusion by an attacker can give him access to your digital documents and passwords.

ILLUSTRATION 1:

As head of a famous online retailing company, Abhinav Sinha has access to a lot of sensitive information. In order to keep that information safe, he always uses strong passwords with letters, numbers, and special characters. However, this makes it hard for him to remember all of the login/password pairs he uses. So he thought keeping the passwords on my Personal Digital Assistant (PDA) would solve that problem. It was certainly safer than using a sticky note taped to my computer monitor.

One day, as he was walking back to the office from lunch, Abhinav Sinha reached into his pocket to check his calendar and the PDA was gone. He panicked. The passwords on it allowed access too many areas of the company's operations. Financial records. Customer databases. Proprietary information. Abhinav Sinha had lost the keys to the kingdom.

As soon as Abhinav Sinha realized his PDA was missing, he called the company's network and security administrator, who immediately went to server room for assessing the system logs, from where it is revealed that the stolen information had in fact already been used to access the system. The company is still trying to determine exactly what data was compromised before the passwords were changed. Has Abhinav Sinha kept his password file does not kept encrypted or used a password security tool; otherwise it would have taken the thief much longer to access his login information.

Tips:

- Conduct regular anti-virus scans
- Conduct regular spyware removal scans
- Don’t open digital files on your computer if you are not sure about the source
- Do not send any passwords or sensitive files through email unless you have an encrypted or secure email server
- Do not store sensitive data on your mobile device in clear text
- Do not store sensitive data on your laptop
- Set your anti-virus package for "Real-time Protection
- Set your anti-virus package for the types of files you want it to check

- Set your anti-virus software to make scheduled automatic scans
- Encrypt files that contain sensitive information
- Set your firewall to filter the appropriate ports
- Disconnect from the network if you have any security concerns.

Case Study 5: E-COMMERCE RISKS

E-commerce which is also called e-business is the term for conducting business over the Internet. However, you can run into some dangers. Online advertisements in the form of banner ads and pop-up ads commonly appear while you access e-commerce sites. These advertisements can lead users to untrustworthy Web sites and install cookies and spyware on computers.

Credit card information can be stolen while it is being sent over the Internet or later, if the business saves it for further transactions. Along with credit card information, you may also be asked for personal information like your address or date of birth during a transaction. This information could be stolen as well.

ILLUSTRATION:

Joseph has five brothers and sisters, so he watches every penny when buying Christmas presents. He knew his youngest brother, a budding artist, had his heart set on a new photo-editing program this year, but when Joseph did some online shopping; he saw that it was way out of his price range. A couple of days later, though, Joseph got an email advertising the photo-editing software for half of what it sold for in stores. It seemed like too good a deal to pass up, so he went to the Web site listed in the email and entered his credit card information.

The software in the end arrived, and Joseph was thrilled to see the smile on his brother's face on Christmas morning. But that good feeling didn't last long. The next week, Joseph's brother called him and told him that the software wouldn't work on his computer and worse, it had installed a damaging virus on his machine.

Tips:

- You never purchase anything from an online auction
- You need to create a strong password
- Always check for the secure connection
- Always set the web browser security settings
- Always use automatic updates to your computer operating system
- Always use latest, genuine and updated antivirus programs and scan it twice a day

Case Study 6: FILE SHARING

This type of Programs are designed to harm your computer Malware (short for “malicious software”) is any software designed to harm your computer, such as viruses, worms, Trojan horses, and rootkits.

ILLUSTRATION:

Like many teenagers, Shilpa loved to use file-sharing Web sites to find new music and videos. Her parents made sure she didn't download anything that was copyrighted, so they figured her file-sharing activities were harmless.

However, Shilpa's parents soon noticed that their computer wasn't working as well as it had been. A scan with their antivirus software showed that the computer had been invaded with loads of malware. It turned out that Shilpa had been downloading files from people she didn't know, and many of these files contained viruses and worms that wreaked havoc as soon as they got on Shilpa's computer.

Tip:

- Make sure to only download files from people you know and scans every file with antivirus software before downloading it.
- Scan all files that you receive through file transfer
- Always set the web browser security settings
- Always use automatic updates to your computer operating system
- Always use latest, genuine and updated antivirus programs and scan it twice a day

Case Study 7: FORTUNE IN FILLING EMAIL FORM

Rahul considered himself to be a pretty sharp guy, especially when it came to spotting a scam. When he got an email one day from a Mumbai widow who needed help getting her husband's fortune out of the bank, Rahul's first instinct was to delete it. But the email promised half the fortune to whoever would help, which made Rahul curious enough to reply asking for more information.

The woman wrote back, and Rahul was surprised by how legitimate her story sounded. They communicated back and forth a few more times, and the widow seemed to become more desperate with each email. She said she needed to pay Rs 10,000 in bank fees to get the money released, so finally Rahul decided to take the leap and send her the money.

But instead of getting his share of the fortune, Rahul just kept hearing about new problems that had cropped up, requiring him to send more and more money to resolve them. By year's end, Rahul was out Rs 50,000 with nothing to show for it.

Tip:

- Take the time to really check out her story before sending the money
- Never trust the online strangers
- Simply delete the such mails arriving at your inbox
- Enable the spam filter option in your email secure settings options
- Always enable and update with the latest Antispyware, Antimalware and Antivirus program.

Case Study 8: P2P FILE SHARING RISKS

File sharing is when you share computer data or space with others on a network. File sharing allows multiple users to read, modify, copy or print the same file. Different users may have different levels of access to files on the network. Peer-to-peer (P2P) file sharing has no central file server. The shared files are stored on users' computers where they can be accessed by the other users on the network.

During download one of the file mysteriously emailed to everyone in my address list. Your computer may be infected with malware, specifically a worm that self-propagates and forwards mail to everyone in your address list. This email is also infected and anyone who reads it also gets infected

ILLUSTRATION 1:

Anupama was a music lover with a huge collection of CDs that she had built up during high school. But when Anupama went off to college she found all her money going to rent and bills rather than CDs. Soon she found a new way to satisfy her music habit. She joined online file-sharing communities and quickly became a popular trader due to her extensive music collection. As her collection grew, her computer attracted more and more attention from other music lovers, and eventually from the law.

One day, I was sitting at my desk doing homework when I heard a loud knock at the door. There were five or six guys with dark uniforms and badges standing there, carrying huge guns," she remembers. It was the Cyber Police task force had come across her collection on the Music CD's and begun an investigation.

Because of her young age and clean criminal record, Anupama was charged with a low level criminal act. After her conviction, she was given a three month deferred jail sentence with three years. She was also ordered to pay an Rs 10,000 fine.

ILLUSTRATION 2:

Anil generally used to download from famous file sharing server in the form of music and movies etc. He has very good number of music and all other music lovers use to download from various parts of the India. One day he observed that sudden all the desktop icons are missing and files in his hard disk where he used to share has been deleted. And my friend Sunil called and told me that all my bank statements are posted on a web site, and then I realized it was the act of file sharing malware.

If you do not carefully set up your shared information or shared drives, you may end up sharing more information than you intended. This is especially true in the case of P2P applications where the other peers in the network have direct access to your computer**.**

Tips:

- Always read terms & conditions and privacy policies during downloads

- Install file sharing (P2P software) carefully so that what files or Directory you are sharing and what's being shared to other systems in P2P network.
- Use filtering software you trust to filter the data communication from your system.
- Use file sharing program controls and adjust the P2P program to run whenever you required. Disable automatic starting.
- Always update Operating System, Antivirus and Anti Spyware packages.
- Take back up of important files. This will help you in recovering the files.
- Delete any pirated software, files, etc. Alternatively, do not download them at all.

Case Study 9: EBOLA VIRUS MALWARE

Attachments are the main way malware gets onto your computer. Attachments include office document files (e.g., with .doc or .xls suffixes), program files (e.g., with .exe or .bat suffixes), and compressed files (e.g., with .zip suffixes), all of which can contain malware

ILLUSTRATION:

Dr. Ankur Saxena professionally is a doctor in the Ayurvedic field; generally he used to study the various articles from the Internet and blogs. Also he keeps on updating to his friends, patients across the India for the healthy tips. He has number of online blogs where he answers his patients about their health related issues. Recently there is an Ebola virus which is spreading the African country and found to be very dangerous. Dr Ankur got a mail from some famous health related agency regarding a high-level presentation on the Ebola virus. An attached zip file with a title like "EBOLA – PRESENTATION.pdf.zip"

As soon as he downloaded a file without scanning the same to his computer, it is infected with a virus, which was probably downloaded as a file or an email-attachment. And my computer ON and OFF and also cannot connect to the Internet.

Tip:

- If an email with attachments fails any of these tests, delete it. If you know the sender, contact him or her to make sure that the message is legitimate.
- Conduct regular anti-virus scans and update operating system patches with security patches
- Disable Local area network (LAN) and wireless connection interfaces when you are not using them
- Keep email software up-to-date and use any alternative email address for such type of downloads
- Perform frequent backups and enable firewall in your OS level

Example:

Ebola scare gives cybercriminals new phishing and malware attack targets: Symantec

By Tasneem Akolawala on Aug 18, 2014 at 6:43 PM

Case Study 10: TARGET ORDER CONFIRMATION MALWARE

Order confirmation email appears to be from Target claims that the company's online store has an order addressed to you. The message advises you to click a link to obtain full order information. The email is not from Target. The link in the message opens a compromised website that contains malware. The Target version is just one in a series of similar malware messages that have falsely claimed to be from well-known stores.

ILLUSTRATION 1:

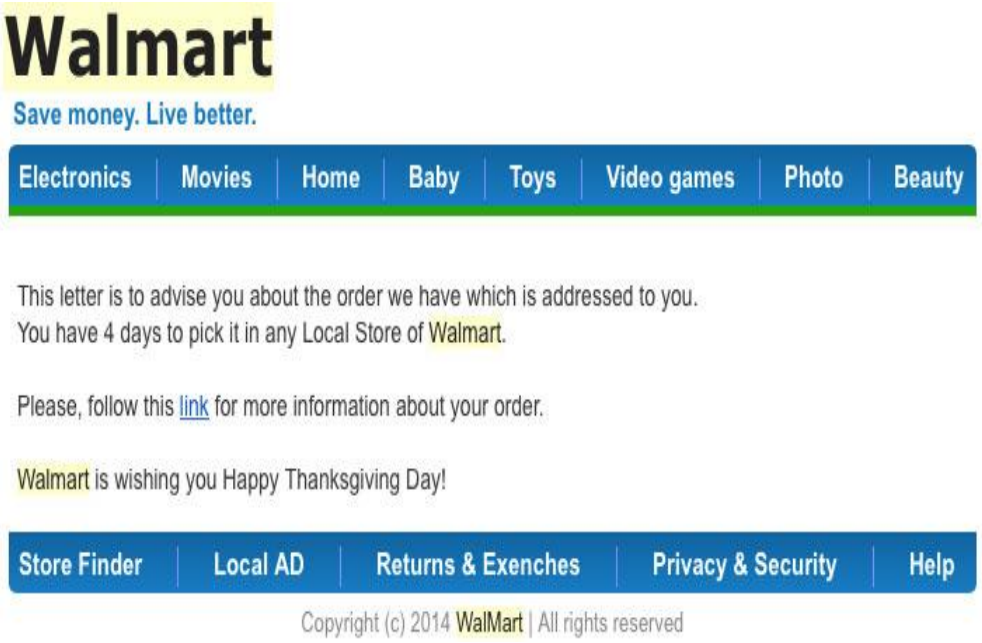
One day while Pranav opened his Gmail account, he received a mail saying as Thanksgiving nears we want to advise you that our online shop has an order addressed to you. You may pick it in any store of Target.com closest to you within four days.

Please, open the link for full order information. As soon as I clicked the link provided in the email I was re-directed to some suspicious website where I asked to provide all my personal information in the form of my name, mobile number, email address and banking related information for security related and confirmation of the product.

The malicious file may start downloading automatically. Alternatively, a message on the website may instruct you to click a link to download the file. Typically, the download will be a .zip file that hides an .exe file inside. Opening the .exe file will install the malware. After waiting

for some days I approached the number and email id provided, but it's no use as it was not reachable. But, typically, the malware can steal personal and financial information from your computer and pass on it to online scammers.

Examples:



Case Study 11: NAKED WOMAN EATEN BY SHARK POST LEADS TO MALWARE

This type of attacks happens generally when a user clicks on the link which he received during an attachment or through email link with a shocking subject and when you click on that link results in hijacking of your web browser and resulting to report each and every activity to the attackers remotely.

ILLUSTRATION:

Last week I got an email link from strangers with subject “Naked woman eaten by shark”. This email features an image of a naked woman apparently being eaten by a shark and includes a "Play" button that apparently opens a video showing the attack. Clicking the "Play" button takes you to a "news video" website. The site features teaser images for a large number of "shocking" videos, including the supposed shark attack.

However, when you click on any of the teaser images, a popup message will claim that you must install a plug-in before you can watch any videos. But, unfortunately, the plug-in is a malware program that can hijack your browser, show malicious advertisements, and interfere with security settings on your computer. Once installed, these malicious programs can be quite difficult to remove. After a few days some un-usual activities have been observed like my web browser are suddenly getting ON and OFF, and many number of shortcut icons created on my desktop and my file system also crashed in a week.

Tips:

- Be wary of any shocking video posts that come your way to your email as a link or attachment.
- Many are scams that try to get you to like and share bogus messages on email and participate in suspect online surveys.
- Others are designed to promote a particular webpage or as in this case - trick people into downloading malware into their computer.
- Always update your operating system patches, antivirus program
- Always run Antivirus program once in a week with latest security updates.
- Always enable operating system firewall and block any unwanted services in your system**.**

Example:

Case Study 12: IDENTITY THEFT RISKS

Identity Theft occurs when someone, without your knowledge, acquires a piece of your personal information and uses it to commit fraud. Identity theft is a crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it.

The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain. Identity theft is somewhat different from identity fraud, which is related to the usage of a false identity' to commit fraud.

ILLUSTRATION:

I was at our local library and was checking my email which said someone had tried to hack my PayPal account and asked me to re-enter all my details in the form of my name, mobile number, Valid Passport number, driving license number and my bank details like Account number, CVV code and PIN number. I should have known then that this was a scam, but I wasn't paying much attention and didn't think. The next day, I got a phone call from this man who said "Miss I don't want you to be scared, but your identity has been stolen.

I only had Rs 0.85 in my account at the time. Thank god, because any money in the account would have been taken. The bank looked at my transactions after I told them. They tried to assure me the man calling me was a hoax, but he wasn't. The bank worker looked at my account and there were all kinds of charges from all over the country, although most of them in china and Korea. I was almost in tears.

Tips:

- Never Trust the strangers email which come for updating the personal information
- Always enable the Antivirus and Firewall option in your machine for safer communication
- Always use filtering services as part of secure and financial transactions.
- Updated your Operating system files with the latest security patches from the concerned websites.

Case Study 13: PAYMENT GATEWAY 'CREDIT CARD TRANSACTION RESULT' MALWARE EMAIL

Payment gateway transaction result notification email claims that your credit card has been charged several hundred dollars. The email includes an attachment that supposedly contains a sales receipt for the transaction. The email is not a genuine transaction notification. The email includes an attached file that appears to be a sales receipt. Instead, the attached .zip file harbors a file that, if opened, can install malware on your computer. It may also download and install further malware and join the infected computer to a botnet.

ILLUSTRATION:

Aman generally used to shop online, one day he got a mail attachment with name “Payment Gateway Transaction Email Lists Credit Card Charge”. He was panicked into opening attachments or clicking links because they believe that their credit card has been used to make fraudulent transactions. According to this 'transaction result' email, a credit card transaction for some Rs 10,000 has been accepted. The email lists details of the supposed transaction and includes a payment gateway order and transaction code. The email includes an attached file that appears to be a sales receipt.

After checking my credit card information, there was no such illegal transactions happened. So he deleted that mail thinking it is spam or fake email attachment. Next day he observes some of the files from his system is affected with virus and by seeing this he run the “Antivirus program and it detected many number of malwares and because of this activity my system was crashed with blue screen.

Example:

Subject **Credit Card Transaction Result**

To

Transaction APPROVED

Merchant Web Site:	G.P. LTD
Order Number:	326054311303
Payment Gateway Order code:	6201989891692972
Payment Gateway Transaction code:	2479560813277048
Amount:	$ 524.49
Brand:	VISA
Authorization Code:	085848

********** Note **********

This e-mail has been sent automatically and represents a payment confirmation only.
Please don't reply because your message will not be read.
Should you have any questions or concerns regarding your order please contact the Merchant.

Tips:

- Be cautious of any unsolicited email that tries to get you to open an attachment
- Always scan an downloaded files from the Internet
- Always enable the Antivirus and Firewall option in your machine for safer communication
- Always use filtering services as part of secure and financial transactions.
- Updated your Operating system files with the latest security patches from the concerned websites.

Case Study 14: PARCEL NOT DELIVERED

Email appears to be from Australia Post claims that your parcel was not delivered to your address because nobody was home. The email instructs you to click a 'Track Your Item' link to get more information about the undelivered parcel. The email is not from Australia Post and the link does not open information about an undelivered parcel. Instead, the link leads to a website that harbors malware. In many cases, the malicious payload consists of CryptoLocker ransomware which is an harmful malware This malware may lock your computer until you pay an unlock fee to online criminals.

ILLUSTRATION:

Mishraji got an e-mail saying that your parcel has not been delivered to your address on October 15, 2014, because nobody was at home. Please view the information about your parcel, print it and go to the post office to receive your package. Track your item for more with the link provided. If you don't receive a package within 30 working days it will return back to the Australia post office. You can find any information about the procedure and conditions of parcel keeping in the nearest post office.

However, the email is not from Australia Post and the link does not lead to information about an undelivered parcel. Instead, the link opens a compromised website that installed malware in background without user attention. Once installed, this type of malware can lock files on your computer and demand a large fee for an encryption key to retrieve your files. Often, the scammers will claim that you must pay this fee within a specified time frame such as 72 hours or they will destroy the key thereby locking your files permanently.

Case Study 15: MALWARE: IMPORTANT - NEW OUTLOOK SETTINGS EMAIL

Email with the subject line 'Important - New Outlook Settings' advises you to click a link to download instructions before updating settings for Microsoft Outlook. The email is not legitimate. The link opens a compromised website that installs malware. It may download further malware components that collect sensitive information such as banking login details and send them back to online criminals.

ILLUSTRATION:

One fine day in the afternoon after having my lunch at the office canteen I received an email with subject important for updating “New outlook settings” with the link provided in the mail with all the necessary security patches. Generally I used to type the link which comes to my mail, but I was getting late to office I clicked the same link provided in the mail.

Next day all our office members were not getting the emails, then I checked the logs of the email server which says that we are the attack of malware and within a no time entire our emails server got crashed.

Tips:

- If you receive one of these emails, do not click any links or open any attachments that it contains. Simply delete it.
- Always enable the filtering service at your corporate firewall
- Always enable the Antivirus program for such kind of suspicious activity to block
- Always update the operating system with security patches

Case Study 16: SHAKIRA DEATH HOAX EMAIL CONTAINS MALWARE

In this type of attack a user receives an email claims that Colombian entertainer Shakira has been killed in a car accident and invites you to open an attached file for further details. Opening the attachment loads a document that claims that you must change your Office security settings to enable macros before the accident pictures and report can be viewed. But, following the instructions in the document will run the malicious macro. The macro can then downloads and install further malware.

ILLUSTRATION:

Recently Alox Mishra received an email regarding the death news of famous pop singer Shakira; I was shocked for the first time. Then I carefully studied about the content return and opened the word document which contains the images and the complete details. As soon as I opened, my browser crashed and unable to open for some time. After two days my system get slow down and unable to open the files and folders from my computer. However, the claims in the email are untrue. Shakira is alive and well. And the attachment does not contain images and information about a car accident as claimed.

Tips:

- Disable the macros security default in the Microsoft word document's and excel etc.
- Always open the attached file's with an antivirus software installed in your computer, before opening it
- And be very cautious of any document or message that claims that you must enable macros to view content
- Always update the operating system with security patches

Case Study 17: DENAIL OF SERVICE ATTACK

Denial of service (DoS) attacks interferes with an Internet connection by deliberately sending more traffic to the connection than it can handle. A network is designed to be able to handle only a certain amount of traffic, so when this level is exceeded it won't let any more connections be made, like a telephone sending out a busy signal. This causes problems not only for the computer that's being bombarded with traffic, but also for the computers that are legitimately trying to make a connection with that computer.

ILLUSTRATION 1:

Anupama was the CEO of an online bookseller. Her company made thousands a day in sales, but with shipping costs rising, each day of business just barely kept her afloat. Therefore, Anupama was horrified when one day she got an anonymous email threatening to shut down her website unless she paid the sender a large amount of money.

Anupama checked with her IT department and found that the company was indeed vulnerable to such an attack. The attacker could easily create a network of "zombie machines" that would send way more traffic to her site than it could handle, effectively crippling it. Anupama paid the money to the attackers and then spent twice as much getting the site's security up to date so that this sort of thing couldn't happen again.

Tips:

- Protect your usernames and passwords
- Increase your Web server's computing resources
- Create a separate hard drive partition for Web server activities
- Use Bandwidth-limiting software's to monitor the traffic and limit the same if it exceeds
- Increase your security settings for web server and network

Chapter 9:

Online Threats

9. ONLINE THREATS

9.0. INTRODUCTION:

Children may face different security risks when they use a computer or when they are online. Not only do you have to keep them safe, you have to protect the data on your computer. By taking some simple steps and can reduce the risks.

9.1. WHAT ARE THE RISKS?

- Exposure to inappropriate images or content
- Solicitation by sexual predators in chat rooms and by email.
- Online bullying or harassment.
- Piracy of software, music or video.
- Disclosure of personal information.
- Spyware and viruses.
- Excessive commercialism: advertising and product-related websites.
- Illegal downloads, such as copyright-protected music files.

9.2. GENERAL SAFETY TIPS

- If you suspect a pedophile may be grooming or trying to befriend your child or your child is being stalked or harassed, contact your local police.
- Set ground rules for children.
- Use Internet content filtering and spam filters to reduce the risk of accidental exposure to unwanted content.
- Set up shared computers properly to restrict what children can do.
- Consider setting up a family e-mail account which can be used specifically to register for websites, competitions, etc.
- Be careful about peer-to-peer file sharing.

Monitor children's use of the Internet

All the web browsers keep a record of recently visited sites and also make temporary copies of web pages. To see recently visited sites, click on the *History* button or press Ctrl and the H key.

- To see temporary files, open Internet Explorer Select *Internet Options*, on the *General* tab under *Temporary Internet Files* click the *Settings* button and click *View Files.*

- Understand the risks yourself and plan ahead before monitoring and allowing children access to the Internet.
- Discuss with children what they can and cannot do online.

- Make a contract with children on usage of computer with signing.
- Work out how you are going to monitor their Internet use.
- The boundaries you set and the kind of conversations you have with your children will depend on their age and technical ability as well as your judgment as parents.
- These factors will change as they grow up and should be reconsidered regularly.

Monitoring children's behavior online

- If a child is too young to access computer always sit with them while they are online.
- Ask your children to share all their online user names and passwords with you.
- Set browser settings to limit the access to inappropriate content.
- Put the computer in an open area in the home rather
- Consider installing Internet monitoring software to track what they do online.

Create a user account for each user

Set up a separate user account for your child with a limited permission and can give limited control over the computer. For example, they won't be allowed to install new programs or change settings without your permission. It also helps monitor and control what they do online.

9.3. MOST COMMON ONLINE THREATS

Online Scam

Online scam is an attempt to trap you for obtaining money. There are many types of online scams; this includes obtaining money with fake names, fake photos, fake e-mails, forged documents, fake job offers and many more. Generally, it happens by sending fake e-Mails for your personal details like online banking details, credit card details. Sometimes e-Mails are sent from lottery companies with fake notice, whenever you participate in online auction and e-Mails received for fake gifts.

Phishing scam

Online scammers send you an e-mail and ask your account information or credit card details along with a link to provide your information. Generally, the links sent will be similar to your bank. So whenever you post your details in the link then the details will be received by scammers and money is misused.

Lottery scam

Sometimes you receive an email like "you won a lottery of million dollars" receiving such a kind of mails is a great thing, and really it's a happiest thing. By responding to such a kind of mails huge amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money.

Online Auction

If you bid for a product you never get the product promised or don't match the product, and the description given to you may be incomplete, wrong, or fake. The scammer accepts the bid from one person and goes for some other sites where they can get less than the winning bid so scammers may not send the product you wanted.

Forwarding Product or Shipping Scam

Whenever you answer an online advertisement for a letter or e-mail manager like some US based corporation lacks address or bank details and needs someone to take goods and sent to their address or ship overseas, and you are asked to accept the transfers into your bank.

Generally, it happens for the products that are purchased using stolen credit cards and shipped to your address and then you will be fooled and asked to reship the product to others they might be thieved who reship the product overseas. The stolen money will be transferred to your account.

Email Scam Like --Congratulations you have won Webcam, Digital Camera, etc.

Sometimes you get an e-mail with a message like -- you have won something special like digital camera webcam , all you need to do is just visit our web site by clicking the link given below and provide your debit or credit card details to cover shipping and managing costs. However the item never arrives but after some days the charges will be shown on your bank, and you will lose money.

By e-mails

Generally, fraudsters send you an e-mail with tempting offers of easy access to a large sum of money and ask you to send scanned copies of personal documents like your address proof, passport details and ask you to deposit an advance fee for a bank account. So once you deposit the funds, they take money and stop further communication, leaving you with nothing in return.

Unscrupulous Websites for Income Tax Refund

Generally, websites feel like official websites and seek the details of credit card, CVV PIN of ATM and other personal details of the taxpayers in the name of crediting income tax refund through electronic mode.

9.4. TIPS TO PREVENT ONLINE SCAMS

Confirm whether email is received from bank or not

Be cautious while providing bank details via online, before proceed further confirm with the bank about the email you received. Think that if something is important or urgent why don't bank calling me instead of sending email?

Confirm the shipping

Beware of shipping scam make sure you get authorized signed via fax before proceeding further and make sure you received from an authorized company.

Be cautious while online auction

Don't be trapped with discounts think wisely before you proceed with online auction. Think why $200 product would be $ 20.

Be aware about the product you received via email

Be aware about the products you get for a less price just think why only I received email for products that I never enter for any online shopping or contest.

Don't be trapped by lottery scam

Don't get trapped by scammers and e-Mails with a subject line you won some $10000 just think why only you received the email without your participation.

9.5. ONLINE BANKING

Online Banking can also be referred as **Internet Banking**. It is the practice of making bank transactions or paying bills through the Internet. We can do all financial transactions by sitting at home or office. Online banking can be used for making deposits, withdrawals or even we can use it for paying bills online. The benefit of it is the convenience for customers to do banking transactions is very high, the customers need not wait for bank statements, which arrive by e-mail to check their account balance. They can check their balance each and every day by just logging into their account. They can catch the discrepancies in the account and can act on it immediately.

Link Manipulation

Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the Attacker Database of your bank website; actually this URL points to the "yourbank" (i.e. phishing) section of the Attacker Database website.

Filter Evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

9.6. MALWARE ATTACKS

Example:

Clampi Virus Targets Users at Banks and Credit Card Sites

Keeping up with the latest Web security threats is a daunting task, because viruses and Trojans emerge, evolve, and spread at an alarming rate. While some infections like Nine Ball, Conficker, and Gumblar have hit the scene and immediately become the scourge of the cyber security world, others take their time -- quietly infiltrating more and more computers before revealing the true depth of the danger they pose.

One such slow grower is Clampi, a Trojan that made its debut as early as 2007 (depending on who you ask) but is only now raising hairs outside professional security circles. Clampi primarily spreads via malicious sites designed to dispense malware, but it's also been spotted on legitimate sites that have been hacked to host malicious links and ads. Using these methods, Clampi has infected as many as half a million computers, Joe Stewart, of Secure Works, told a crowd at the Black Hat Security Conference in July, USA Today reports.

Once installed on a PC, the Trojan quietly waits for you to visit a credit card or banking Web site. When it detects you're on one of the roughly 4,600 financial Web sites it's trained to watch, it records your username and password, and feeds that information back to the criminals. Clampi can even watch for network login information, allowing it to spread quickly through networked PCs (e.g., those in an office).

In fact, it seems that businesses have been the primary target of Clampi so far. According to the Times Online, in July, an auto parts shop in Georgia was robbed of $75,000 when criminals stole online banking information using Clampi. The Trojan was also used to infiltrate computers for a public school district in Oklahoma and submit $150,000 in fake payroll payments.

9.7. ONLINE SHOPPING

Online shopping has become a most popular to purchase all the things without leaving your home, and it is the very convenient way to buy things like electronic appliances, furniture, cosmetics, and many more. We can avoid the traffic and crowds. There is not particular time to buy things we can buy at any time instead of waiting of when the store will be open. Apart from all these advantages risks are involved and there are unique Internet risks so it is very important to take some safety measures before you go for online shopping.

Tips for safe online shopping

- Before you go for online shopping make sure your PC is secured with all core protections like an antivirus, anti-spyware, firewall, system updated with all patches and web browser security with the trusted sites and security level at high.
- Before you buy things online research about a web site that you want to buy things from, since attackers try to trap with websites that appear to be legitimate, but they are not.
- So make a note of the telephone number's physical address of the vendor and confirm that the website is trusted site. Search for different web sites and compare the prices. Check the reviews of consumers and media of that particular web site or merchants.
- If you are ready to buy something online check, whether the site is secure like https or padlock on the browser address bar or at the status bar and then proceed with financial transactions.
- After finishing the transaction take a print or screenshot of the transaction records and details of product like price, confirmation receipt, terms and conditions of the sale.
- Immediately check the credit card statements as soon as you finish and get them to know about the charges you paid were same, and if you find any changes immediately report to concern authorities.
- After finishing your online shopping clear all the web browser cookies and turn off your PC since spammers and phishers will be looking for the system connected to the Internet and tries to send spam e-Mails and try to install the malicious software that may collect your personal information.
- Beware of the e-Mails like "please confirm of your payment, purchase and account detail for the product." **Remember legitimate business people never send such a type of e-Mails.** If you receive such a type of e-Mails immediately call the merchant and inform the same.

9.8. IDENTITY THEFT

Identity Theft occurs when someone, without your knowledge, acquires a piece of your personal information and uses it to commit fraud.

Identity theft is a crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain. Identity theft is somewhat different from identity fraud, which is related to the usage of a false identity' to commit fraud.

Identity theft can be divided into two broad categories:

- Application fraud
- Account takeover

Application fraud happens when a criminal use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. On the other hand they may create counterfeit documents.

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, then contacting their card issuer masquerading as the genuine cardholder, and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent.

Chapter 10:

Desktop Security

10. DESKTOP SECURITY

10.0. INTRODUCTION

Securing your computer is essential to protecting your privacy, reducing the risk of identity theft, and preventing hackers from taking over your computer. Unfortunately, maintaining the security of your computer can be challenging. Hackers often seem to be one step ahead of even those computer users who are following the best security practices.

Maintaining your privacy requires you to take a multi-pronged approach. It involves protecting your sensitive information by preventing, detecting, and responding to a wide variety of attacks. There are many potential risks to your computer. Some are more serious than others. Among these dangers are:

- Viruses corrupting your entire system
- Someone breaking into your system and altering files
- A hacker using your computer to attack others
- Someone stealing your computer and accessing your personal information

There's no guarantee that even with the best precautions some of these things won't happen. However, you can take steps to minimize the risks to your computer and your sensitive information. Ultimately, the security of your computer is dependent upon you.

10.1. CHOOSING OPERATING SYSTEM AND SOFTWARE

Operating system: An operating system is the main program on a computer. It performs a variety of functions, including determining what types of software you can install, coordinating the applications running on the computer at any given time, and allowing your software applications (web browsers, word processors, and email clients) to operate. When you buy a computer, you are usually also choosing an operating system. Manufacturers typically ship computers with a particular operating system. Most PCs ship with the latest version of the Windows operating system. Apple computers use the Macintosh operating system.

Windows operating systems traditionally have been targeted more often than other operating systems. This may be due to the larger base of Windows installations, which makes it a more attractive target. Indeed, Macintosh computers historically have been subject to far fewer attacks than Windows computers. However, Apple products are definitely not immune to security flaws. As Apple's market share increases, the odds of malware being written for Apple products also increase.

One of the most contentious issues among computer security professionals may be the answer to the question "Which operating system is the most secure?" The general consensus among security researchers is that there's nothing about Apple's Macintosh operating system that makes it inherently more secure than Windows. In fact, the only truly secure operating system is one that has absolutely no contact with the outside world.

Some computer security professionals consider Linux and other lesser known operating systems to be the most secure, primarily because they tend not to be targeted. For those interested in trying out the Linux operating system, many people recommend Ubuntu, a free, open-source Linux distribution available at www.ubuntu.com/.

No matter which operating system you use, it's important that you update it regularly. Windows operating systems are typically updated at least monthly, typically on so-called "Patch Tuesday." Other operating systems may not be updated quite as frequently or on a regular schedule. It's best to set your operating system to update automatically. The method for doing so will vary depending upon your particular operating system.

If your computer uses Windows XP as the operating system, it's very important to be aware that Microsoft support for Windows XP ended on April 8, 2014. This means that you will no longer receive software updates from Windows Update, including security updates that can help protect your computer from harmful viruses and malware. You should upgrade your operating system (if your computer can support it), purchase a new computer, or switch to a different operating system to avoid the risks of an unsupported operating system.

Internet browser. Many people regard the Mozilla Firefox browser as superior to Microsoft's Internet Explorer. Mozilla tends to patch Firefox security vulnerabilities more quickly than Microsoft patches Explorer. One advantage of Firefox is that it is an "open source" program. This allows security professionals to become involved in fixing bugs and building stronger security features. Another advantage of Firefox is its so-called Add-Ons, which can be used to strengthen Firefox's built-in security and privacy features. Three Firefox Add-Ons that we recommend are NoScript, Better Privacy, and HTTPS Everywhere.

NoScript. When you install NoScript, executable contents or "scripts" such as JavaScript, Java, Flash, Silverlight and others, are blocked by default. You can allow these scripts to run on a site that you trust (for example, your bank) through a simple mouse click. You can "whitelist" or authorize scripts for a particular session or permanently if you trust a website.

Better Privacy. Many websites have begun to utilize a type of cookie called a "flash cookie" (sometimes known as a "super cookie") that is more persistent than a regular cookie. Normal procedures for erasing standard cookies, clearing history, erasing the cache, or choosing a "delete private data" option within the browser will not affect flash cookies. Flash cookies thus may persist despite user efforts to delete all cookies.

HTTPS Everywhere. HTTPS Everywhere encrypts connections to over 1,000 popular websites. Without HTTPS, your online activities are vulnerable to eavesdropping and your accounts are vulnerable to hijacking. HTTPS Everywhere makes it easier for you to keep your user names, passwords, and browsing histories private.

It's important to note that HTTPS everywhere can protect you *only when you're using sites that support HTTPS and for which HTTPS everywhere includes rules*. HTTPS Everywhere depends entirely on the security features of the individual websites that you use. It *activates* those security features, but it can't *create* them if they don't already exist. If you use a site not supported by HTTPS Everywhere or a site that provides some information in an insecure way, HTTPS Everywhere can't provide additional protection for your use of that site.

No matter which browser you use, it's important that you update it as newer versions come out which address security vulnerabilities. The Firefox browser will automatically deliver updates on a fairly frequent schedule, typically every few weeks. Other browsers may not update as frequently and may not update automatically.

Portable Document Reader: Most people use Adobe Reader to read and print portable documents (.pdf files), such as forms and publications. Like Internet Explorer, the Adobe Reader is extremely popular, so it has become a target for the bad guys. Adobe tends to be slow in patching security vulnerabilities. Many security experts believe that you are safer using alternative document readers.

Adobe Flash Player: Most computer users have Adobe's Flash Player installed. In many cases, users are running an older version of Flash Player that may contain numerous security vulnerabilities. You can update your Flash Player at http://get.adobe.com/flashplayer/. Be sure to uncheck the bundled McAfee Security Scan plus download if you don't want it.

Java: If your computer has Java installed, the Department of Homeland Security has recommended that you disable it. It's unlikely that a typical computer user will ever need to use Java. Java has been responsible for a large number of malware attacks on the computers of unsuspecting users. You can disable Java by following these instructions: http://www.infoworld.com/t/web-browsers/how-disable-java-in-your-browsers-210882.

10.2. USING FIREWALLS, ANTI-VIRUS PROGRAMS, AND ANTI-MALWARE PROGRAMS

Every user of a personal computer should be familiar with firewalls, anti-virus programs, and anti-malware programs. These programs complement one another and must be used together to provide the highest level of protection to your computer. They are necessary to protect you from threats designed to damage, disrupt, or inflict illegitimate activity on your computer.

The term *malware* is short for malicious software. The more common types of malware include viruses, worms, Trojans, spyware, and adware. The damage inflicted by malware may range from minor annoyances to more serious problems including stealing confidential information, destroying data, and disabling your computer.

Most security software that comes pre-installed on a computer only works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software only protects you against the newest threats if it is kept up-to-date. That's why it is critical to set your security software to update automatically.

Firewalls, anti-virus programs, and anti-malware programs are important elements to protecting your information. However, none of these is guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk. Some anti-virus programs also contain anti-malware capability. However, given the increasing sophistication of malware programs, it's best to use two different anti-malware programs in addition to an anti-virus program. Each one looks for slightly different sets of threats, and used together they may offer increased security.

Firewalls: A firewall helps to prevent data from entering or leaving your computer without your permission. It helps make you invisible on the Internet and blocks communications from unauthorized sources. Every computer that is connected to the Internet should run a firewall at all times. There are two types of firewalls—software and hardware. You can run both simultaneously. In fact, it is a good idea to use both a software and hardware firewall. But never run two software firewalls simultaneously.

Some operating systems have built-in software firewalls. An example of a software firewall is the one built into most new Windows operating systems. Windows 7and 8, Vista and XP Service Packs 2 and 3 have built in firewalls that are turned on by default. You should leave the Windows firewall turned on unless you replace it with third-party firewall software.

Hardware firewalls can be purchased as stand-alone products or may be found in broadband routers having firewall features. A router sits between your modem and your computer or your network. It is hard to hack your computer or a network when it is hidden behind a hardware firewall box. However, it is important to properly configure your router, particularly by changing the default password to one that is difficult to crack. To ensure that your hardware firewall is properly configured, consult the product documentation.

Anti-virus programs: A virus is simply a computer program. It can do anything that any other program you run on your computer can do. A computer virus is a program that spreads by first infecting files or the system areas of a computer and then making copies of itself. While some viruses are harmless, others may damage data files, some may destroy files, and others may just spread to other computers.

You should not have two anti-virus programs actively running resident on your computer at the same time. Running more than one anti-virus program at the same time can potentially cause conflicts that affect your computer's performance. Be sure to fully disable or remove any anti-virus programs that you are no longer using or which are not currently being updated with new definitions.

On the other hand, it is permissible to run a periodic scan with a second anti-virus program (such as an online virus scanner) as long as the program is not actively running resident on your computer.

Anti-malware (anti-spyware) programs: Malware is a broad category of computer threats including spyware, adware, Trojan horses, and other unwanted programs that may be installed without your knowledge or consent. Spyware can secretly gather your information through your Internet connection without your knowledge. Once spyware is installed, it may deploy numerous files onto your system. Some of these files are so well hidden that they are difficult to find and remove.

When spyware is running on a computer system, there is almost no data outside of its reach. Commonly targeted data includes your Internet activity, email and contact information, and your keystrokes. Spyware can track your online activity, looking for websites visited, and financial data such as credit card numbers or financial account numbers on your screen, browsing and online purchasing habits, and passwords. When keywords of interest like names of banks or online payment systems are observed, the spyware starts its data collection process.

Spyware programs may be included with other software you want. When you consent to download a program, such as a music sharing program, you may also be consenting to download spyware. You might not be aware that you agreed to the spyware installation because your consent is buried in an end-user-license agreement (EULA).

Be cautious about clicking on pop-up boxes. Spyware programs may create a pop-up box where you can click “yes” or “no” to a particular question. If you click on either choice your browser may be tricked into thinking you initiated a download of spyware.

Anti-malware and anti-spyware programs can help to eliminate many of these threats. Security experts recommend that you use at least two and preferably three anti-malware/anti-spyware programs on your computer, as no one program has been found to be fully effective at detecting and removing these threats. For more about spyware and malware, read www.us-cert.gov/cas/tips/ST04-016.html.

Examples of sites offering free anti-malware software include:

- Malwarebytes www.malwarebytes.org/
- Spybot Search and Destroy www.safer-networking.org/en/index.html
- Super Anti-Spyware www.superantispyware.com/

10.3. USING YOUR COMPUTER SAFELY

Use a limited access or standard account: Most recent versions of Windows operating systems allow you to create a limited or standard account that does not have administrative privileges. This limited account is intended for someone who is prohibited from changing most computer settings and deleting important files. A user with a limited account generally cannot install software or hardware, but can access programs that have already been installed on the computer. On the other hand, the administrator account is intended for someone who can make changes to the computer and install software.

Security professionals recommend that you create a limited or standard account and use it at all times except when you actually need to install software or hardware or change your system’s settings. Log in to your administrator account only when you need to do so to make system changes.

Using administrator rights sparingly can help protect your computer from numerous vulnerabilities. An account without administrative rights can offer a great deal of protection. Creating and using a limited account for most daily tasks, such as surfing the web and reading emails, will reduce the amount and type of malware that is able to infect your computer. Many forms of malware require a user to be running as an administrator in order to infect your computer. Operating as a limited or standard user greatly reduces the effectiveness of many types of malware.

You can read how to set up a limited access or standard user account on Windows Vista and Windows 7 operating systems at www.howtohaven.com/system/standard-user-account.shtml.

Keep your software up-to-date: Computer hackers are always finding new ways to penetrate the defenses of your software programs. Software vendors respond with patches that close newly found security holes. To stay protected, you need to download and install patches for both your operating system and your software applications whenever they become available. Software patches or updates often address a problem or vulnerability within a program.

Sometimes, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. It is important to install a patch as soon as possible to protect your computer from attackers who would take advantage of the vulnerability. Attackers may target vulnerabilities for months or even years after patches are available.

Some software will automatically check for updates, and some vendors offer users the option to receive automatic notification of updates through a mailing list. If these automatic options are available, take advantage of them. If they are not available, check your software vendors' websites periodically for updates. Only download software patches from websites that you trust. Do not trust a link in an email message. Beware of email messages that claim that they have attached the patch to the message—these attachments are often viruses.

If you are using Windows XP, Vista, or Windows 7 or 8, you can configure the Automatic Updates features in Windows to notify you when important updates are available for your computer. For step-by-step instructions see http://support.microsoft.com/kb/306525.

It's also very important to keep your other software programs up to date. This can be a daunting task, since many computers contain dozens of software programs. Many are pre-installed when you buy your computer. Hackers are constantly attacking flaws in popular software products such as Adobe PDF Reader**,** Adobe Flash Player, QuickTime, and Java.

A good solution to the problem of updating your computer's software is Secunia Personal Software Inspector (PSI). Secunia PSI is a free software program designed to detect vulnerable and outdated programs on your Windows computer. This program alerts you when your programs require updating to stay secure. You can download Secunia PSI at http://secunia.com/vulnerability_scanning/personal/.

Use strong passwords: Whenever you have an opportunity to create and use a password to protect your information, make sure that you use a strong password. Passwords are frequently the only thing protecting our private information from prying eyes. Many websites that store your personal information (for example web mail, photo or document storage sites, and money management sites) require a password for protection. However, password-protected websites are becoming more vulnerable because often people use the same passwords on numerous sites.

Password managers: It can help make it easier for you to use unique and strong passwords for any website requiring a login. Never store an unencrypted list of passwords on or near your computer. Password recovery methods are frequently the "weakest link", enabling a hacker to reset your password and lock you out of your account. Make sure your security questions aren't easily answerable. It's also a good idea to have your password resets go to a separate email account designed for resets only. .

Avoiding spam: Spam is loosely defined as unsolicited, unwanted email messages from a sender you don't know. Spam email is usually sent in bulk with messages having substantially identical content. Spam messages, by the billions, flood computer mailboxes each year.

Spam breaks down further into two categories:

- *Nuisance* emails, such as solicitations to buy products or services
- *malicious* emails, which often seek to trick you into revealing personal information that then can be used to defraud or damage you and your computer

The vast majority of spam falls into the first category. Since this fact sheet deals with computer security, we will focus on the latter category.

Be skeptical: Think before you click. Don't open unexpected email attachments from unknown persons. Just because an email message looks like it came from someone doesn't mean that it actually did. Scammers can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. For more information, read www.us-cert.gov/cas/tips/ST04-010.html.

Don't click on links embedded in email messages. It's usually safer to go to the company's website directly from your browser than by clicking on a link in an email message, unless you are absolutely certain that the email was actually sent by the person or company claiming to have sent the message.

Spear phishing: It is a type of phishing attack that appears to be from a colleague, employer or friend and includes a link or something to download. Spear phishing often targets senior executives at organizations that may have valuable information stored on their computers. These messages may be personalized with publicly available information about the recipient to make them look genuine.

No matter how official an email message looks, never access a financial account by clicking on an embedded link. If the email is fraudulent, a scammer could use the account number and password you enter to steal your identity and empty your account. One way to protect against this is to use an incorrect password on the first try. A phishing site will accept an incorrect password, while a legitimate site won't. You should also avoid calling any telephone number in an unsolicited email unless you have confirmed that it is a legitimate number.

Be cautious when using P2P (peer-to-peer) file sharing: Peer-to-peer (P2P) file-sharing allows users to share files online through an informal network of computers running the same software. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. While P2P file sharing can be used for legitimate purposes, much of the content shared includes copyright-protected material that is being shared illegally, that is, in breach of copyright laws.

Every day, millions of computer users share files online. To share files through a P2P network, you download special software that connects your computer to other computers running the same software. Millions of users could be connected to each other through this software at one

time. The software often is free. For more information on P2P, see www.onguardonline.gov/topics/p2p-security.aspx.

Turn off your computer or disconnect if from the Internet: It's best to turn off your computer if you will not be using it for a long period of time. The development of DSL and cable modems has made it possible for computers to be online all the time, but this convenience comes with risks. The likelihood of your computer being compromised is much higher if your computer is always connected to the Internet. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. This can reduce the chance that a malicious remote computer will penetrate your computer.

Alternatively, you can simply turn your computer off. This has the added advantage of saving energy. It's also a good idea to turn off your computer periodically, since Windows will reboot when you restart your computer. Rebooting clears your computer of files that can degrade your computer's performance.

Do not leave unencrypted sensitive documents on your device. It's best to encrypt sensitive files and store them on an unconnected device such as a password protected USB thumb drive. For added security, keep the USB drive in a locked filing cabinet or a safe deposit box.

Back up all your data: While your computer may be an expensive asset, it is replaceable. However, the data and personal records on your computer may be difficult or impossible to replace. Whether or not you take steps to protect yourself, there is always the possibility that something will happen to destroy your data.

Regularly backing up your data can reduce the impact of a computer malfunction. Determining how often to back up your data is a personal decision. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

There are many hardware and software alternatives for backing up your data including USB flash drives and external hard drives (hardware) as well as archiving and disk imaging programs (software). Each method has its own advantages and disadvantages. For a simple solution, important files can be saved to an encrypted USB flash drive. It's a good idea to keep your backup media in a locked and secure location.

Type carefully: Scammers sometimes create look-alike sites that may utilize common misspellings of popular URLs. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

Protect sensitive information: Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. Don't send sensitive information over the Internet before checking a website's security.

Encrypt files on your computer, laptop or portable device: Computers are lost, stolen or hacked every day. As a result, your personal information can become available to anyone and

may lead to privacy invasion and identity theft. Many computers and other devices contain sensitive files such as financial records, tax returns, medical histories, and other personal files.

Many computer users rely on laptops and other portable devices because they are small and easily transported. But while these characteristics make them convenient, they also make them an attractive target for thieves. Make sure to secure your portable devices to protect both the machine and the information it contains. It's important to encrypt any sensitive data on such devices. USB flash drives pose security risks for similar reasons. Use them cautiously. Some flash drives offer built-in encryption features. Encryption is a way to enhance the security of a file or folder by scrambling the contents so that it can be read only by someone who has the appropriate encryption key to unscramble it.

Unencrypted files on your computer can be read by anyone *even if your computer is password protected!* There are methods by which a person who has physical access to your computer can read unencrypted files without entering your Windows password. So it's important to encrypt sensitive files even if they are on a password-protected desktop computer.

Windows has a built in file encryption program called Encrypting File System (EFS). EFS allow you to store information on your hard disk in an encrypted format. To use EFS, the user must affirmatively choose to encrypt a particular file or folder. It is not automatic. You can read about EFS at http://windows.microsoft.com/en-US/windows-vista/Encrypt-or-decrypt-a-folder-or-file.

You can read about additional free encryption programs for Windows at www.techsupportalert.com/best-free-file-encryption-utility.htm. For a comprehensive guide to encrytion, see

http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html?page=0.

A few additional "Don'ts"

- Don't download free screensavers, wallpaper, games, or toolbars unless you know they're safe. These free downloads may come with embedded malware.
- Don't visit questionable websites. Hacker sites, sexually explicit sites, and sites that engage in piracy are known for having malware. Just viewing a page can download malware to your computer.
- Don't give out your full name, address, phone number, Social Security number, financial account numbers, full date of birth, or other personal information in a chat room or social networks.

10.4. USING WIRELESS CONNECTIONS (Wi-Fi)

An increasing number of households and businesses are establishing wireless networks to link multiple computers, printers, and other devices. A wireless network offers the significant advantage of enabling you to build a computer network without stringing wires. Unfortunately, these systems usually come out of the box with the security features turned off. This makes the

network easy to set up, but also easy to break into. Most wireless networks use the 802.11 protocol, also known as Wi-Fi.

Security risks of using wireless data networks: Wireless networks have spawned a past-time among hobbyists and corporate spies called war-driving. The data voyeur drives around a neighborhood or office district using a laptop and free software to locate unsecured wireless networks in the vicinity, usually within 100 yards of the source. The laptop captures the data that is transmitted to and from the network's computers and printers. The data could include anything from one's household finances to business secrets.

Most home Wi-Fi access points, routers, and gateways are shipped with a default network name (known as an SSID) and default administrative credentials (username and password) to make setup as simple as possible. These default settings should be changed as soon as you set up your Wi-Fi network. In addition, some routers are equipped by default with "Guest" accounts that can be accessed without a password. "Guest" accounts should be disabled or password protected.

The typical automated installation process disables many security features to simplify the installation. Not only can data be stolen, altered, or destroyed, but programs and even extra computers can be added to the unsecured network without your knowledge. This risk is highest in densely populated neighborhoods and office building complexes.

Home networks should be secured with a minimum of WPA2 (Wi-Fi Protected Access version 2) encryption. Routers purchased in the last six years should include WPA2 security technology. Often, you have to specifically turn on WPA2 to use it. The older WEP encryption has become an easy target for hackers. Also, do not name your home network using a name that reveals your identity.

Setting up your home Wi-Fi access point can be a complex process and is well beyond the scope of this fact sheet. To ensure that your system is secure, review your user's manuals and web resources for information on security.

Two other useful guides can be found at:

- www.practicallynetworked.com/support/wireless_secure.htm
- http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

Security risks of using Wi-Fi hotspots: The number of Wi-Fi hotspot locations has grown dramatically and includes schools, libraries, cafes, airports, and hotels. With a Wi-Fi connection you can be connected to the Internet almost anywhere. You can conduct the same online activities over Wi-Fi as you could at home or work, such as checking email and surfing the web.

However, you must consider the risks to your privacy and the security of your laptop or netbook when using a Wi-Fi hotspot. Most Wi-Fi hotspots are unsecured and unencrypted. This is the major security risk of Wi-Fi. Even the expensive fee-based Wi-Fi service available in many airplanes may be as insecure as the free Wi-Fi offered at your corner coffee house. www.privatewifi.com/flying-naked-why-airplane-wifi-is-so-unsafe. Therefore, you must take additional steps to protect your privacy.

Secure surfing/SSL: When checking your email or conducting any important transaction, adding an "s" after "http" may give you a secured connection to the website (for example, https://www.gmail.com). Many webmail services provide this feature. This ensures that your login details are encrypted thereby rendering it useless to hackers. Although your email login may be encrypted, some webmail providers may not encrypt your Inbox and messages.

Check for SSL (Secure Sockets Layer) certificates on all websites on which you conduct sensitive transaction. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely.

Wi-Fi settings: Ensure that your computer is not set to automatically connect to the nearest available Wi-Fi access point. This may not necessarily be a legitimate connection point but instead an access point on a hacker's computer.

Disable file sharing: Make sure that file sharing is disabled on your computer to ensure that intruders cannot access your private files through the network. With file sharing enabled, it's possible for unauthorized individuals to access your files.

Firewall: Install a firewall on your computer and keep it enabled at all times when using Wi-Fi. This should prevent intrusion through the ports on the computer.

Security updates: Keep your computer's software and operating system up-to-date. This will help plug security holes in the software or operating system.

10.5. SAFELY DISPOSING OF YOUR COMPUTER

Before you donate, sell or discard your computer, you must take steps to insure that no trace of your personal data remains. Although you may not see them, hundreds of "deleted" files can be recovered with the right kind of software. When a file is deleted, it is not actually removed from the hard disk. All that is done is that a marker is set on the hard disk to indicate that the file is no longer available. The contents of the file are still present on the hard disk.

Therefore, in order to make sure that your data cannot be recovered, your hard drive must be either physically destroyed or scrubbed by a utilities program designed for this purpose. Hitting the delete button is not enough as anyone with minimum skills can easily retrieve the data. Likewise, reformatting your hard drive may delete the files, but the information is still there somewhere. Unless those areas of the disk are effectively overwritten with new content, it is still possible that knowledgeable attackers may be able to access the information.

The exact method you use to wipe your hard drive depends on whether you intend the hard drive to be reused. But no matter what your intent is, the hard drive should be completely clean before it leaves your hands.

Chapter 11:

Mobile Security

11. MOBILE SECURITY

11.0. INRODUCTION:

As our phones are becoming smarter and smarter, threats through mobile phones also becoming smart now-a-days. Mobile computing devices have become a critical tool in today's networked world. Enterprises and individuals alike rely on mobile devices to remain reachable when away from the office or home. While mobile devices, such as smartphones, laptops, personal digital assistants (PDAs) and Universal Serial Bus (USB) memory sticks have increased convenience, as well as productivity in the workplace, these benefits are not without risks. Many malicious programs have come which will try to get access over mobile phones and steal the personal information inside it.

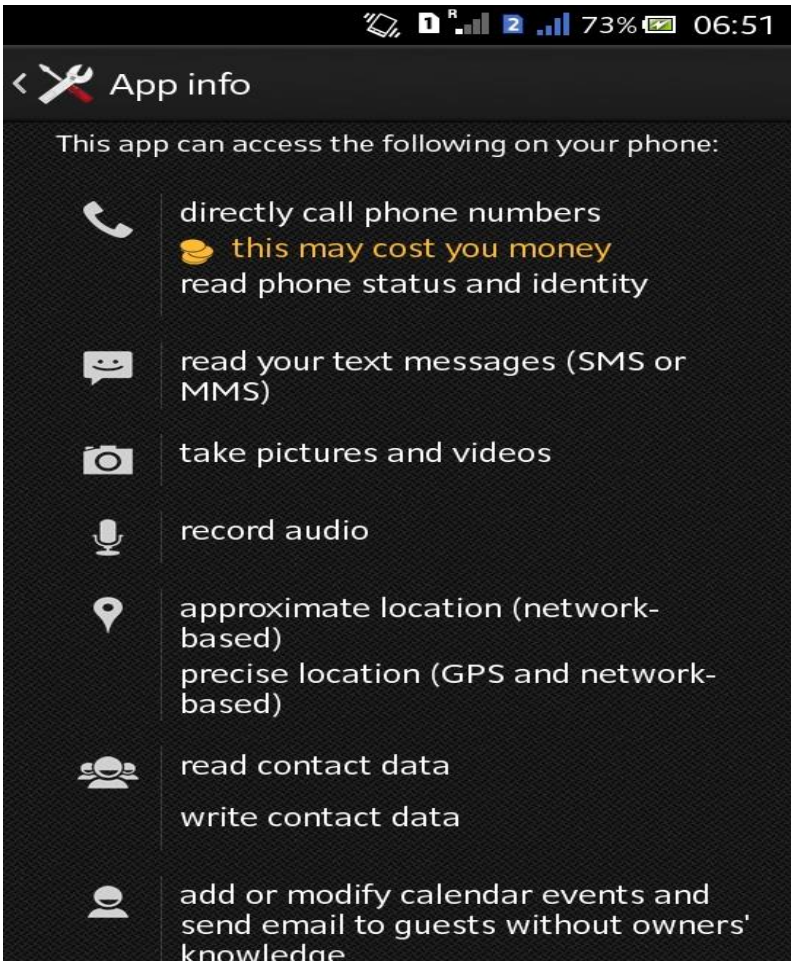
11.1. TYPES OF THREATS

Mobile threats have been classified into following categories: application-based threats, web-based threats, network-based threats and physical threats

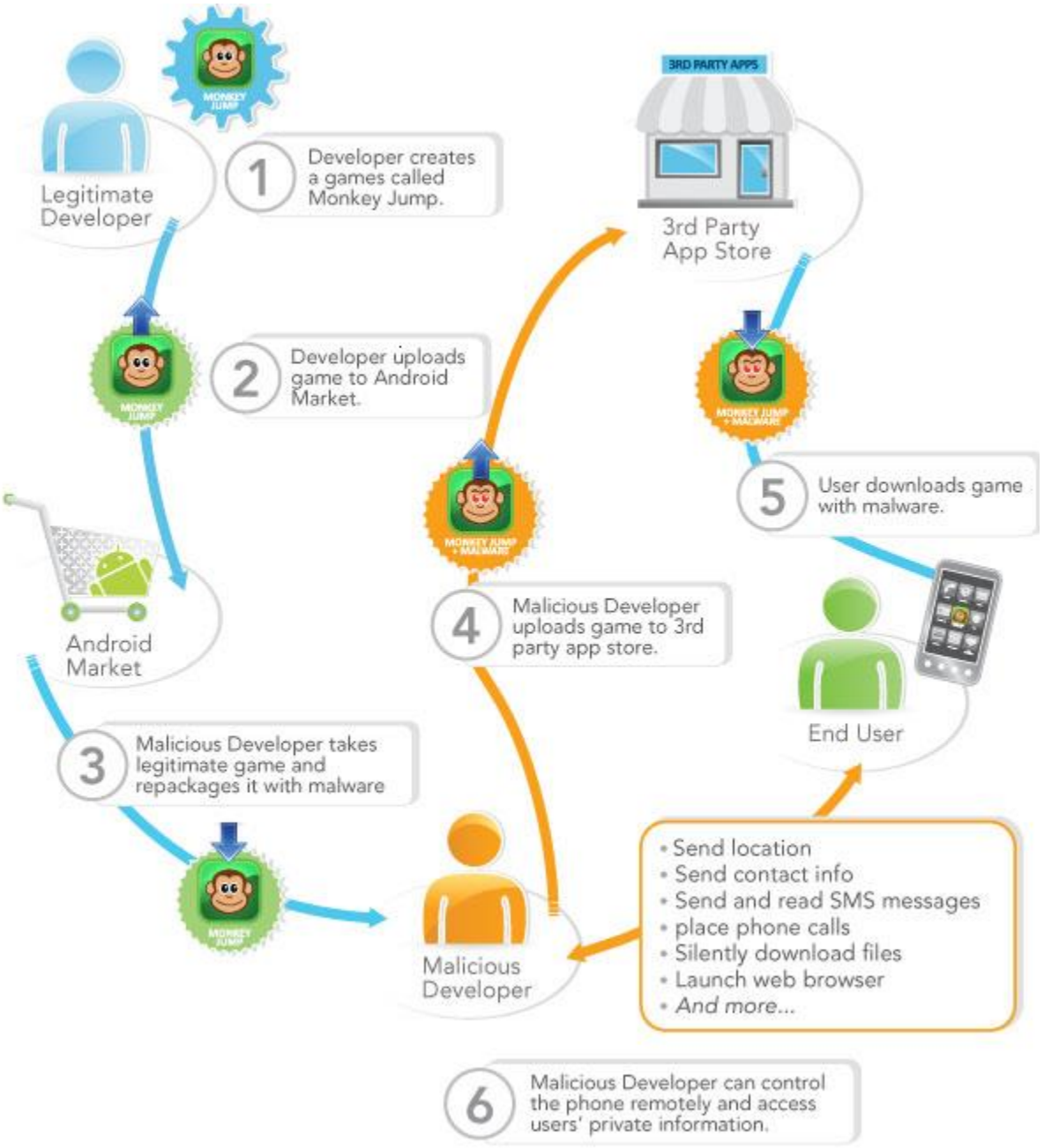
11.1.1 Application-Based Threats

Downloadable applications from trusted sites or through some 3rd party sites can present many types of security issues for mobile devices. "Malicious apps" may look fine on a download site, but they are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes. Application-based threats generally fit into one or more of the following categories: Malware is software that performs malicious actions while installed on your phone. Without your knowledge, malware can make charges to your phone bill, send unsolicited messages to your contact list, or give an attacker control over your device.

- Spyware is designed to collect or use private data without your knowledge or approval. Data commonly targeted by spyware includes phone call history, text messages, user location, browser history, contact list, email, and private photos. This stolen information could be used for identity theft or financial fraud.



- Privacy Threats may be caused by applications that are not necessarily malicious, but gather or use sensitive information (e.g., location, contact lists, personally identifiable information) than is necessary to perform their function.



- Vulnerable Applications are apps that contain flaws which can be exploited for malicious purposes. Such vulnerabilities allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, or download apps to your device without your knowledge.

11.1.2 Web-based Threats

Because mobile devices are constantly connected to the Internet and frequently used to access web-based services, web-based threats pose persistent issues for mobile devices:

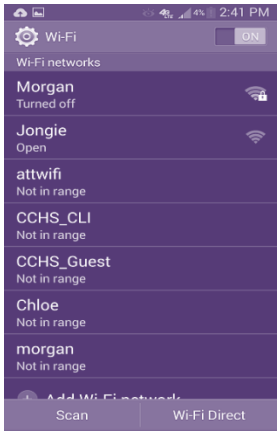
- Phishing Scams use email, text messages, Facebook, and Twitter to send you links to websites that are designed to trick you into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of your bank or other legitimate sources.
- Drive-By Downloads can automatically download an application when you visit a web page. In some cases, you must take action to open the downloaded application, while in other cases the application can start automatically.

- Browser exploits take advantage of vulnerabilities in your mobile web browser or software launched by the browser such as a Flash player, PDF reader, or image viewer. Simply by visiting an unsafe web page, you can trigger a browser exploit that can install malware or perform other actions on your device.

11.1.3 Network Threats

Mobile devices typically support cellular networks as well as local wireless networks (WiFi, Bluetooth). Both of these types of networks can host different classes of threats:

- Network exploits take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.
- Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the WiFi access point. Many applications and web pages do not use proper security measures, sending unencrypted data across the network that can be easily read by someone who is grabbing data as it travels.
- Bluejacking is sending nameless, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops.Bluejacking depends on the capability of Bluetooth phones to detect and contact another Bluetooth enabled devices.
- The Bluejacker uses a feature originally proposed for exchanging contact details or electronic business cards. He or she adds a new entry in the phone's address book, types in a message, and chooses to send it via Bluetooth.The phone searches for other Bluetooth phones and, if it finds one, sends the message.
- Despite its name, Bluejacking is essentially harmless. The Bluejacker does not steal personal information or take control of your phone.Bluejacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising.
- If you want to avoid such messages, you can turn off Bluetooth, or set it to "undiscoverable".



- Bluesnarfing is the theft of data from a Bluetooth phone. Like Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby.In theory, a Bluetooth user running the right software on their laptop can discover a Near by phone, connect to it without your confirmation, and download your phonebook, pictures of contacts and calendar.
- Your mobile phone's serial number can also be downloaded and used to clone the phone.You should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.

11.1.4 Physical Threats

Mobile devices are small, valuable and we carry them everywhere with us, so their physical security is also an important consideration.

- Lost or Stolen Devices are one of the most prevalent mobile threats. The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.

11.2. MITIGATION AGAINST MOBILE DEVICE AND DATA SECURITY ATTACKS

Do's and don'ts for Mobile Device

Do's:

6. Record IMEI number:

Record the unique 15 digit IMEI number. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

7. Enable Device locking:

Use autolock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict acess to your mobile phone.

8. Use a PIN to lock SIM card:

Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.

9. Use password to protect information on the memory card.

Report lost or stolen devices

- Report lost or stolen devices immediately to the nearest Police Station and concerned service provider. Use mobile tracking feature.
- Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen. Every time a new SIM card is inserted in the mobile phone, it would

automatically send messages to two preselected phone numbers of your choice, so that you can track your Mobile device.

Don'ts:

• Never leave your mobile device unattended.

• Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

Do's and Don'ts for Data Security:

Do's:

- Backup data regularly

Backup data regularly and set up your phone such that it backs up your data when you sync it. You can also back up data on a separate memory card. This can be done by using the Vendor's document backup procedure.

- Reset to factory settings:

Make sure to reset to factory settings when a phone is permanently given to another user to on sure that personal data in the phone is wiped out.

11.3. MITIGATION AGAINST MOBILE CONNECTIVITY SECURITY ATTACKS

Bluetooth:

Bluetooth is a wireless technology that allows different devices to connect to one another and share data, such as ringtones or photos. Wireless signals transmitted with Bluetooth cover short distanes, typically 30 feet (10 meters).

Do's:

- Use Bluetooth in hidden mode so that even if the device is using Bluetooth it is not visible to others.
- Change the name of the device to a different name to avoid recognition ofyour Mobile phone model.

Note: The default name will be the mobile model number for Bluetooth devices.

- Put a password while pairing with other devices. The devices with the same password can connect to your computer
- Disable Bluetooth when it is not actively transmitting information.
- Use Bluetooth with temporary time limit after which it automatically disables so that the device is not available continuously for others.

Don'ts:

1. Never allow unknown devices to connect through Bluetooth.
2. Never switch on Bluetooth continuously.
3. Never put Bluetooth in always discoverable mode.

Note: Attackers can take advantage of its default always-on, always discoverable settings to launch attacks.

11.4. MOBILE AS Wi-Fi:

Wi-Fi is short for "Wireless Fidelity." Wi-Fi refers to wireless networking technology that allows computers and other devices to communicate over a wireless signal.

Many mobile devices, video game systems, and other standalone devices also include Wi-Fi capability, enabling them to connect to wireless networks. These devices may be able to connect to the Internet using Wi-Fi.

Do's:

- Connect only to the trusted networks.
- Use Wi-Fi only when required. It is advisable to switch off the service when not in use.
- Beware while connecting to public networks, as they may not be secure.

Don'ts:

- Never connect to unknown networks or untrusted networks.

11.5. MOBILE AS USB:

The mobile phones can be used as USB memory devices when connected to a computer. A USB cable is provided with the mobile phone to connect to computer. Your mobile's phone memory and memory stick can be accessed as USB devices.

- Your mobile's phone memory and memory stick can be accessed as USB devices.

Do's:

1. When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti-virus.
2. Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.
3. Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Don'ts:

1. Never keep sensitive information like user names/passwords on mobile phones.
2. Never forward the virus affected data to other Mobiles.

11.6. MITIGATION AGAINST MOBILE APPLICATION AND OPERATING SYSTEM ATTACKS

Application and Mobile Operating System:

1. Update the mobile operating system regularly.
2. Upgrade the operating system to its latest version.
3. Always install applications from trusted sources.
4. Consider installing security software from a reputable provider and update them regularly.
5. It's always helpful to check the features before downloading an application. Some applications may use your personal data.
6. If you're downloading an app from a third party, do a little research to make sure the app is reputable.

11.7. CASE STUDIES:

- Apple has admitted that they have deleted songs from the iPhone users who have downloaded songs from other sites rather than iTunes.
- Sachin was wondering why the deleted photos are showing again in the gallery once he restarts his mobile phone, later he came to know that he had installed apps from a 3rd party app store and that application had the access to delete or modify his memory card data.
- Once in a threat bomb attack, police have identified from whom they received the call and enquired him but the suspect told the police that he had lost his mobile one month back and he didn't block his phone or made any complaint to police regarding it.
- Rohit mobile data have reduced a lot within a single day ,when he checked his phone he came to know that unknowingly he has switched on the option that makes his phone to act as a Wi-Fi access point and that to without any authentication.
- Sneha and vasundara shared their tour photos through Bluetooth in their college then sneha received e-mails which contains morphed images of her. Later through police enquiry they came to know that their photos have also been shared to rohit because they made their visible to all nearby devices.

Chapter 12:

Wireless Security

12. WIRELESS SECURITY

12.0. INTRODUCTION TO WLAN

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

WLANs have become popular due to hassle free installation and mobility where a user can move to any place (within the range of the WLAN) and still be connected to Network at office or home.

12.1. WI-FI SECURITY

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points (wireless routers).Anyone in the range of Access point can connect to an Access Point if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victim's computer to get long term control on it through Internet, etc.

All these criminal acts will naturally be associated with the legal user of Access Point (wireless router). It is up to the legal user of the Access Point to defend him to prove that he has not been involved in these acts. It now becomes the responsibility of the user to secure his/her own Access Point.

12.2. DIFFERENCE BETWEEN WLAN AND WIFI

WI-FI and WLAN are used interchangeably by most of the people today. But the difference between WLAN and **WI-FI** are as stated below:

WLAN or Wireless LAN is a way of transmitting data between multiple computers in a LAN with radio waves within a distance of few meters. WLAN offers point to point communication between LAN to WLAN, WLAN to WLAN and WLAN to LAN.

Wireless Fidelity in short called as **WI-FI** is WI-FI is a trademark name to brand devices compliant to IEEE 802.11 standards i.e. WLAN devices. They test the interoperability between various Vendors.

12.3. WIRELESS OPERATING MODES:

1. Station (STA) Infrastructure Mode
2. Access Point Infrastructure Mode
3. Ad-hoc Mode
4. Monitor Mode

12.4. TYPES OF ATTACKS ON WIRELESS ENVIRONMENT:

DENIAL OF SERVICE ATTACK

Denial of Service Attack aims at preventing the users from accessing the network resources. In a Wireless network, denial of service attack can be applied in various ways.

MAN-IN-MIDDLE ATTACK IN WI-FI DEVICES

Performing Man-In-Middle Attack in a wireless network is much easier, when compared to wired network. As the transmissions from an access point are broadcasted, it is easy for an unauthorized user to collect the traffic sent by other wireless clients. And the process of collecting the packets in this manner is known as Eavesdropping.

Also the third party user can manipulate the packets sent to the legitimate users which results in breaking the user's privacy. So In order to avoid these kinds of attacks, Strong encryption should be used for transmitting the data between wireless client and access point.

WAR DRIVING

It is a process of tracking Wi-Fi hotspots located at a particular place, while moving with a hand held device or a laptop in a vehicle. This helps the user in finding out the access points that does not use encryption and takes control over it for performing the attacks on the network.

12.5. HOW THE ATTACK OCCURS IN WI-FI ENVIRONMENT?

- At the physical layer of TCP/IP Model, denial of service attack can be implemented by introducing a device which will generate noise in the same frequency band in which wireless access point is operating. This makes the users who are trying to connect to the access point may not be able to connect to it.
- Also the other possibility of Denial of service Attack is spoofing the access point. Normally wireless clients connect to the wired network with the help of an access point. For associating with the access point they require SSID of it.

- When an unauthorized user places an access point with the same SSID, then there is a chance of authorized user getting associated with the attacker's access point. If that happens, the attacker will try to collect sufficient number of packets from the wireless client and cracks the WEP key used by the legitimate access point.
- Then the attackers gets associated with the legitimate access point and generates large ping requests in the network or generate some abnormal traffic, which may finally result in Denial of Service Attack.

12.6. TIPS FOR SECURING WIRELESS COMMUNICATIONS

- Always use strong password for encryption
- A strong password should have at least 15 characters, uppercase letters, lowercase letters, numbers and symbol.
- Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.
- Do not use WEP for encryption, rather use WPA/WPA2.
- Always use the maximum key size supported by access point for encryption
- If the key size is large enough, then it takes more time to crack the key by the hacker. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.
- Isolate the wireless network from wired network with a firewall and a antivirus gateway.
- Do not connect the access point directly to the wired network. As there is a chance of compromised wireless client in turn affecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the accespoint and the wired network.
- Restrict access to the Access Point based on MAC address
- In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
- Change the default username and Password of the Access Point
- Most of the users do not change the default passwords while configuring the Access Point.
- But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
- Shutdown the Access Point when not in use, Hackers try to brute force the password to break the keys, so it is good practice to turn off the Access points during extended periods of Non-use
- Do not broadcast your network name, SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information.
- Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- Always maintain a updated firmware and Updating the firmware of access point is recommended, as it will reduce the number of security loop holes in the access point.

- Use VPN or IPSEC for protecting communication
- When the information flowing from wireless client to the wired network receiver is critical, then it is recommended to use VPN or IPSEC based communication so that the information is protected from sniffers in the network.
- Do not make the SSID information public
- SSID information is used to identify a access point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- Disable DHCP service: When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.
- Disable SSID broadcasting in wireless access point.
- Never auto-connect to open Wi-Fi networks in public places.
- Do not use copyrighted software without the author's permission.
- Set BIOS password to prevent unauthorized users from rebooting and manipulating your system
- Switch off the Internet modem when not in use
- Secure your wireless communication with additional network security such as SSH, or VPN, or SSL tunneling and turn off the wireless devices when not in use.
- Immediately report lost or stolen items like laptops, mobile, USB keys and ID cards to the competent authorities.
- Reject all the unexpected pairing requests for Bluetooth devices.
- Dial 112 your mobile will search any existing network to establish the emergency number for you interestingly this number 112 can be dialed even if the keypad is locked

12.7. SECURITY FEATURES IN WLAN:

WLAN in more vulnerable compared to traditional Ethernet based wired technology since any unauthorized user within the range of a Wireless Network can access and seamlessly use their network if proper security is not implemented.

The confidentiality of the data transmitted will be at risk in such environments. WLAN Security Standards have been implemented to provide confidentiality and integrity to the data transmitted over wireless.

12.8. WLAN SECURITY STANDARDS

Name	Year	Who Defined It
Wired Equivalent Privacy (WEP)	1997	IEEE

Name	Year	Who Defined It
The interim Cisco solution while awaiting 802.11i	2001	Cisco, IEEE 802.1x Extensible Authentication Protocol (EAP)
Wi-Fi Protected Access (WPA)	2003	Wi-Fi Alliance
802.11i (WPA2)	2005+	IEEE

Siting this issue Wireless Technologies have implemented various Encryption and Authentication techniques to protect the data transmitted over the wireless network. Following Security Algorithms are used to protect the confidentiality of the data transmitted over wireless Network:

1. WEP (Wired Equivalent Privacy)
2. WPA (Wi-Fi Protected Access)
3. WPS (Wi-Fi Protected Setup)

WEP (Wired Equivalent Privacy):

WEP the original Security Standard used to maintain the confidentiality of the data transmitted over the wireless networks. Introduced as part of the original 802.11 standard in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, was widely in use. WEP uses the following Encryption and Authentication mechanisms:

ENCRYPTION:

- WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 check-sum for integrity.
- Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. Size of the key was restricted in the initial draft made for this standard.
- Once the restriction over the size of the key is removed its extended versions have been used to increase the strength of the WEP namely WEP-128bit, WEP-256bit.
- A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters. 26 digits of four bits each give 104 bits; adding the 24-bit IV produces the complete 128-bit WEP

key.

- CRC is used to verify the integrity of the Data transmitted over the network

AUTHENTICATION:

WEP provides two type's authentication mechanisms that can be used give Wireless Network access to authorized users.

Note:-Infrastructure mode will be used for understanding the authentication process. Wireless LAN Clients and an Access Point are the two terminologies will be used to explain the below methods.

A) Open Authentication

WLAN Client can directly access the Access Point without providing any credentials to associate with the Access Point. Once associated with the Access Point the data frames transmitted by client will be the encrypted using WEP keys.

B) Shared Key Authentication

WLAN Client will need to provide credentials to connect to the Access point. A Four Step Challenge-Response Handshake is used to authenticate the client.

A. The client sends an authentication request to the Access Point.

B. the Access Point replies with a clear-text challenge.

C. The client encrypts the challenge-text using the configured WEP key, and sends it back in another authentication request.

D. The Access Point decrypts the response. If this matches the challenge-text the Access Point sends back a positive reply.

Once on successful Authentication and Association with the Access point the pre-shared key will be used to encrypt the Data Frames.

It might look like Shared Key authentication is more secured than Open System authentication, but it is quite the reverse. It is possible to derive the key stream used for the handshake by capturing the challenge frames in Shared Key authentication. Therefore, data can be more easily intercepted and decrypted with Shared-key authentication than with Open System authentication.

If privacy is a primary concern, it is more advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication; however this also means that any WLAN client can connect to the AP. (both authentication mechanisms are weak; Shared Key WEP is deprecated in favor of WPA/WPA2.)

12.9. COMMON ATTACKS IN WEP:

- Since RC4 is a Stream Cipher no two keys can be same but with Initialization Vectors of only 24bit length there is possibility of generating same keys after every 5000 packets made it possible for attackers to crack the WEP encryption.
- Attackers could successfully generate more packets when the network traffic is very low using various replay attacks to generate traffic.
- Attackers have successfully exploited WEP and many free tools are available in the Internet that can do the same.

WPA (Wi-Fi Protected Access):

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy)

WPA is referred to as 802.11i Standard is made available in 2003. To improve the security and complexity of the encryption WPA2 was improved and made available in 2004.

Encryption (WPAv1):

- ✧ WPA follows a different Encryption standard than WEP. It uses **Temporal Key Integrity Protocol (TKIP)** for encrypting the data frames.
- ✧ In WEP the key used for encrypting in the data frames in constant and should be manually entered into the Access Points. But TKIP operates in a dynamic manner creating **per packet based keys** generating new 128-bit key for every packet.
- ✧ The above method eliminates risks that occurred with WEP.
- ✧ WPA also includes Message Integrity Check to protect the integrity of the data. It is designed to prevent an attacker to capture, alter or re-send the packets.
- ✧ ***Michael*** is an algorithm used to verify the integrity of the messages which is stronger and more efficient than CRC used in WEP.

Encryption (WPAv2):

- ✧ TKIP used in WPA was significantly stronger but packets of short length can be decrypted (like ARP Messages). This is exploited using the same flaw in WEP but doesn't reveal a key but only the key stream used to encrypt the data.
- ✧ WPA2 uses Counter Cipher Mode with block chaining message authentication code Protocol **(CCMP)** an AES based encryption mode to encrypt the data packets.
- ✧ To achieve high bit rates of 54Mbits/s i.e. 802.11n standard specified this encryption protocol must be enabled.

Authentication (WPAv1 & WPAv2):

- ✧ WPA supports both Shared Key and 802.1X standard to use complex authentication servers.
- ✧ Pre-Shared Key **(PSK)** or Personal Mode can use at home and small networks. A **ASCII character of length 8 to 63** or **Hexadecimal String of 64 digits** can be inserted in the access point to use for authentication.
- ✧ If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.

- ✧ Authentication servers like Radius servers etc., can be used to maintain the credentials for authorized users rather than sharing a single key across all clients.

WPS (Wi-Fi Protected Setup):

WPS is designed in view to simply the configuration to easily connect to the Wireless Home Network. But it is prone to Brute Force attack which could easily be exploited if the access point is not safe guarded.

- ✧ This leads to a serious Vulnerability since it exits with WPA and WPA2 protocols an attacker can easily bypass them any can even obtain the **Pre-Shared Key** used for authenticating WLAN clients in WPA and WPA2.
- ✧ The access points with no support for WPS are not affected by this kind of Brute force attack.
- ✧ It is advisable to disable support for WPS if your access points given an option to disable since some of them have no option to disable it.
- ✧ Firmware upgrades have been released by many vendors to disable the WPS support in their access points.

12.11. REFERENCES:

http://en.wikipedia.org

http://www.ciscopress.com/articles/article.asp?p=791594&seqNum=5

12.12. CASE STUDIES:

Let's see some real incidents that took place in the recent years.

- Terrorists and hackers used unsecured Access Points to perform illegal activities on the Internet.
- Hackers penetrated into open Wi-Fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private emails sent by the guests.

- The hackers then attempted to extort money from the hotel chain by threatening to publish the emails.(www.abczyz.in)
- Just 5 minutes before Delhi blasts on September 2008 terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai to send terror emails to authorities and news channels.
- These hackers do not leave a trail of footprints for the investigators to arrive at a logical conclusion. The audit trail ends at Wi-Fi Access Point of the legal user.
- So it is becomes imperative for the users to secure their own Access Points (wireless router). The following are the steps to secure an Access Point.

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events, etc.,

For more details visit
www.infosecawareness.in

Ministry of Electronics & Information Technology,
Government of India

सी डैक CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय का वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India