Jan – Mar 2010

www.infosecawareness.in

Information Security Awareness

Program by
Information Security Education and Awareness (ISEA)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India

MOBILE BANKING TIPS

- Set up a PIN/password to access the handset menu on your mobile phone.
- Delete junk messages and chain messages regularly.
- Do not follow any URL in messages that you are no sure about.
- If you have to share your mobile with anyone else or send it for repair/maintenance.
  - Clear the browsing history
  - Clear cache and temporary files
  - Block your mobile banking application by contacting your bank and unblock them when you get the mobile back.

InfoSec Tip

Do not allow Internet Browsers (IE, Mozilla, Safari etc) to store passwords for you.

Internet browser (for example Microsoft Internet Explorer, Mozilla Firefox, Apple Safari browsers etc) have the option to store passwords but stored passwords allow anyone who access your machine to log in to your web accounts. In addition, there are numerous utilities that can expose hidden information and reveal the password. If the same password has been used for other logins, many systems or web sites could be compromised.

Guidelines for using Internet Browser

- Always maintain an operating system with all security patches or updates installed.
- Update the web browser before browsing the net.
- Block popup windows while browsing Internet. Some pop-up messages may contain helpful information but in cases they are advertisements with some hidden code introduced by a hacker.
- Always clear private data after completing Internet browsing and do NOT save your login information.
- Never click links in your web based e-mails and always type that address in URL.

InfoSec Quote

When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.

— David Brin

InfoSec Cartoon

Encourage children to gain knowledge from Internet and use Internet wisely.

Executed by :
Center for Development of Advanced Computing
Hyderabad

InfoSec Quiz

1) **Which of the following is an example of strong and easy to remember password ?**
(a) cdachyd (hint: C-DAC Hyderabad)
(b) password (hint: password)
(c) my@123 (hint: my generic password)
(d) Mdni$aslc9 (hint: My daughter name is Saathia and she loves chocolates and S=$ and a favourite random number)

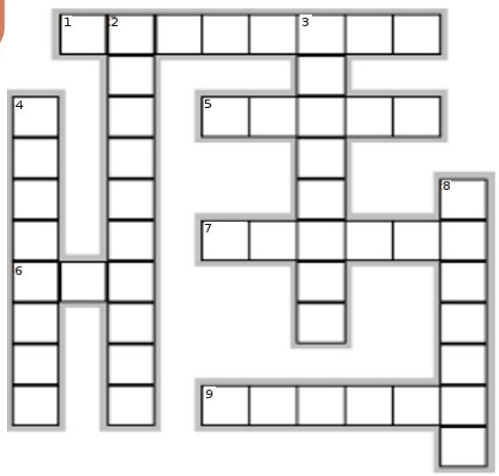
2) **If you have a firewall on your network you don't need to turn on your Desktop firewall.**
(a) True
(b) False

3) **You just got a brand new computer and it has anti-virus software installed. Is it safe to connect to the Internet?**
(a) Sure, They wouldn't sell something which is unsafe
(b) No, it might be pre installed and not updated. So I may use only after installation of latest patches
(c) Yes, I believe the product which I bought will scan for viruses immediately
(d) It is safe to use

4) **If you ever receive an unsolicited telephone call from someone claiming to need your account details such as username and password, what would you do?**
(a) Refuse and report immediately
(b) Submit the details related to username and password to Bank through mail
(c) Tell him/her about your personal details
(d) Submit the details through post or walk in to the concerned office

5) **What are the possible consequences of someone breaking into your computer ?**
I. Your files may be deleted.
II. Your personal information may be exposed to the attacker.
III. Your monitor will be shattered and not available.
IV. Your computer may be utilized for a cyber crime.
(a) All of the above
(b) I, II, III are True
(c) I, II, IV are True
(d) I, III, IV are True

InfoSec Crossword



ACROSS

1. The process of recreating files which have disappeared, or corrupted, from backup copies
5. Similar to a 'Fix', a _____ is a temporary arrangement used to overcome software problems or glitches.
7. A mechanical device used by software developers to prevent unlicensed use of their product
6. Short for Robot, - the term describes little programs designed to perform automated tasks on the Internet
9. An individual whose primary aim in life is to penetrate the security defences of large, sophisticated, computer systems

DOWN

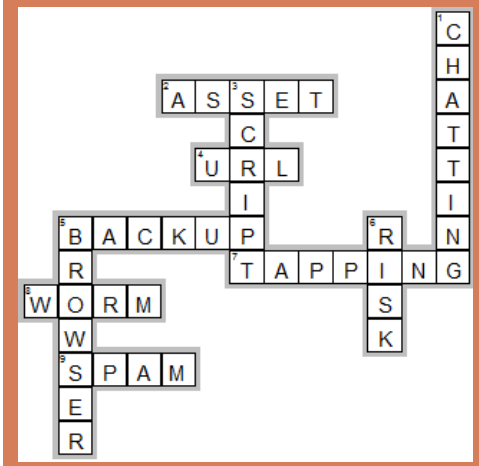
2. _____is the transformation of data into another usually unrecognisable form
3. An _____ is a private network which uses the Internet protocols and extends beyond an organisation's premises
4. A collection of files, tables, forms, reports, etc., held on computer media that have a predictable relationship with each other for indexing, updating, and retrieval purposes
8. The human nervous system, as opposed to electronic computer hardware or software

Sep '09 Dec '09 Contest Answers

InfoSec Quiz

1) B 2) D 3) C 4) C 5) B

InfoSec Crossword



Logon to
www.infosecawareness.in
to participate in the
InfoSec Contest

Congratulations
Last Edition Contest Winners

InfoSec Crossword
Mr. G. Praveen Kumar
Hyderabad

InfoSec Quiz
Mr. Ashish Thapar
Gurgaon

InfoSec Virus Alert

Net-Worm.Win32.Kido **Status : moderate risk**

Kaspersky Lab has detected that multiple variants of Kido, a polymorphic worm, are currently spreading widely.

Net-Worm.Win32.Kido exploits a critical vulnerability (MS08-067) in Microsoft Windows to spread via local networks and removable storage media. It has already infected around 610534 computers during the month of December'2009 and stood first in top 20 viruses.

The worm disables system restore, blocks access to security websites, and downloads additional malware to infected machines.

Users are strongly recommended to ensure their antivirus databases are up to date. A patch for the vulnerability is available from the following Microsoft link.
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

InfoSec News

Terrorists' new target - Hiring unemployed techies

Bangalore: At the time of recession, when most of the top IT companies slashed lakhs of jobs techies were forced to take a different step to earn money and joined different terrorists groups across the world. Indian security agencies say that the recruitment of techies was maximum in 2009 when recession hit the world.

According to the research done by, European sociologists Diego Gambetta and Steffen Hertog, who surveyed over 400 terrorists, including 25 men involved in the 9/11 attack, it was found that 44 percent were engineers. Intelligence Bureau (IB) said that that recruiting techies for terror operations has become quite a common phenomenon the world over.

It was first started by the Al Qaeda when it undertook the 9/11 attack. However, the Lashkar was quick to pick up this plan and gradually the Students Islamic Movement of India and the Indian Mujahideen, too, followed suit.

For more details,
http://www.siliconindia.com/shownews/Terrorists_new_target_Hire_unemployed_techies_-nid-64463-cid-1.html

Microsoft warns of IE bug used in Chinese attacks on Google

Microsoft has issued Security Advisory (979352) after its own investigations into the highly-organized hacking attack in late December, the one that Google earlier this week attributed to China, led the software giant to conclude that a Remote Code Execution (RCE) vulnerability in Internet Explorer was used by the perpetrators.

"The company has determined that Internet Explorer was one of the vectors used in targeted and sophisticated attacks targeted against Google and other corporate networks," a Microsoft spokesperson told Ars. "Microsoft continues to work with Google, other industry partners and authorities to actively investigate this issue. To date, Microsoft has not seen widespread customer impact, rather only targeted and limited attacks exploiting IE6."

For more details
http://arstechnica.com/microsoft/news/2010/01/microsoft-warns-of-ie-security-flaw-used-in-google-at
http://www.microsoft.com/technet/security/advisory/979352.mspx

MOBILE DEVICES SECURITY

InfoSec Concept (s)

In 2009, some surveys on Mobile usage and telecommunications reveal that there are 3.3 billion subscribers worldwide, out of which 375 million mobile subscribers are Indians. The survey also says that around 63 million urban users access Internet by using their phones on monthly basis and 16 million urban users do so on daily basis in India. Mobile phones are commonly used for checking e-mails and searching for information using search engines. Children in India have a great influence in the purchase of mobile phones according to the survey. Indians ranked the highest among Asian countries in shooting voyeuristic pictures with their mobile phones. People in India are not only using mobile phones for talking and messaging, but also for downloading and sharing music, playing games and watching videos. 32% Indians believe that giving out mobile phone details on social networking sites and forums is okay. 68% of Indian parents who have children between the ages of 7 – 15 years buy their children their first new phones while only 20% hand down their used phones to their kids.

The latest generation of mobile phones offers users exciting new capabilities. Smart Phones typically allow access to the internet and email. They usually have an operating system similar to that of a personal computer. Many Smart phones allow users to download third-party applications.

However, asmobile phone forInternet access for e-mails, Social networking, downloading applications and usage in these advanced capabilities also mean that there is an increased risk of information on your phone being , Your phone could even infected by malicious software. In addition, if your phone is lost or stolen, your personal information including passwords, banking details, emails and photos could be put tounlawful and criminal use.

The following are Symptoms of malicious software infection

- ✔ There is a large increase in your phone bill with no clear reason
- ✔ Your Mobile phone suddenly restarts or hangs
- ✔ Your phone has emails and messages in the sent folder that you did not send
- ✔ The user interface (colors, background images etc) has changed without your taking any action to change it

Most phones include browsers that allow the user to surf the Internet, and many mobiles now have the capability for the user to watch television, videos, and photos on Internet. While this is an appealing feature for children or youngsters, Internet access on a mobile phone carries some risks

- Like personal computers, mobile phones with Internet capability are vulnerable to spam, viruses and other malicious content
- Sharing the Mobile Phone numbers at social networking sites or forums may affect your privacy and that of your family.
- Photos/videos sent to other users can be reproduced, altered, or posted online without the subject's consent or knowledge and the same can disclose a user's appearance and location
- Text messages/IMs containing private, personal information could be sent to the wrong address
- Children/youngsters whose mobile phones do not feature unlimited Internet access could prove to be costly to their family
- A child / youngster could receive harmful or unwanted text messages and/or spam text messages which could contain inappropriate material
- Can have an impact on learning at school if restrictions aren't placed upon cell/Mobile phone use

Some key risks involved with Internet access by mobile phone

What can parents do to reduce the risks associated with their child / youngster's accessing the Internet Using a mobile phone ?

Safeguarding your child from mobile phone usage requires more than just knowing the technology—parents need to educate themselves regarding online content that poses to be the greatest threat to their child/adolescent. What is being said or sent via the Internet can pose an even bigger concern than the technology itself.

Many risks are associated with mobile phone usage .It may lead to contact with unknown individuals Children are keen to carve out their own friendships and relationships, but doing so by mobile phone carries its own risks . Children also tend to experiment with mobiles trying to test some applications and may appear to be well-versed with its usage .Still parents need to insist on safer access to Internet. Also as Internet is across boundaries and cultures, it is the duty of the parents to guide children on how to communicate with others on Internet and respect others culture.

Children or youngsters may establish their relationships online through mobile phones or wired Internet . Relationships can develop rather quickly and the child or youngster may be invited to personal meetings as part of social networking and they may proceed to do so without realising the need for safety precautions. Parents therefore need to monitor their usage of Internet over mobiles .

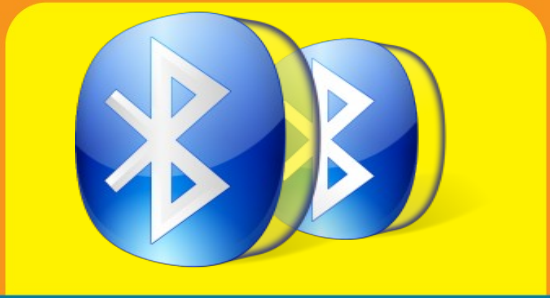
Tips for Securing Mobile Phones / Smart Phones

- **Always use strong passwords and maintain the same** as mobile phones allow users to set a password or Personal Identification Number (PIN) that must be entered to use the phone. Passwords and PINs make it more difficult for thieves to steal your personal information if your phone is lost or stolen.
- **Keep your Bluetooth connectivity in invisible or hide mode** as Bluetooth lets you wirelessly connect to devices and transfer information over short distances. It is best to leave your phone in hidden mode, so that it is only visible when you specifically need other people or devices to see it.
- **Be smart with WiFi.** When connecting to the internet using WiFi, try to use an encrypted network that requires a password
- **Be wise while clicking the links in your mobile Internet as** also opening multimedia messages (MMS) or attachments in emails, or clicking on links in emails and SMS messages Never open them unless you are expecting them and they are from a trusted source. They could contain malicious software or take you to a malicious website.
- **Check for updates to your phones operating system regularly.** Install them as soon as they are available. These updates contain changes that will make your phone more secure.
- **Install security software from a reputable provider.** Anti-virus and firewall software is available for some mobile phone operating systems. Check with your phone manufacturer for recommendations.
- **Be careful when downloading applications from the Web.** Smart phones have Internet browsers that let you surf the web and download content to the phone. Do not download content such as applications from an unknown or unreliable source. They could contain malicious software.
- **Back up your data regularly.** Set up your smart phone so that it backs up all your data each time you connect with a computer or a secured web site. Alternatively, backup your device to a memory card regularly and keep it in a safe place.
- **Encrypt your data.** Some smart phones allow you to encrypt the data stored on your phone or memory cards through the use of third-party encryption products.

Bluetooth Technology

The Bluetooth technology is a wireless communication that operates as radio waves, using a band set at 2.4GHz. This frequency is available at no charge. The Bluetooth technology allows two devices to connect wirelessly with each other, and incorporates the use of "Centrino" chips. These chips are available easily in most standard electronic devices such as laptops, cellular phones, computers, headsets, etc.

There are many advantages of using Bluetooth wireless technology. The most important is the fact that any two devices can be connected with each other without the use of any cables or wires in short distance of 10 meters.



Attacks on Bluetooth Technology

Bluejacking - Bluetooth devices have the ability to send so-called wireless business cards. A recent trend has been to send anonymous business cards with offensive messages, . But it doesn't put data in jeopardy. Bluejacking requires an attacker to be within 10 meters of a device. If someone bluejacks you, you could probably see his face. Never add bluejack messages to your contacts list. And to avoid the nuisance altogether, simply put your phone on non discoverable mode

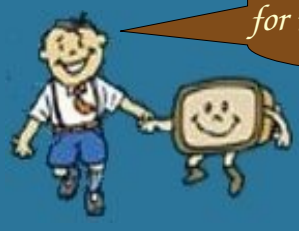
Bluesnarfing - is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages and on some phones users can copy pictures and private videos

Bluebugging - is a form of Bluetooth attack often caused by a lack of awareness. It the most serious threat of all. A hacker has the ability to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet

Denial of Service (DoS) - attacks occur when an attacker uses his Bluetooth device to repeatedly request pairing with the victim's device. Unlike on the Internet, where this type of constant request can bring down services, a Bluetooth DOS attack is mostly just a nuisance, since no information can be transferred, copied or attained by the attacker.

Tips for avoiding above attacks

- It is suggested that mobile users antivirus, firewall, data encryption technologies for their mobile devices such as phones, laptops etc
- Turn off Bluetooth when you do not need that service
- You may keep your Bluetooth connection in invisible or hidden mode as your device ID is not visible to others
- Never accept and run attachments from unknown resources unless you are expecting them
- Always keep the connectivity by using password with large number of digits and change default password



Visit www.infosecawareness.in for more details

InfoSec Tools

LAPTOP PHYSICAL SECURITY TOOLS

As number of surveys revealed about the number of laptops (In 2003, an estimated 1.5 million laptops were stolen worldwide. Today, that number has climbed to 2.6 million—a 70% increase in just a few years) that go missing every year and what can we do to be more proactive?

One solution might be using recovering software tools that automatically informs through a SMS or dialling your telephone and help you and the authorities (Kind of Tracking Software). The following Tools may help in this regard.

ZTRACE GOLD is an invisible software security application that traces the location of missing laptops for recovery (http://www.ztrace.com)

MyLaptopGPS protects laptop assets for all types of organizations and individuals with a proven multi-layered approach to laptop security (http://www.mylaptopgps.com)

PC PhoneHome is our multi-award winning software product that tracks and locates lost or stolen laptop and desktop computers. http://www.pcphonehome.com)

A second alternative is to look at central monitoring and image automation tools, such as **Symantec's Altiris (** http://www.symantec.com/business/theme.jsp?themeid=altiris) and **Kaseya** (http://www.kaseya.com/) that can be used in a stolen laptop situation.

The above tools are just part of an overall laptop security solution that should also include disk encryption and password-protecting your boot drive. If these tools live on your hard disk and if you haven't enabled a firmware or disk password, any intelligent thief can just reformat your hard drive and remove this protection, or just remove the hard drive itself. So it makes sense to start by putting password protection on all of your machines as first line of defence. Disk encryption is especially important if you need to protect confidential corporate or business data, not to mention your own personal data, such as bank account passwords, as well

SOME SECURITY TOOLS

Virus Protection & Cleaner Tools

- ***Windows based***
  - Avast Home Edition
  - AVG free edition
  - Avira Antivir Personal Edition Classic
  - Bit defender 10 free edition
- ***Linux based***
  - Avast Home Edition
  - AVG Free Edition
  - Calmtk

OS Updates & Patches

- Security Update Solution Tools
- Windows based tools
- Updates
- Microsoft Update
- Microsoft Office Update

Security Update detection tools

- Microsoft Baseline Security Analyzer (MBSA)
- Microsoft Office Visio 2007 Connector

Guess the tip which suits the above cartoon picture & win prizes.

Logon to www.infosecawareness.in *to send the tip.*

InfoSec Workshops – Dec '09 / Jan '10

Information Security Trainers Training

@ Hyderabad
@ Uppal
@ Visakhapatnam
@ Mohali

→ **324 Members Participated**

Information Security Awareness to Students

@ Secunderabad
@ New Delhi
@ Hyderabad
@ Visakhapatnam
@ Rourkela
@ Mohali
@ Chandigarh

→ **935 Members Participated**

Information Security Awareness to Others

(NGO's / CSI Operators, Air Force, Govt. Employees)

@ Shimla
@ Chandigarh
@ Krishnagiri
@ Tiruvannamalai

→ **400 Members Participated**

InfoSec Comments & Reviews

Got to know many new technologies in the computer field

- P. Rajini, Teacher
Sreenidhi International School

The information is really useful for us as parents and teachers.

-Mrs.Azuba, Teacher
NTPC, Ramagundam

Useful in getting aware of information security problems and their possible ways to get protected from them.

-P. Sravan Kumar, Teacher
JNV, Srikakulam

The seminar was wonderful and we would like to participate in many more seminars like this

- Harshad Reddy, Student
KV, Picket, Secunderabad

It is good to interact with your people. It's really interesting to know many things related to Teachers. Hoping for many more interactions are worthy in coming day so.

Mrs.Bharathi,Teacher
Kendriya Vidyalaya,NFC Nagar

The programme was very good and it created awareness for us to access the net with safety measures.

Sangita Rajan, Student
KV, Picket, Secunderabad

This seminar is useful for everyone, gives us a clear picture how we can get trapped into the hands of hackers or attackers.

M. Malathi,Teacher
Sreenidhi International School

Very useful and frequent such type of training programme or workshop should be conducted to bring awareness in usage of internet.

K A Vijay Kumar,
JNV, Kommadi ,Visakhapatnam

Get satisfied on this workshop. I got more information about information security

Prashanth Raware,
I.C.I.T, Pune

The workshop is a good idea to enlighten us regarding the importance of securing the information with caution.

Sarat Chandra Keerthi,
Teacher

JNV, Kommadi, Visakhapatnam

Interested to organize InfoSec Workshop at Your Location ?

for more details visit ....
www.infosecawareness.in/isea-pi

Download

- ✔ Cartoon Videos
- ✔ Brochures
- ✔ Posters
- ✔ Handbooks

from
www.infosecawareness.in/downloads

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Information Technology, Ministry of Communications & Information Technology, Government of India, is primarly an R&D institution invoved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-Learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain management and Wireless Sensor Networks

For Information Security Awareness Workshops at your place contact

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115
Fax: 040-2315 0117.