Cyber Investigations and Cyber Forensics

As per the current state of research in database forensics a proper mechanism is needed for data recovery from devices. This section presents you the recent trends for data recovery in digital forensics.

Cyber Crime : Challenges to Law Enforcement Agencies

Dr. S. Murugan
IPS, Joint Director / IGP
Directorate of Vigilance and Anti-Corruption, Chennai

Introduction

Cyber crime is defined as a crime in which an electronic communication device is the object of the crime, or used as a tool / target or used incidental or as a witness to commit an offence. Cyber criminals may use information technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. New technology is evolving day-by-day. Dark net become an important Point Of Sale(PoS) in the on line market Accordingly, Cyber crime investigators are also required to update their skills and use appropriate tools. Impact of Social Media also gives more ideas, strategies not only for the Law Enforcement Agencies but also for the Cyber criminals.

Types of Cyber crimes

Cyber crime may be classified as against target group of computer devices and target group of personal computer devices. Those against the target group of computer devices are classified as Denial of service, Malware and computer viruses. Those against the target personal computer devices are further classified as against person, against property and against Government.

Recent changes in the strategic technologies have created many challenges for the Law Enforcement Agencies across the globe as it is a borderless crime. Before discussing the challenges faced by the Law Enforcement Agencies in Cyber crime investigation, some of the recent trends in cyber crime are presented in the following sub section.

Recent trends in Cyber Crime

Crime-as-a-Service (C-aa-S)

Crime-as-a-service is when a professional criminal or group of criminals develops advanced tools, "kits" and other packaged services which are then offered up for sale or rent to other criminals who are usually less experienced. This is having a powerful effect on the world of crime and cybercrime in particular because it lowers the bar for inexperienced actors to launch sophisticated cyber attacks and scams. In 2017, Europol released a new study that flagged C-aa-S as the major facilitator of serious online crimes, as well as traditional crimes like illegal weapons sales. The Digital underground is underpinned by a growing Crime-as-a-Service model that interconnects specialist providers of cyber crime tools and services with an increasing number of organized crime groups. Criminals provide this C-aa-S by using TOR and crypto currencies.

Ransomware

Ransom ware is a subset of malware in which the data on a victim's computer is

locked, typically by encryption, and payment is demanded for the data to be decrypted and access is returned to the victim upon successful payment of ransom in the form of crypto currencies. The motive for ransom ware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack. Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity isn't known.

Criminal misuse of Data

Criminal misuse data for various reasons but mainly for harassing the privacy of individuals and for affecting the business establishments. Some of the recent data breaches are presented in Table to project the magnitude of the problem.

Table:1 - The 09 Biggest Data Breaches of 2018

S. No.	Name	How many people affected	Disclosed on
1	Exactis	340 million records	June 26, 2018
2	Under Armour	150 million records	May 25, 2018
3	My Heritage	92 million records	June 4, 2018
4	Face Book	87 million records	March 17, 2018
5	Panera	37 million records	April 2, 2018
6	Ticketfly	27 million records	June 7, 2018
7	Sacramento Bee	19.5 million records	June 7, 2018
8	PumpUp	6 million records breached	May 31, 2018
9	Saks, Lord & Taylor	5 million records	April 3, 2018

Online payment Frauds

A fraudulent online transaction in any bank account, or and through debit or credit card by unknown criminals from unknown destination is another major headache for Law enforcing agencies across the globe. Over 25,800 fraud cases involving about Rs.179 crore related to credit/debit cards and Internet Banking have been reported in 2017.

Cyber attack on Core Banking System

Recently Cyber attack on CBS (core banking system) gives some serious disturbances to the existing banking sector and few online cases have also been reported. During 2016, a Cyber attack was reported on Bangladesh Central Bank server which resulted $ 80 million loss. During February 2018 in India, a similar attack was organized against Punjab National Bank CBS which resulted in Rs.280 cores loss to the bank. City Union Bank of India also faced similar issue during the same period in which around 13,000 transactions have been executed from 28 countries. On August 11, 2018, a Canadian hacker attacked the COSMOS Bank through malware which was sent as a link to the target with an executable code in which 14,800 transactions took place from 28 countries which resulted in Rs.94 crores loss to the bank.

On October 2, 2018 another similar malware attack was against the server of State Bank of Mauritius which resulted in Rs.143 crores loss to the bank. All these cross border cyber criminal activities through online resulted in so much of loss to the banking sector.

Pornography

Though Pornography is not a punishable offence in some of the countries, whereas child sexual abuse is a punishable offence across the globe. Child pornography is one of the heinous crimes in Darkent market.

Dark net crime

Accessing Dark net through The Onion Router (TOR) provides anonymous and invisible way to trade viz., drugs, digital pirated items, arms and ammunition which are serious threats and are prohibited by the Law Enforcing Agency.

Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. An increased number of phishing attacks which aimed at high value targets have been registered by various agencies.

Virtual Currencies

Crypto currencies viz, Bit coin, etc, remain the currency of choice for criminals for their criminal transactions in the electronic underground economy and in the Dark net.

Tech Militants

Globally militants are effectively utilizing Information technology and IoT (Internet of Things) which give serious security threat both for virtual and real world in many countries. Besides that the terrorists are using VPN, TOR, etc for their communication which gives serious trouble for the Law Enforcement Agencies for surveillance and investigation of these outfits activities.

Conclusion

Challenges for LEAs are not only for them but for the Nation also. Urgent remedial measures through proper legislative support, technical support and periodical capacity building exercise will provide confidence to LEAs to handle the challenges related to cybercrime in future.

For queries on Information Security
Call us to Toll Free No.
1800 425 6235

For details on
Cyber Crime Cells in India and Cyber Crime Reporting Portal
visit https://www.infosecawareness.in

Challenges to Law Enforcement Agencies

1. Getting basic details and account information etc from service providers of social media is the biggest challenge for Law Enforcing Authorities (LEAs). Servers of major social media service providers are located in USA and other countries which creates certain legal issues for LEAs.
2. Privacy laws of some countries also prohibit exchange of information/data from the service providers of social media to LEAs.
3. Lack of MLAT (Mutual Legal Assistance Treaty) with all the countries is a major hindrance for LEAs while collecting evidence from servers located abroad. As on date, India has signed MLAT with only 39 foreign countries.
4. One of the main conditions for MLAT is that the particular offence must be a punishable offence in both the countries. For instance pornography is not a punishable offence in USA, even though we have MLAT with USA, we are not able to take legal action against few cyber criminals who are indulging revenge pornography websites , operating from USA. A criminal case registered by Chennai police related to this type is pending only for this reason for more than 18 years.
5. Every day innumerable Electronic communication devices are compromised due to millions of viruses and other type of malicious code that are in global circulation.
6. Dark net is an increasingly popular corner of the Internet where thousands of Electronic Communication Device (ECD) users from around the globe interact anonymously and in many cases, illegally. For instance, 10,000 plus valid credit cards can be bought at an average price of $2 to $10 each, and one can also get blank bank-specific slug cards and magnetic strip printers. There are also clues to surface net security vulnerabilities that are being exploited for profit. It is reported that an anonymous website rang up $8 million in monthly drug sales.
7. The Dark net is a privileged place for cyber criminals and terrorist that, under specific conditions, they could operate in anonymity and transactions through crypto currencies. Anonymity means the darknet is structured such that there is no source and not easy to trace the evidence. This creates an incredibly difficult tracing process.
8. Understanding the technical process that occurs during the transaction methods for each crypto currency algorithm. Major players of crypto currency are addressing information which is not able to be obtained and not visible to an investigator.
9. Lack of visible and stronger KYC/ AML (Know Your Customer / Anti-Money Laundering) norms for crypto currencies transaction, gives a major setback to LEAs.
10. TOR network employs a special browser for encrypted internet traffic. This poses difficulties for evidence collection by law enforcement agencies. TOR network is not readily visible through popular Internet search sites. The buyers and sellers don't exchange cash, instead in the form of untraceable crypto currencies, usually Bitcoin. So there are no banking records for investigators to subpoena.
11. Those who created and support the TOR network claim it as a way to protect online users' privacy and anonymity in the digital age. They do not condemn its use for illegal activities as it was originally created for U.S. Navy for end to end encrypted transaction. The same browser has been misused by terrorists to unfortunately affect the meaning, scope and depth of the transaction and the related illegal activities are a grey area for Law Enforcement Agencies.
12. The issue of illegal pharmaceutical crime on Dark net market places poses a great challenge to law enforcement and a severe risk to public health on a global scale.
13. Lack of training poses a challenge to handle the dark net crimes. Even though internet had been introduced in the 20th Century, only 60 percent of LEA is trained on internet crimes. The TOR based dark net is not at a tangible distance for LEA due to lack of technical knowhow.
14. Tech militancy through TOR or and VPN are a serious threat for investigators.

Counter Measures to overcome challenges with Cyber Crime

The following are some of the measures to overcome the challenges associated with cyber crime:

1. An Investigatory Power Act with provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal data sets and other information in view of National Security has to be enacted. Similar Act / bills were already introduced to strengthen the powers of investigators in few western Countries. In India, similar type of Act is the need of the hour. Otherwise, it is very difficult to investigate Dark net and surface net crimes and the surveillance of criminals in the TOR , VPN environment.
2. Periodical training for LEA should be provided to handle the challenges originating from both surface web and dark web.
3. In order for law enforcement to stay ahead of the curb and effectively mitigate the threat posed by criminals operating on the Darknet, INTERPOL IGCI offers capacity development support for member countries that want to create or further develop cybercrime units with specialized training on analyzing darknet infrastructure. In parallel, INTERPOL's specialized crime units, such as MPCPC, will continue to give member countries tailored support for particular crime areas. In the case of pharmaceutical crime, international and interagency cooperation are essential to combat this global problem and protect public health. This type of training shall be given to all LEAs.
4. Law enforcement agencies in many countries are still not in a position to deal effectively with the illegal activities that leverage infrastructures both in the surface web and in the Dark Web. The anonymity of the actors and jurisdictional issues are the most common issues that obstacle their activity. When dealing with the growth of illegal activities in the Dark Web, legislation, technical abilities and capacity building are essential components of a strategy that must be shared by law enforcement agencies worldwide. They should build technical capabilities in order to support technical investigations into subjects using Darknets, in accordance with relevant legislation.
5. A Master Circular may be issued by RBI/Central Bank on How to handle Crypto currencies in India and how to proceed further in cases of frauds reported therein.

Data Recovery in Digital Forensics : Recent Trends

Rupali Chopade
Research Scholar Department of Computer Engineering & IT College of Engineering, Pune

Dr. Vinod K. Pachghare
Associate Professor Department of Computer Engineering& IT College of Engineering, Pune

Digital forensics is an upcoming research area. Digital forensics mainly aimed at the recovery of deleted data. Data recovery may be related to database, computer system, hard disk, pen drive or similar devices. Database forensics is a sub-field of digital forensics. Forensic is a process of detailed investigation of activities performed in the background to find out any suspicious or malicious activity, which can be presented as proof in the court.

Keywords: Database, Forensics, Recovery

Introduction

Now a day most of the activities are performed online. It is almost impossible to imagine our life without digital devices. We are not able to complete any task without these digital gadgets. With the increased use of such devices, cyber-crimes are also increasing day by day. Cybercrimes are nothing but the criminal activities performed using devices like computer, mobile, the internet etc. Forensic science is an investigation process to solve crime cases. Digital forensics is a branch of forensic science in which the investigation process is carried out with digital devices, to find out the suspect. There are various types of digital forensics like computer forensics, mobile forensics, network forensics, Cloud forensics, and database forensics. For computer or mobile forensics, there are again sub-types like file forensics and memory forensics. With the increase in the use of these devices, criminal attacks are also increasing to steal sensitive information by deleting it. Data recovery is an important aspect as far as digital forensics is concerned [1].

Literature Review

Digital forensics is a field of finding what, how and when data tamper. Digital forensics involves forensics phases such as collection, identification, preservation, analysis, and presentation [2] [3]. As per information security act like Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPPA), it is important to find evidence and convey the same to customers, what was compromised [4] [5].

Databases play an important role as far as storage and computing are concerned. Every organization must require it. Today a lot of sensitive and personal information is stored in databases, as we are performing a number of activities online, which leads to criminal activities. Similarly, we are storing our sensitive and personal information on mobile phones, which is required for our daily online activities. Though a lot of research is going on data security, still attackers are trying and coming with new techniques to either steal the data or to delete the data.

- Matthew Geiger analyzed 13 commercial counter-forensic tools in 2006 [6] and showed their shortfalls which prevent the data recovery. Tools are compared by using features like wiping failures with free space and targeted files, registry records missed, activity files missed and data recoverable from file system structures.
- In 2016, Woo Yeon Jo et al. developed [7] a digital forensic approach for file recovery from a UNIX file system. Authors showed the internal file structure of UNIX. Actual file data is available with the inode table. When a file is deleted then inode will be removed. Deleted file information is stored with time values, called a magic number. By using a magic number and confirm the technique file is recovered. For forensic analysis of any database, it is important to know and understand the underlying file structure of the database.
- CHANG Xu et al. [8] presented data recovery from an android mobile phone with Yaffs2 (Yet another flash file system) file system. Android system is based on the Linux kernel. Deleted data can be restored by analyzing the Yaffs2 file system in memory. Yaffs file is embedded with NAND flash design. For analysis, data is checked from two chunk files object header and data chunk.
- In the year 2010, Yinghua Guo and Jill Slay invented that many forensic tools available for a forensic purpose are not actually useful for forensic purpose because they are not designed for that specific reason [9]. It is important to validate and verify these tools before using for forensic purpose. In this paper, the authors suggested a systematic framework for the validation and verification of these tools.
- Here authors proposed [10] how to recover deleted data from MySQL database file system. InnoDB is a storage engine used by MySQL. All information is stored in one file which is created as a TableName.frm file. Authors have shown how to convert most of the data types in readable string format. In extended work, authors have shown the reconstruction of data manipulation operations like insert, update and delete. Recovery of DDL statements like Alter, Truncate or Drop table is not considered here.
- In this paper, authors have suggested a method to recover deleted and partially

References:

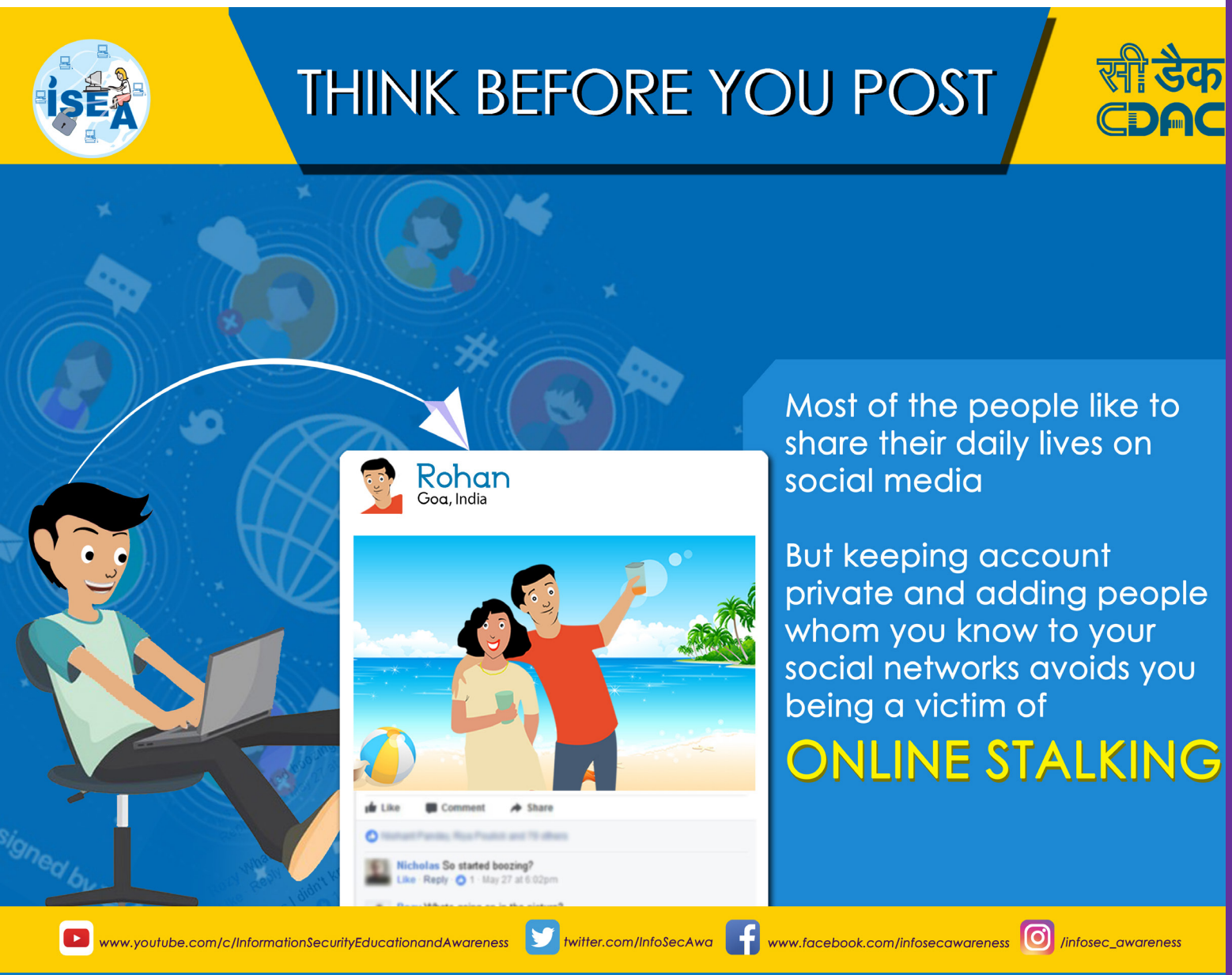
- *Werner K. Hauger and Martin S. Olivier, "The state of Database Forensic research", IEEE Information Security for South Africa (ISSA), 2015.*
- *YunusYusoff, Roslan Ismail and Zainuddin Hassan, "Common Phases of Computer Forensics Investigation Models", International Journal of Computer Science and Information Technology, Vol. 3, No. 3, pp. 17-31, 2011.*
- *Arafat Al-Dhaqm, ShukorAbdRazak, Siti-Hajar Othman, AsriNagdi and Abdulalem Ali, "A Generic Database Forensic Investigation Process Model", Journal Teknologi, Penerbit UTM Press eISSN 2180–3722, Malaysia, pp. 45-57, 2015.*
- *Sarbanes Oxley Act, http://www.soxlaw.com/*
- *HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html*
- *Matthew Geiger, "Counter-forensic tools: Analysis and data recovery," 18th Annual FIRST conference, Maltimore, Maryland, 2006.*
- *WooYeon Jo, Hyunsoo Chang, and Taeshik Shon, "Digital Forensic Approach for File Recovery in Unix Systems - Research of Data Recovery on Unix File System", IEEE Information Technology, Networking, Electronic and Automation Control Conference", 2016*
- *CHANG Xu, TANG Xin-hua and WU Jian, "Forensic research on data recovery of android smartphone", 2nd International*

overwritten data [11]. From SQLite, this is used mostly for mobile phones. For this implementation, they have used three tools SQLite Exert, Android 5.0 ADB tool, and WinHex software. SQLite database file system consist of 4 pages namely free page, overflow page, B+ tree page, and B tree page. Though there are various tools available for the forensic purpose, still there is a need for a proper technique to recover data deleted from the database [14]. Further research is needed for NoSQL databases [15] [16] [17] [18].

- The work carried out by researchers [12] with respect to trigger is as below. Database triggers are actions performed on data when changes are made with respect to data. Current forensics investigators assume that the forensics process will not have any effect though database triggers are available. Through different examples, authors presented that the forensics process needs to be improved to handle the presence of database triggers.
- File metadata [13] is associated with a file like a file name, size, date of creation etc. Files are represented using FAT, NTFS, and ext3. As compared to files, databases have a more complex structure. They are represented using two dimensions. One dimension shows schema structure namely external, conceptual and internal levels. The second dimension called an orthogonal intention-extension dimension which consists of the data model, data dictionary, application schema, and application data. In this process copy of the disc is prepared known as imaging. Sometimes file reassembling is needed if the file structure is damaged and it is known as file carving. During the acquisition process, the system may be analyzed without switching it off known as live analysis and analyzing it after turning off, known as dead analysis.

Conclusion

Digital forensics is an upcoming field of research. As per the current state of research in database forensics NoSQL databases needs attention, as most of the work on relational databases is already done. As far as data recovery from devices is concerned, the proper mechanism is needed. Many digital forensic tools are available but they are not designed for specific purpose, hence suffers from limitations. Researchers have done forensic analysis using log files, metadata, data files etc. File carving is a renowned method for computer forensics, but analysis of the database using the carving method is a new approach for research.



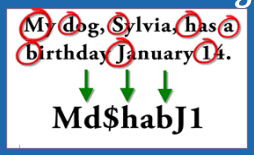
TIPS TO PROTECT YOUR PASSWORD

Password are like socks change them regularly

Use different passwords for different accounts

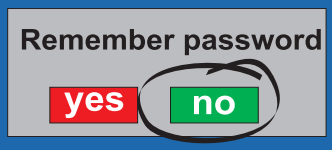
Be aware of Shoulder Surfers at public places while you are entering your passwords into the login accounts

Make passwords more complex to increase the difficulty of attacks that rely on brute force or guessing



If it is hard to remember a password, switch to passphrase

Never share your password with others

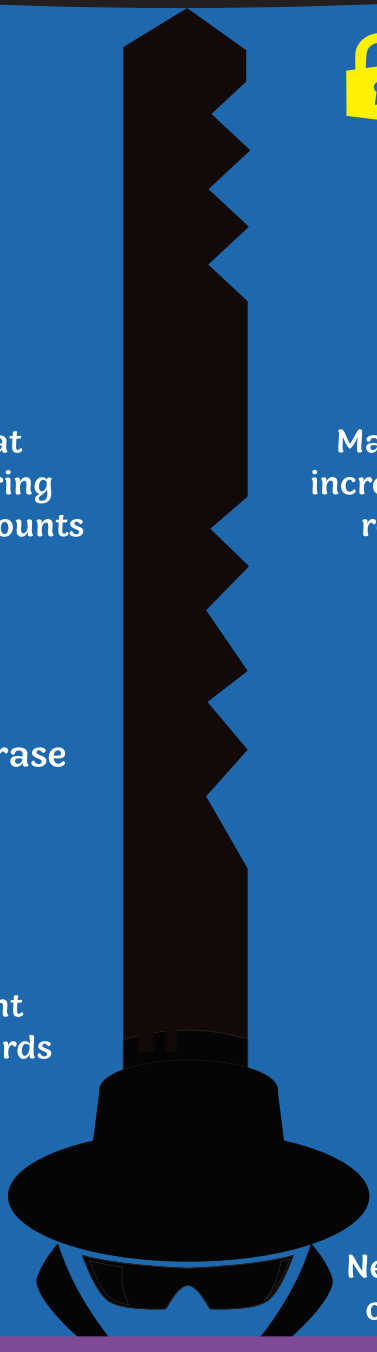


Do not select 'Yes' when any application ask you if you want them to remember your passwords

Never use dictionary words (like animal, plants, etc.,) while creating passwords

Your brain is the best place to store your passwords

Never write passwords on paper or on any disk drive to store it



For more details / queries on Cyber Security visit or call us to our Toll free number

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

1800 425 6235

For Virus Alerts,Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

Financial Transactions: Security Guidelines

Sunit Kr.Nandi
Leading Officer,
TechnoFAQ.org
Mentor and consultant

India is moving toward digital payments and has encouraged consumers to leave traditional banking services and move to online banking services through Apps. This requires login credentials which are crucial information that need to be handled with care. Everyone who is new in online banking has many questions in mind, like where and how are the banking credentials stored. Banks plays a major role in safeguarding our money and user credentials while using online banking. But Safeguarding banking credentials is the responsibility of the consumer as well as the bank.

The bank must:

- Enforce strong passwords.
- Use OTPs/tokens or 2-factor authentication wherever possible.
- Store the passwords in hashed form in their data store (and not in plaintext) and use a strong hashing function like SHA256, bcrypt, scrypt or BLAKE2. Also, the password should be mixed with a secret string, known as a salt, known only to the bank before hashing so that direct bruteforce attacks are thwarted.
- Communication of credentials between application and transaction servers to the AAA server should always be encrypted with modern ciphers, like AES-GCM and ChaCha20-Poly1305, plus any secret part of the credentials should always be sent in hashed form (with the salt, ofcourse) for extra security.
- Not store credentials and transactions in the same data store.

A user must:

- Not share their banking credentials with anyone
- Memorize and not write it down anywhere. Password managers are convenient, but I suggest that you still avoid them if they rely on a central service. Memorizing is the best option.
- Change their passwords and PINs regularly
- Report to the bank immediately if an unauthorized transaction occurs.
- Not access banking accounts on shared devices. If you are in a cyber-café and require access to your bank, use your phone instead. Restrict all banking activities to trusted devices only.
- Protect computer from malware by not installing apps from unknown sources.
- Use a more secure OS, like GNU/Linux or macOS, instead of Windows and enable full-disk encryption on your trusted devices if possible.
- Make sure account recovery details like phone number, identity documents, etc. are up-to-date with the bank. In the unlikely event of a fraud, updated information will help banks to verify that it is you quicker and solve your problem ASAP.

In the rare event of a bank breach, the bank and the RBI should compensate you according to present financial laws.

Banks make better use of data, to understand their customers better.
Generally Banks use transaction data to determine the nature of income and expense of a customer, to understand the trustworthiness of the customer, i.e., how likely a customer will repay a loan given to them by the bank. More trustworthy customers are likely to get bigger loans with lower interest rates as they pose a lower risk compared to others. Similarly, credit/debit card transaction data can be profiled to understand a customer's spending patterns. This is important, because, any significant deviation from the pattern is likely to be a fraud.

Big data is going to play a major role in banking sector and will be a great help to the customers.
Big data will help banks disburse loans to trustworthy customers without excessive financial documentation, as well as combat card fraud at a huge scale, without requiring extra manpower and human intervention. Big data also helps banks to sell financial products like insurance and vouchers and send appropriate marketing offers that are more likely to be accepted by the customer and also gain the customer's trust and loyalty in the process.

Most of the Banks in India both small and big are well equipped to handle security breaches today.
Banks today, adhere by PCI compliance and financial regulations. While banks all over the world are not perfectly secure as you would want them to, mainly because they prefer stability in their system, and adapt very slowly to change, they still have good levels of security. If a bank follows all the best practices, the majority of bad actors cannot affect it. For the small minority of extremely talented bad guys, almost anything on this planet can be breached. In that case, monetary reserves and insurance should take care of the situation.

Will size of the bank give it an advantage?

A size of a bank is a double-edged sword. The bigger a bank is, the more likely it has more capital and manpower to ensure better security and larger monetary reserves. However, the increased number of branches introduce increased attack surface due to more failure points. Ideally, a bank should adapt its security practices according to its size.

Machine learning and AI plays a major role in financial fraud detection and prevention. Banks are integrating artificial intelligence to change the cyber security scenario of online banking which in turn can bring benefit for the customers.

ML and AI will help banks learn customer habits in real-time and on a big scale. The presence of ML means that bank systems can adapt to the changing nature of the customer, while the presence of AI means that bank systems can take quick decisions without involving a human for most cases. When it comes to cyber security, the bank can use ML and AI to block threats in real time, for example, deny netbanking access from a place you are not currently in, block a fraudulent transaction as the bank knows you will never shop in that place/website, and so on. Customers are going to see a huge benefit as they will be more secure from fraud, while banks will deal with less cases of fraud and is less likely to lose customers' money.

Most of us are integrating bank accounts with E-Wallets. But these are not free from cyber threats.

E-wallets Paytm, Google Pay nor Airtel Pay are payments app that runs on the Unified Payments Interface (UPI), an initiative by the NPCI. UPI assigns you a virtual payment address (e.g. abcdefi@oksbi) with which you can pay to another user on their address. You can also receive payments on your address. The benefit of this is that, you

do not need to remember or provide bank details to transfer money. As only addresses are exchanged, it also preserves privacy of the users. Any payments coming to/from an address are automatically sent to/from the bank account associated with the address. That means e-wallets are essentially a non-custodial payment service provider that does not actually hold your funds. You need to explicitly link your existing bank account with-wallets, upon which you are assigned an address for that account by the app. When you make a payment, a bank page appears requesting you to enter your UPI PIN, known only by you. Once you enter the PIN, the bank authorizes the E-wallet to send the payment to the target address. Once the recipient address receives the amount, the UPI app that has assigned that address contacts the target user's bank and deposits the money in the target user's account. Here are few tips to for safe use of E -wallets

Go ahead and use them to enjoy the increased competition in our democracy's free market. More competition means that traditional banks will soon offer better and more unusual banking offers.

CYBER THREATS IN FINANCIAL TRANSACTIONS

Financial security has different meaning to different individuals. But basically it is deep rooted feeling giving individuals a peace of mind that, 'Everything will be good'. The world of finance including financial transactions and investments has moved into a new phase where internet plays a key role. Electronic devices like smart phones, computer, laptop, tablet, POS machines, ATM etc..., are used to for online means of banking and investments. Most of these devices have become an integral part of an individual's life resulting in online means of banking and investments overtaking the traditional banking methodology. As all of us are aware that Internet also has a negative side which puts all means of online financial transactions at high risk. Cybercriminals rely on the vulnerabilities present in Internet to seize your hard earned money. Due to this it is a necessity to take extra step to secure your hard earned money and investments.

HOW FINANCIAL FRAUDS HAPPEN ?

Cyber criminals employ various methods to attain the sensitive personal information to execute fraud. Few methods used by cyber criminals are Phishing, Smishing, Vishing, Skimming, SIM Swapping fraud, Fraudulent policy applications, Payment hijacking, Malware, DDos attack, Man in the middle Attack, Ransomware, Business email Compromise.

Beware of external wires or devices connected to swiping machines

Always use secure communications for your financial transactions

Ensure that your transaction is ended/ completed at ATM machine before leaving

If you are a victim of identity theft, report it immediately

IMPACT OF ONLINE FINANCIAL FRAUD ON AN INDIVIDUAL

The first thing that comes to mind when we talk about 'impact of online financial fraud on an individual' is the direct financial loss. Victims often pass through wide range of emotional and psychological impacts of fraud. Many feel panicked, angry, afraid, anxious, ashamed and blamed themselves after the fraud was committed. They even feel vulnerable, lonely, violated and depressed and in the most extreme cases, suicidal, as a result of the fraud they experienced. These emotional and psychological impacts relate to both the stress of financial loss and also the loss of self-confidence that followed the fraud. The experience also may affect relationships with others, making it difficult for victims to trust others. It can be summerised as

becoming a financial fraud victim carries emotional as well as financial costs

Financial and emotional costs vary across fraud categories, and

Individual personality traits influence the victims' perceptions of impact.

DO'S

- ✓ Always keep your device updated, locked & protected with a strong password.
- ✓ Keep a watch on transaction logs and alerts; and report suspicious or fraudulent attempts to relevant service providers & police officials.
- ✓ Immediately block your SIM if your device gets lost or stolen and inform respective bank/wallet organization & police officials.
- ✓ Beware of unsolicited calls, texts or emails asking for sensitive financial information.
- ✓ Download applications on your devices from authentic apps stores with good reviews only.
- ✓ Ensure authenticity of applications by validating from links on bank websites.
- ✓ Always verify and install authentic e-wallet Apps
- ✓ Ensure your phone number is protected with a PIN.
- ✓ Make sure the beneficiary's mobile number is correct before transactions
- ✓ Use only verified and trusted browsers & HTTPS secured websites for payments.
- ✓ Ensure you change passwords frequently and promptly if compromised.
- ✓ Ensure that you securely dispose of receipts and statements.

DON'T'S

- × Refrain from clicking suspicious links received in SMS or email.
- × Steer clear of using jailbroken or rooted devices for mobile banking.
- × Never handover your device to strangers.
- × Avoid responding to emails, phone calls or text messages asking for debit card/credit card/ATM pin/CVV/expiry date or passwords.
- × Avoid using a common password for all wallets.
- × Refrain from open Wi-Fi or unverified services for making payments.
- × Do not scan untrusted QR codes.
- × Never store login credentials on phone also don't enter credentials on untrusted kiosks
- × Avoid transacting through public devices and on unsecure/open networks.
- × Never allow merchants to store your card information.
- × Do not leave your credit or debit card with anyone.
- × Never share or write down your UPI M-PIN.
- × Refrain from transferring money without verifying the recipient first.
- × Never allow merchants to store your biometrics and card details.
- × Avoid giving away your Aadhaar and personal details

For more details / queries on
Cyber Security visit or call us to our Toll free number

Ministry of Electronics & Information Technology, Government of India

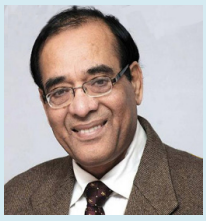
www.InfoSecawareness.in

1800 425 6235

For Virus Alerts,Incident & Vulnerability Reporting
cert-in Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

Our Sincere thanks to all the dignitaries



Dr. Gulshan Rai

Dr. Gulshan Rai holds a doctoral degree and M.Tech and has over 35 years of experience in different areas of Information Technology which include different aspects of e-Governance, Cyber Security, Cyber Laws and several related fields. Prior to that he was National Cyber Security Coordinator, Government of India in the Office of Prime Minister. Earlier he was Director General, CERT-In (Indian Computer Emergency Response Team) and Group Coordinator of E-Security and Cyber Law Division in the Ministry of Communications and Information Technology (now MeitY). He has led the team to set up National Watch and Alert System in the country as part of cyber security initiative and Computer Emergency Team. Several international cooperation agreements have been entered under his leadership. He led a team from time to time to draft and bring out National Policies in the area of cyber security and cyber laws. Dr. Rai has been working since 1998 in the area of evolving legal framework to address issues arising out of cyberspace, which resulted in second Technology Legislation in the country i.e. Information Technology Act and amendments in the Act. He was Executive Director, ERNET India for over 7 years and was instrumental in setting up of the first large scale education and research network in close collaboration with the leading educational and research institutions in the country. During his tenure, the project of National Knowledge Network was evolved and designed. He has been leading team, designing and implementing IT solutions in the areas of Finance, Taxes and Law & Order. He has several publications in the area of Security. He has represented country in various official forums and bilateral discussions and negotiations in the area of Security and Internet related matters.

Our Sincere thanks to all Participating Institutes

S Gangopadhyay
IIT Roorkee

Manoj Misra
IIT Roorkee

Vijay Laxmi
MNIT, Jaipur

Ashok Turuk
NIT, Rourkela

Dhiren Patel
SVNIT Surat VJIT Mum

Uday Pratap Rao
SVNIT Surat

Alwyn Paise
NITK Suratkal

Shanthi Thilaga
NITK Suratkal

DVLN Somayajulu
NIT Warangal

Ravi Chandra
NIT Warangal

Sandip Chakraborty
IIT, Kharagpur

Debdeep Mukhopadyaya
IIT, Kharagpur

MNNIT Allahabad

IIITM Gwalior

Eng Clg Puducherry

Eng Clg Pune

IITISM Dhanbad

IIT Kurukshetra

NIT Raipur

NIT Patna

IIITM Kerala

MANIT Bhopal

DTU Delhi

IIIT Hyderabad

IIIT Delhi

IIIT Bhubaneswar

IGDTU Delhi

Eng Clg Goa

AU Visakhapatnam

NIT Durgapur

VNIT Nagpur

NIT Srinagar

NIT Jalandhar

Tezpur University

College of Engineering Gunidy Anna Unverstiy

GTU Gujarat

JNTUH Hyderabad

Makaut West Benagal

RGPV Bhopal

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

सी डैक
CDAC

ERNET India
Education & Research Network

NATIONAL INFORMATICS CENTRE

रा.इ.सू.प्रौ.सं
NIELIT

STQC

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Our Sincere thanks to all the dignitaries

Prof. N. Balakrishnan
Indian Institute of Science, Bangalore

Prof. N. Balakrishnan, Honorary Professor, Indian Institute of Science (IISc, Bangalore). JC Bose National Fellow, Honorary Professorships and Directorship & Membership of Boards for many National and International Academic Institutions, Industries / Companies, Member of Editorial Boards of International Journals. Professor received many Awards / Honours / Recognition's including prestigious Padmashree by the President of India, 2002- One of the highest CIVILIAN HONORS bestowed upon for seminal contributions to Science and Engineering- Has its origin in the Knighthood in the Pre-independent India.

Prof RK Shyamasundar is a JC Bose National Fellow and Distinguished Visiting Professor at the Department of Computer Science and Engineering, IIT Bombay. He was the Founding Dean of School of Technology and Computer Science at Tata Institute of Fundamental Research. He is a Fellow IEEE, Fellow ACM and Fellow of all National Science and Engineering academies and a Fellow of the World Academy of Sciences (TWAS), Trieste. He has authored over 300 peer reviewed publications, 8 patents, and 8 books. More than 35 Ph.D. students have graduated under his guidance in India and USA.

Prof. R. K. Shyamasundar,
Indian Institute of Technology Bombay

Prof. Sukumar Nandi,
Indian Institute of Technology, Guwahati

Professor Sukumar Nandi, Head Centre for Linguistic Science & Technology, and Professor Department of Computer Science & Engineering, Indian Institute of Technology, Guwahati, India.

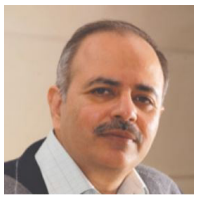
Areas of Interest: Computer Networks, Internet of Thing, Information Security, Data Mining, VLSI Design and Testing, Approximate Computing. Specialization: Wireless Networks, Traffic Engineering (QoS and QoE), Systems Security, Network Security, VLSI, Data Mining

Kamakoti Veezhinathan is a Professor at the Department of Computer Science and Engineering, Associate Dean, Industrial Consultancy & Sponsored Research (IC&SR), Indian Institute of Technology Madras, Chennai, Tamil Nadu India. His areas of specialisation includes Secure Systems Engineering, Computer Architecture and CAD for VLSI Design Systems. He is also an independent Director in the board of City Union Bank since 2011 and a member of the Standing Technical Committee of National Stock Exchange. He was awarded the Inaugural IIT Madras Young Faculty Recognition Award in 2007. He received the DRDO Academic Excellence award in 2014 from Hon'ble Prime Minister Shri. Narendra Modi.

Prof. V. Kamakoti,
Indian Institute of Technology Madras

Manoj Singh Gaur
Director, IIT Jammu

Dr. Manoj Singh Gaur assumed the charge of Director, Indian Institute of Technology, Jammu in June, 2017. Prior to joining IIT Jammu he was a Professor and Head of the Department of Computer Science and Engineering at Malaviya National Institute of Technology (MNIT) Jaipur, India. Additionally, he was Professor-In-Charge (Coordinator) of IIIT Kota, which is currently being mentored by MNIT Jaipur. He has been Dean, Students Affairs and Head, Central Computer Centre at MNIT Jaipur as well. He also served as Chairman, Senate UG Board at MNIT Jaipur.



Dr. Sanjay Bahl,
Director General, CERT-In

Arvind Kumar
Scientist G,
Group Coordinator, MeitY

Rakesh Maheshwari,
Scientist G,
Group Coordinator, MeitY

Shri.Sitaram Chamarthy
Principal Consultant, TCS

Dr. Bishwajit Saha,
Additional Director (ATR & I), CBSE

Dr. Amarendra Prasad Behera (Ph.D.)
Joint Director, CIET

Shri U Rama Mohan Rao
SP, Cyber Crimes, CID, Andhra Pradesh

Anil Kumar Pipal
Head, HRD Division, MeitY

Sanjay Kumar Vyas
Scientist E & OSD to Secretary, MeitY

Surendra Singh
Scientist 'D',
HRD Division, MeitY

ACTION GROUP MEMBERS

HoD (HRD), *MeitY*
Shri.SITARAM CHAMARTHY *(TCS)*
Dr. M S GAUR *(Director, IIT Jammu)*
Prof. DR.DHIREN R PATEL *(Director, VJTI Mumbai)*
REPRESENTATIVE OF CHAIRMAN *(CBSE)*
CEO, DSCI (NASSCOM)
REPRESENTATIVE OF PRASAR BHARATI, MEMBER OF I & B
Shri U RAMA MOHAN RAO *(SP, Cyber Crimes, CID, Andhra Pradesh)*
Shri S K VYAS, *MeitY*

SUB COMMITTE OF PRSG TO REVIEW / CLEAR CYBER SECURITY CURRICULLUM FOR SCHOOLS

RAKESH MAHESHWARI, *Scientist G*
Dr. B K MURTY, *Scientist G*
Dr. BISHWAJIT SAHA, *Additional Director (ATR & I), CBSE*
Dr. ANGEL RATNABAI, *CIET NCERT*
Shri CH A S MURTY, *Associate Director*

COORDINATION COMMITTE FOR GOVERNMENT OFFICIAL TRAINING

REPRESENTATIVE OF SECRETARY, P&T,
MISS. NEETA VERMA, *DG, NIC,*
SHRI UMESH KUMAR NANDWANI, *DG, STQC,*
DR. SANJAY BAHL, *DG, ICERT*
SHRI RAJIV KUMAR, *DG, NIELIT*
DR. HEMANTH DARBARI, *DG, C-DAC*
DR. MEENA PAHUJA, *DG, ERNET*
PRO V KAMAKOTI, *IIT, Madras,*
PROF. DHIREN PATEL, *Director, VJTI Mumbai,*
SHRI ALOK TRIPATI, *Director Incharge, NIELIT Patna*

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

InfoSec awareness.in

www.isea.gov.in

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

CYBER DOST

CYBER shikshaa

CYBER SAFE GIRL
Beti ko Bachao, Cyber Crime Se

For queries on Information Security Call us on Toll Free No.

1800 425 6235

Supported by
सत्यमेव जयते
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Programme by
सत्यमेव जयते
Ministry of Electronics & Information Technology, Government of India

सी डैक CDAC
प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via (Keshavagiri Post)
Hyderabad - 501510