Vol. IX No. 2 April-June, 2015 ISSN-2249-1996

e-track

PUNJAB NATIONAL BANK INSTITUTE OF INFORMATION TECHNOLOGY

SAILING SAFE IN CYBER WORLD...

e-track

Editor
Pratima Trivedi

Editorial Team
A. K. Wahi
Pramod Dikshit

Printed by
Shree Keshav Print Point
G-7, Arif Chambers-V, Sector-H,
Aliganj, Lucknow-226024
Mobile : 9335532342

punjab national bank institute of information technology

Vibhuti Khand, Gomti Nagar,
Lucknow-226 010 (U.P.)
T : +91 522 2721442, 2721174
F : +91 522 2721201, 2721441
E-mail : bankingtech@pnbiit.co.in
URL : www.pnbiit.com

From the desk of editor

Dear Readers,

E-banking implies a service that allows customers to use some form of computer to access account-specific information and possibly conduct transactions from a remote location - such as at home or at the workplace. The obvious advantage to the consumer is convenience and freedom to conduct routine banking transactions from the comfort and security of his/her home 24X7. But e-banking is always attached with security threats and Cyber crime. Cyber crime is anything done in the cyber space with a criminal intent. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium.

This issue of e track is focusing on various aspects of cyber crimes, its modus operandi, cyber forensic etc. Digital Certificate is one of the foundations of a public key infrastructure (PKI). It is the electronic equivalent of a passport or driver's license, and may be used to identify and authenticate someone making online transactions. The article “security using digital signature” focuses on various aspects of this.

Hope you will savor this serving of e track .....

Happy Reading.....

Pratima Trivedi
e-mail : pratima@pnbiit.co.in

Thought for the quarter

A successful man is one who can lay a firm foundation with the bricks others have thrown at him.

David Brinkley

Reader's Comments

Good attempt.

- Shri Arvind Tewari, Field General Manager, PNB, FGMO, Lucknow

Nice to have this issue of e track on my screen. 32 pages of beautiful presentation and meaningful articles. Above all was the introductory editorial. Some latest developments may be inducted in small boxes. I am sure some good reading is in store in time to come. Congrats to the Institute, its director, editorial team and of course to the editor.

- Shri Punit Jain, Circle Head PNB, Haridwar Circle.

Contents

MESSAGE FROM THE DESK OF EXECUTIVE DIRECTOR

Virtually everything in business today is an undifferentiated commodity, except how a company manages its delivery value. A good way to outdo competition is to render it passé by pleasing customers in new ways. Essentially, that's what electronic business is all about.

E-commerce is a fundamental component of e-business. It is primarily associated with the buying and selling of goods and services over internet or private networks, without partners to the transaction coming face to face. E-business uses technology and e-commerce processes to build better customer relationships and create new value propositions. The virtual shops deliver value by innovative business designs and processes. Electronic commerce renders exchange of business information across internet.

The information can range from the simplest data about products and services to complex, multipart financial documents used among trading partners to support extensive business transactions. With sophisticated software, enterprises can use electronic commerce to debit and credit accounts, passing funds electronically among partners without actually touching paper based monetary instruments. The applications are vast, and the possibilities can be extremely rewarding to enterprises in terms of savings, increased competitiveness, and enhanced market position. Payment and settlement of value of goods and services between buyer and seller is a natural component of any trade / commercial transactions to eventually conclude.

Electronic banking or e-banking enables electronic transfer of funds from buyer to seller as also between two entities for non-commercial purposes. Evolved over the years, e-banking today offers customers to choose from Internet banking, debit or credit cards, bank to bank electronic funds transfer and mobile banking (or banking using mobile telephone devices). The concept of transmitting vital information electronically is always paired with the corollary of security. There are numerous potential security risks, like viruses, malicious hackers, destructive hackers, spoofing, sniffing, line trapping etc .To tackle the issue innumerable security products are offered by vendors ranging from simple password and authentication procedures to complex packages that provide electronic wallets, cash registers, encryption, and verification. Security can also be enhanced by using digital certificates. As standards are being set and security concerns are being addressed, the resultant increase in confidence of users will facilitate e-banking to grow exponentially. In the meanwhile, let us keep e-banking with due compliance of security prescriptions laid down by service providers.

I am happy to note that PNBIIT is bringing out its quarterly journal "e-track", for awareness and spreading IT innovations as well as enhancing the use of technology among the banking fraternity. The journal has collection of informative articles, which for sure will add to the Knowledge of Readers.

I wish all success to PNBIIT and “e-Track” in its endeavor to educate people on the use of e-banking.

K V Brahmaji Rao
Executive Director
Punjab National Bank

MESSAGE FROM THE DESK OF FIELD GENERAL MANAGER, LUCKNOW

The tech trends in recent years have reshaped how business operate. Emerging trends and technologies continue to appear and evolve. The tablets, smart phones, and other devices continue to be marketed in a consumer-like manner. The smaller size of data centers and the advent of personal clouds are making the use of mobile devices more practical. Devices have become efficient communication portals and enable employees to work and interact with business systems from just about anywhere. More storage, bandwidth, and other resources are being fit into tighter rack space. Energy consumption is becoming more efficient as well. Companies are growing their assets without taking up more physical space. New wireless radio technologies are expected to emerge as well, pushing aside many familiar cellular methods and systems.

In the midst of IT revolution Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. With costs to the global economy running to billions of dollars, new types of cyber crimes are emerging day by day. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing criminal organizations working with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. Highly complex, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

In such a scenario all individuals, especially bankers have to learn methods of curbing such crimes.

I am happy that PNBIIT Lucknow has come out with the journal 'e-track' on quarterly basis and is focusing attention of the readers on various crucial aspects of Banking Technology. This will add to the knowledge of banking fraternity towards IT innovations, security measures and will finally benefit the society as a whole.

I wish success to PNBIIT and e-track in its endeavor to educate people.

Arvind Tiwari
Field General Manager
Punjab National Bank
FGMO, Lucknow

MESSAGE FROM THE DESK OF DIRECTOR

Banking sector has undergone a sea change in the last two decades. These years have witnessed deregulation, liberalization and evolution of Core Banking Solutions. The Banking system has absorbed Information Technology fast and deep thus facilitating real time solutions, spectrum of customized products, handling of very large volumes of sensitive financial transactions, and managing critical financial data. This has created a need for qualified personnel not only for operations but also to manage critical installations like Data Centers, Network Centers and Security Operation Centre etc as well as for developing and upgrading products and services. As a consequence, banks are faced with the twin challenges of upgrading the skills of employees from being pure bankers to techno- bankers and scouting for next generation of bankers possessing technical skills inherently.

In line with vision of the bank, Punjab National Bank Institute of Information Technology, Lucknow is running " Advanced Diploma in Banking Technology " (ADBT) programme that prepares fresh B Tech & MCA pass outs to be employable as next generation bankers. Inputs include Banking & Financial System, Credit Appraisal, Financial Analysis, Project Evaluation, Legal Aspects, various Products & Services, Core Banking Operations, and Advanced Concepts of Operating Systems such as Linux, Data Based Management System (Oracle-10 g), Network Management and Soft Skills etc for all round development.

Since the year 2010-2020 is witnessed as a retirement year in Banking Industry but there is great need of skilled bankers who are trained in banking software. PNBIIT is coming out with a "certificate course in Banking Technology" (CCBT) that prepares graduates in any discipline to become smart next generation bankers of future.

These programs are conducted through a mix of classroom instructions, hands on exercises, tutorial and assignments, case studies, interaction with Industry experts and project work/ internship. The course equips the students to be ready to deliver from day one to prospective employers i.e. banks and BFSI sectors.

Apart from these PNBIIT offers customized software / Financial trainings to bankers and also conducts skill development programs for various personnels.

PNBIIT's mission is to make it a self sustaining Institute of International standards having the status of a deemed university and having organic linkages with other national and transnational academic Institutions in the area of IT, in various fields of universal banking.

To increase the IT knowledge of readers, PNBIIT is bringing out quarterly journal 'etrack' . The theme of this issue is very apt, considering the fact that Digital India has been inaugurated by honourable Prime Minister Mr. Narendra Modi on 1st July ,2015. Government is emphasizing on digital transactions considering the volume of transactions for customer's convenience. E commerce will provide impetus to the business which in turn will improve the economy. But security of transactions is one of the important issue which has to be looked into.

PNBIIT is in the process of establishing Forensic Lab along with innovative courses to spread the knowledge to counter menace of ever increasing cyber crimes.

Shri P S Ganapathy
Director –PNBIIT
Email: psganapathy@pnbiit.ac.in

CYBER CRIMES

PS Ganapathy

INTRODUCTION

The advancement of technology has made organisations dependent on Internet for all their needs. Internet has given easy access to everything while sitting at one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that one can think of can be done through the medium of internet. Internet is used in almost every sphere. With the development of the internet and its related benefits also developed the concept of cyber crimes. Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

WHAT ARE CYBER CRIMES

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electro-nic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

DIFFERENT KINDS OF CYBER CRIMES

The different kinds of cyber crimes are:

1. Unauthorized Access and Hacking: Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network.

2. Web Hijacking: Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over website and its content.

1. Cyber Stalking: In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

How do Cyber Stalkers operate?

a) They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information.

b) The stalker may post this information on any website related to sex services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

c) People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

d) Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

e) Track the victim to his/her home.

2. Denial of service Attack: This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known

5. Virus attacks: Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse,

Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious.

6. Software Piracy: Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc. Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

7. Salami attacks : These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer.

8. Phishing: Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has.

9. Sale of illegal articles: This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

10. Online gambling : There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

11. Email spoofing : Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

12. Cyber Defamation: When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's

friends, it is termed as cyber defamation.

13. Forgery: Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

14. Cloning of Cheques: Signatures and cheque numbers are of authorized people but the amount and payee is tampered. When cheque comes in clearing, it looks like genuine cheque but without verification authorization is done and cheque is cleared. With the implementation of CTS, the authorization of cheque should have mechanism to avoid cloning as it is very easy to clone the cheque in CTS. RBI has issued guidelines to all the banks to send SMS alerts when the cheque is presented in clearing.

15. Theft of information contained in electronic form : This includes theft of information stored in computer hard disks, removable storage media etc.

16. Email bombing : Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

17. Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

18. Internet time theft : Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

19. Theft of computer system : This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

20. Physically damaging a computer system: This crime is committed by physically damaging a computer or its peripherals.

21. Breach of Privacy and Confidentiality: Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information. Confidentiality means non disclosure of information to unauthorized or

unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

22. Data diddling (Post): Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

23. E-commerce/Investment Frauds: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered.

24. Skimming: It is a process in which small scanner attached to a card slot on ATMs, which can pass off as a part of structure. The devices scan a card before it enters the slot. The information thus collected is used for online fraud on international transaction where pin is not mandatory or, the pin is obtain by shoulder surfing and the card and CVV number is cloned and used in other ATMS and transactions.

25. Cyber Terrorism: Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons. a) It is cheaper than traditional terrorist methods. b) Cyber terrorism is more anonymous than traditional terrorist methods. c) The variety and number of targets are enormous. d) Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.

26. VISHING: This involves use of a voice over internet protocol (VOIP). The Victims gets a call where an automatic recording informs that their card is showing fraudulent activity and caller wants to authorize its blocking. To do this customer is asked to punch their card

details. In some cases part of the details is already available and fraudster asks for remaining credentials.

27. Pornography: Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

28. Child Pornography: The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet.

29. Malware: This kind of fraud largely strikes retail chains that maintain a database of a customer's credit card numbers. Such a fraud is perpetuated by infusing a software into a retailer's server. The software not only searches the database but also scrapes the read-only memory whenever card details are flashed. This kind of fraud does not take place in standalone credit card swipe machines but in outlets where these devices are connected to a retailer's cash registers.

30. Man-in-the-middle (MITM): Everyone loves free WiFi even fraudsters. An MITM attack typically takes place when the hacker plugs into the same WiFi network as the victim. He then uses a set of programs to redirect the victim's data through his machine. While this is happening, he uses other software to scan the data for banking related credentials. Such frauds can be prevented by the victim at the outset as usually his browser issues a warning on the security certificate and gives him an option whether he wants to proceed. It is always safer to say 'No'.

REFERENCES

http://www.helplinelaw.com/family-law/CCII/cyber-crimes-in-india.html
http://www.cyberorgindia.com/2uncategorised/26-joomla-license-guidelines

Shri P S Ganapathy
Director at PNBIIT Lucknow

MODUS OPERANDI OF BANKING CYBER CRIME

Satyendra Sharma

Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause economical, physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet, mobile phones or any other electronic communications are called Cyber Crimes. Such crimes may threaten a nation's security and financial health.

Cyber Crime is a term for any illegal activity that uses a computer as its primary means of commission. Cyber Crimes include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes include crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes.

Types of Cyber Crimes

Hacking- Hacking in simple terms means illegal intrusion into a computer system without the permission of computer owner/user.

Phishing- It is technique of pulling out confidential information such as credit card/debit card, online banking details or account details from the account holder by deceptive means.

Spoofing- Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.

Denial of Service Attack (DOS)- This is an act by the criminal, who floods the bandwidth of the victim's network or fills his email box with spam mails depriving him of the services he is entitled to access or provide.

Software Piracy- Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

Cyber Defamation- Cyber criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website.

Virus Dissemination- Malicious software that attaches itself to other software.

Pornography- Publishing or transmitting any material in electronic form which is obscene and lascivious in nature is known as pornography.

Credit Card/Debit Card Fraud- Cyber criminals steal the credit card/debit card details such as card number, CVV code or

expiry date of the card using various techniques such as by card skimmer, phishing etc. and do online transaction.

Net Extortion- Copying the company's confidential data in order to extort said company for huge amount is called Net Extortion.

Cyber Stalking- The Criminal follows the victim by sending emails, entering the chat rooms frequently.

Salami Attack- In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. Criminal makes such program that deducts small amount like Rs. 1.00 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

Cyber Squatting- Cyber squatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. It generally refers to the practice of buying up domain names that use the names of existing reputed businesses with the intent to sell the names for a profit to those businesses.

DNS Poisoning- Domain name system (DNS) poisoning or DNS cache poisoning, is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. At that point, a worm, spyware, Web browser hijacking program, or other malicious programmes can be downloaded to the user's computer from the rogue location.

Pharming- Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

Some Common Modus Operandi of Banking Cyber Crimes

Modus Operandi 1: Shoulder Surfing:

In Information Technology security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and other sensitive personal data.

Occurrence:

Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:

» Fill out a form.
» Enter PIN at ATM or a POS terminal.

» Enter password at a cyber cafe, public and university libraries, or airport kiosks.

» Enter secret code for a rented locker in a public place such as a swimming pool or airport.

Case 1- Debit/Credit card details, Internet Banking user ID and password can be stolen by illegitimate persons using shoulder surfing. In this case when legitimate user performs online transaction using Internet Banking or using Debit Card/Credit Card, illegitimate persons who stand close enough to the genuine user can capture sensitive information like credit card/debit card number, expiry date of the card, CVV (Code Verification Value) number, PIN, 3D secure code, name of the card holder, internet banking user ID and password etc. Once they get requisite details online transaction can be done easily by them.

Preventive Steps:

» Don't use cyber café or kiosk for online transaction because these are not safe.

» Don't make online transaction at crowded place.

Corrective Steps:

» Change the internet banking password or 3D secure password immediately at the first available opportunity as done to the above event as soon as possible after using cyber café for online transaction.

Modus Operandi 2: Card Swapping:

Nowadays, credit card/debit card swapping during withdrawals, inquiries and Point-of-Sale (POS) transactions is common act performing by illegitimate persons. When legitimate card holder wants to withdraw amount from ATM but does not have sufficient knowledge about functioning of ATM, then illegitimate person stands too close to the legitimate ATM card holder approaches to the legitimate card holder for assisting in withdrawal of amount and thus he interchanges his ATM card with legitimate person's ATM card.

Preventive Steps:

» Don't take assistance from unknown persons for operating ATM.

» Don't give your credit card/debit card to strangers.

» If you are unable to operate ATM, you may take assistance of security guard of ATM.

Modus Operandi 3: Card Skimming:

Card skimming is the illegal copying of information from the magnetic strip of a

credit card or ATM card using an electronic device called card skimmer. A skimmer can be fixed in the ATM slot for copying data from the card to make its duplicate and then steal money. The scammers try to steal your details so that they can access your bank accounts. Once scammers have skimmed your card, they can create a fake or 'cloned' card with your details on it. The scammers are then able to use your account. The skimmer does not have a camera but have a serial interface that can be used for retrieving stolen data through a computer or some other device. It had a small magnetic card reader head which copies the data when the card passes through it. "The skimmer has a tiny microcontroller for processing and a flash disk capable of storing large data. This meant that it could store information stolen from up to thousands of cards. Skimmer also has a mini-USB port for transferring the stolen data to a computer. The whole electronics is to be powered by a tiny lithium ion battery which can keep the skimmer running for several days.

Warning Signs:

» A shop assistant takes your card out of your sight in order to process your transaction.

» You are asked to swipe your card through more than one machine.

» You see a shop assistant swipe the card through a different machine to the one you used.

» You notice something suspicious about the card slot on an ATM (e.g. an attached device).

» You notice unusual or unauthorised transactions on your account or credit card statement.

Preventive Steps:

» Keep your credit card and ATM cards safe.

» Do not share your personal identity number (PIN) with anyone.

» Do not keep any written copy of your PIN with the card.

» Check your bank account and credit card statements when you get them. If you see a transaction you cannot explain, report it to your credit card provider or bank.

» Choose passwords that would be difficult for anyone else to guess.

» If you are using an ATM, take the time to check that there is nothing suspicious about the machine.

» If you are in a shop and the assistant wants to swipe your card out of your sight, you should ask for your card back straight away and either pay with cash, or not make the purchase.

» If an ATM looks suspicious, do not use it and report to the Bank.


Small Card Skimmer


Card Skimmer in ATM

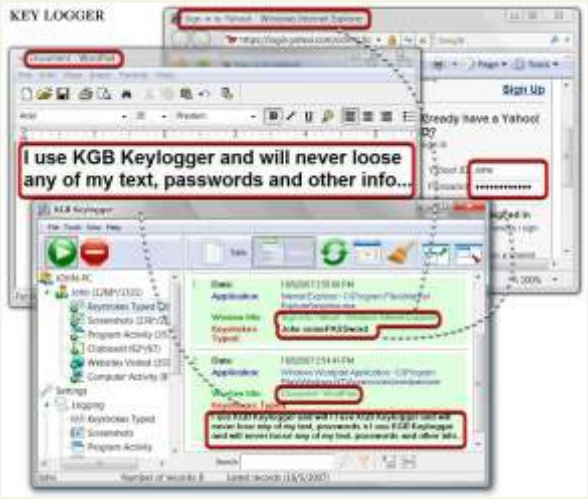
Modus Operandi 4: Spyware and Key Logger:
Spyware is a type of software that spies on what you do on your computer. Key logger is a type of spyware that records what keys you press on your keyboard. Scammers can use them to steal your online banking passwords or other personal information. Scammers can install key logger software in the computers of cyber cafe and capture all key strokes along with the name of application. It also captures the window captions and all URLs (Uniform Resource Locator) visited with a web browser. Scammers can view all the pages visited by the computer users and easily access the debit card/credit card details, PIN, 3D secure password, internet banking user ID and password of the genuine Bank account holder. In key logger, 'Turn on Automatic Screenshot Capture' facility is also available. Generally fraudsters receive the key logger reports through e-mail.

Preventive Steps:

· For identification of key logger open Control Panel--->Add or Remove Programs
Here all installed programs will be displayed. You can identify here Key logger is installed or not.

» If Key logger is being displayed (installed) here, you can uninstall it by selecting Key logger program and clicking on Remove button.

» Always use updated antivirus which will prevent from installing key loggers in your system.



Satyendra Sharma is certified cyber crime Investigator and presently posted as Sr Manager (IT) at PNBIIT

CYBERCRIME CONNECTING WITH BIG DATA

Dr. Parul Verma

1. Introduction

Cybercrime refers to any illegal activity through the computer as primary means, as well as any illegal activity that uses a computer for the storage of evidence. It include crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism.

In this digital age where every person is online 24x7, where online communication is no more need but a norm, all users are the targets of cybercrime. With the advancement in technology, cyber criminals are also moving on their focus and targets. The users and the organizations related to some financial services are the most eligible targets for the cyber criminals.

As per the reports of Global Trade Review (GTR), the conventional Information Technology (IT) approach is no more effective for the financial institutions. The institutions require customized solutions which are made specifically for each class on their transactions. Financial services are prone to the cyber attacks. The frequency of such attacks is increasing day by day. The high level security measures are taken in consideration by financial institution still the security is at breach.

The New York Department of Financial Services queried 154 financial institutions about their cyber security programs, costs and future plans. The objective of the survey was to gain a general perspective of the financial services industry's efforts to prevent cybercrime, protect consumers and clients in the event of a breach, and ensure the safety and soundness of their organizations. The subsequent report issued by the Department found that cyberattacks against banks are “becoming more frequent, more sophisti-cated, and more widespread.” The report also indicated that smaller institutions such as community and regional banks, credit unions, money transmitters and third-party service providers such as credit card and payment processors have experienced attempted breaches.

The number of cybercrimes in India may touch 300,000 in 2015, almost double the level of last year, causing havoc in the financial space, security establishment and social fabric, a study said. "What is causing even more concern is that the origin of these crimes is

widely based abroad in countries including China, Pakistan, Bangladesh and Algeria among others," D.S Rawat, secretary general, ASSOCHAM said while releasing the joint ASSOCHAM-Mahindra SSG study "Cyber and Network Security Framework".

The various studies done by the agencies clarify the state of cybercrime in India and other countries as well. The reports say that the cybercrimes are going to grow annually.

2. Big Data

Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. Since Big Data is a massive data which can be used as potential resource for enterprises looking to enhance their business operations. There are many Data analytics tools that are used to predict latest market trends.

3. Cybercrime and Big Data

Big Data Analytics is working like a two sides of coin. At one end IT security professionals should effectively identify patterns in network activity that would not be noticed by traditional defensive protocols. At another end cybercriminals are working to break such defensive protocols. The battle between cybercriminals and security professionals has largely been an arms race, with one side releasing a new weapon or defense and the other responding with a direct counter method.

The report noted that criminals now move more quickly to commit cybercrime. Just a couple of years ago, hackers often did extensive cyber espionage and then went in for the theft—either money or information. Now, faced with more effective security and fraud prevention measures, they “simply go directly to the theft without a drawn-out reconnaissance phase.

Cybercriminals are getting smarter day by day they are also using Big Data principles to enhance their efficiency. They developed better tools to analyze and monetize the patterns of the voluminous data. In addition to leveraging Big Data analytics to quickly sift through volumes of data, cybercriminals are using these tactics to derive intelligence from their collections of information to better understand trends and effectiveness of attacks. This enables cybercriminals to make better decision for future attacks and investments as they learn more about infected machines, and the success of their existing malicious applications.

4. Tools Used by Cyber Criminals based on Big Data methodologies

Technology is growing day by day and using such technologies cyber criminals are also getting smarter. They are applying Big Data

methodologies in their various operations.. Few of the tools are as follows-

a) IntelegentBot

The "IntelegentBot" log parser plugin, is designed to help a cybercriminal operating a botnet (botmaster) query their databases for valuable data. This web-based platform allows botmasters to connect to their Trojan databases and search for specific words such as bank URLs or names. It also allows botmasters to search for only credit card data. Through the use of this plugin botmasters are able to quickly and easily mine and monetize credit card data, for example. Although some search options are part of basic botnet admin panels, this one is a commercial, standalone interface that can be adapted to different Trojans.

b) IntelegentBot Query Command Box

The "Money Panel" is designed to steal only credit card data and parse into a separate database. This second plugin uses a special set of web injections specifically targeting credit card data, 16 numerical characters. The web injection displays when a victim accesses a specific sites, such as a bank site or Facebook. As soon as a victim enters their card information into the injected field, the data is collected, but instead of reaching the cluttered log repository, it is sent to a separate database in a remote server.

c) Administrative Panel

The sophistication, agility, and speed at which a cybercriminal operates and monitors their fraudulent information have improved through the use of Big Data analytics. Cybercriminals can now sort their collections of data more quickly to extract financial details and view performance metrics for current malware applications. This is certainly a trend to keep an eye on. As cybercriminals continue to master the concepts of Big Data and apply it to their operations, their cyber-attacks stand to become more effective. To combat these attacks, businesses will need to use intelligence-driven solutions that also leverage big data to deliver timely, actionable security decisions.

5. The other side of coin the defensive one

The security professionals can exploit real-time big data analytics programs to identify patterns in network activity which is somehow cannot be observed by traditional defensive protocols. The war between cybercriminals and security professionals is getting interesting day by day where releasing a new defensive weapon by them is counter attacked by the cyber criminals. What this amounts to is the proliferation of anti-virus tools that have very specific functions. With big data's superior processing power, analytics software could monitor network

traffic to identify changes that might suggest the presence of malware.

Data analytics tools could also be used to determine what malware poses the greatest threat to a business' network. By analyzing different factors such as the defensive systems in place and comparable networks' breach rates, big data software could identify a business' largest vulnerability. With that information, security professionals could take steps to improve network defenses.

Cybersecurity is a major concern these days for IT professionals. It is now moved on to the big data problem because of the volume of the data and its complexity. It is difficult now to analyze such complex data using traditional security tools. Using a Hadoop architecture, IT departments can create data analytics programs that monitor network defenses in real time. Without data bottlenecks to slow down processing speeds, security professionals using Hadoop tools can create quick and effective analytics-based solutions.

Apache Hadoop is an open source software framework for storage and large scale processing of data-sets on clusters of commodity hardware. Hadoop is an Apache top-level project being built and used by a global community of contributors and users.

6. Conclusion

It is an endless war between cybercriminals and the IT Professionals. IT professionals are trying their hands on Big Data Analytics to identify the patterns and structures of the threat. At the other end cyber criminals are using same Big Data for their own purpose. So basically it is big data which is helping both of them at either end. The solutions need to be found to make a constructive use of Big Data Analytics.

References:

1. http://zeenews.india.com/news/sci-tech/cyber-crimes-in-india-may-double-in-2015-study_1524563.html
2. https://blogs.rsa.com/cybercriminals-big-data-analytics/
3. https://blogs.rsa.com/cybercriminals-big-data-analytics/
4. http://hortonworks.com/big-data-insights/using-big-data-to-combat-cybercrime/
5. http://www.hosting.com/financial-institutions-face-challenges-with-cyber-security/
6. http://opensource.com/life/14/8/intro-apache-hadoop-big-data

Dr. Parul Verma is Professor at Amity University Lucknow

CYBER FORENSICS

Pratima Trivedi

Is the art and science of applying computer science to aid the legal process. With the rapid progress in technology, it quickly became more than just an art though. It is much more than the technological, systematic inspection of the computer system and its contents for evidence or supportive evidence of a civil wrong or a criminal act.

Computer forensics requires specialized expertise and tools that goes above and beyond the normal data collection and preservation techniques available to end-users or system support personnel. It is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Mostly, computer forensics experts investigate data storage devices; these include, but are not limited to hard drives, portable data devices (USB Drives, External drives, Micro Drives and many more). Such forensics experts identify sources of documentary or other digital evidence, preserve the evidence, analyze the evidence and presents the findings. It is done in a fashion that adheres to the standards of evidence that are admissible in a court of law. It is techno-legal in nature rather than purely technical or purely legal.

It is absolutely vital for the forensics team to have a solid understanding of the level of sophistication of the suspect(s). If insufficient information is available to form this opinion, the suspects must be consi-dered to be experts, and should be presumed to have installed counter-measures against forensic techniques. Because of this, it is critical that the person has to view the equipment to be as indistinguishable as possible from its normal users until he has shut it down completely.

Evidence can be collected from variety of sources. It can be from the workstation, server or the network connecting it.

Like any other piece of evidence, used in an investigation, the information generated by a computer forensics investigation, must follow the standards of admissible evidence. Special care must be taken when handling suspect's files. Dangers to the evidence include viruses, electromagnetic or mechanical damage etc.

There are a handful of cardinal rules that are used to ensure that the evidence is not destroyed or compromised:

1. Tools and methods that have been tested

and evaluated to validate their accuracy and reliability can only be used. In order to verify that a tool is forensically sound, the tool should be tested in a mock forensic examination to verify the tools performance. There are government agencies such as the Defense Cyber Crime Institute that accept requests to test specific digital forensic tools and methods for government agencies, law enforcement organizations, or vendors of digital forensic products , free of cost.

2. The original evidence should be handled in a manner so that there is no change in data.

3. The chain of custody should be established and maintained.

4. Everything done should be documented

If such steps are not followed the original data may be changed, ruined or become tainted, and so any results generated will be challenged and may not hold up in a court of law.

If in any investigation , where the owner of the digital evidence has not given consent to have his or her media examined – as in most criminal cases – special care must be taken to ensure that one should as a forensic specialist, have legal authority to seize, image, and examine each device. Besides having the case thrown out of court, the examiner may find him or herself on the wrong end of a hefty civil lawsuit. As a general rule, if one is not sure about a specific piece of media, one should not examine it. Amateur forensic examiners should keep this in mind before starting any unauthorized investigation.

Some of the most valuable information obtained in the course of a forensic examination will come from the computer user themselves. In accordance with applicable laws, statutes, organizational policies, and other applicable regulations, an interview of the computer user can often yield invaluable information regarding the system configuration, applications, and most important, software or hardware encryption methodology and keys utilized with the computer. Forensic analysis can become exponentially easier when analysts have passphrase(s) utilized by the user open encrypted files or containers used on the local computer system, or on systems mapped to the local computer through a local network.

Unless completely unavoidable, data should never be analyzed using the same machine it is collected from. Instead, forensically sound copies of all data storage devices, primarily hard drives, must be made.

To ensure that the machine is analyzed completely, following sequence of steps must be followed:

Examine the machine's surroundings

The collection phase starts off with the

computer forensic team analyzing its surroundings. A USB key drive, XD Picture Card, Secure Digital card etc can be some of these. Similar to police investigating a crime in any other case, all printouts, disks, notes, and other physical evidence must be collected to take back to the laboratory for analysis. The investigating team must take digital photographs of the surrounding environment before any of the hardware is dealt with. This initial collection phase sets the tone for the rest of the investigation and therefore the evidence must be locked away securely, with limited access granted to authorize team members only.

Examine the Live System and record open applications

If the machine is still active, any intelligence which can be gained by examining the applications currently open should be recorded. If the machine is suspected of being used for illegal communications, such as terrorist traffic, not all of this information may be stored on the hard drive. If information stored solely in RAM is not recovered before powering down it may be lost, so acquiring the data while the RAM is still powered is a priority.

For most practical purposes, it is not possible to completely scan contents of RAM modules in a running computer. Though specialized hardware could do this, the computer may have been modified to detect chassis intrusion (some Dell machines, for example, can do this stock; software need only monitor for it) and removing the cover could cause the system to dump the contents. Ideally, prior intelligence or surveillance will indicate what action should be taken to avoid losing this information.

Several Open Source tools are available to conduct an analysis of open ports, mapped drives (including through an active VPN connection), and of significant importance, open or mounted encrypted files (containers) on the live computer system. Additionally, through Microsoft's implementation of the Encrypted File System (EFS), once a system is powered down, the difficulty to examine previously mounted EFS files and directory structures is substantially increased. Utilizing open source tools and commercially available products, it is possible to obtain an image of these mapped drives and the open encrypted containers in an unencrypted format. For Windows based systems, these Open Source tools include Knoppix and Helix. Commercial imaging tools include Access Data's Forensic Tool Kit and Guidance Software's Encase application. Both companies make available their imaging tools for free; however, in order to analyze the data imaged using these tools

one will need to purchase a full licensed version of the application.

The aforementioned Open Source tools can also scan RAM and Registry information to show recently accessed web-based email sites and the login/password combination used. Additionally these tools can also yield login/password for recently access local email applications including MS Outlook.

With MS most recent addition, Vista, and Vista's use of BitLocker and the Trusted Platform Module (TPM), the importance of developing procedures for examining and imaging live (mounted unencrypted) systems is anticipated to significantly increase.

It is possible that in utilizing tools to analyze and document a live computer system that changes can be made to the content of the hard drive. During each phase of system analysis, the forensic examiner must document what they did and why they did it. Specifically, the examiner should detail the potentially perishable information that can/will be lost during a system power down process. The examiner must balance the need to potentially change data on the hard drive versus the evidentiary value of such perishable data.

The data that is most likely to be modified or damaged first should be captured first. The order of volatility is.

1. Network connections

Network connections can close quickly and often leave no evidence of where they were connected to or the data being transferred.

2. Running Processes

It is important to note which programs are running on a computer before further analysis is conducted.

3. RAM

The systems Random Accessing Memory contains information on all running programs as well as recently run programs. The information that can be gained from the system ram includes Passwords, encryption keys, and personal information and system and program settings.

4. System settings

The Operating system settings can now be extracted. This includes user lists, currently logged in users, system date and time, currently accessed files and current security policies.

5. Hard Disk

The hard disk can then be imaged. It is important to note that it is not forensically sound to image a hard drive while it is running live unless there are extenuating circumstances.

Power down carefully

If the computer is running when seized, it should be powered down in a way that is least

damaging to data currently in memory and that which is on the hard disk. The method that should be used is dependent on many differing values, such as the operating system in use, and the role of the computer to be seized. Performing a proper shut down may cause malicious scripts to be run, or volatile data to be lost. On the other hand, removing the power plug may cause corruption of the file system or loss of crucial data.

Fully document hardware configuration

Completely photograph and diagram the entire configuration of the system. Note serial numbers and other markings. Pay special attention to the order in which the hard drives are wired, since this will indicate boot order, as well as being necessary to reconstruct a RAID array.

Duplicate the electronic media (evidence)

The process of creating an exact duplicate of the original evidentiary media is often called Imaging. Using a standalone hard-drive duplicator or software imaging tools such as DCFLdd or IXimager, completely duplicate the entire hard drive. This should be done at the sector level, making a bit-stream copy of every part of the user-accessible areas of the hard drive which can physically store data, rather than duplicating the file system. Be sure to note which physical drive each image corresponds to. The original drives should then be moved to secure storage to prevent tampering.

Usually some kind of hardware write protection should be there, to ensure that no writes will be made to the original drive. Even if operating systems like Linux there , a hardware write blocker is usually the best practice.

There are two goals when making an image:

Completeness (imaging all of the information)

Accuracy (copying it all correctly)

The imaging process is verified by using the SHA-1 message digest algorithm (with a program such as sha1sum) or other still viable algorithms. To make a forensically sound image, you need to make two reads that result in the same output by the message digest algorithm. Generally, a drive should be hashed in at least two algorithms to help ensure its authenticity from modification in the event one of the algorithms is cracked. This can be accomplished by first imaging to one tape labeled as the Master and then make an image labeled Working. If onsite and time is critical, the second read can be made to Null.

E-mail review

E-mail has become one of the primary mediums of communication in the digital age, and vast amounts of evidence may be contained therein, whether in the body or

enclosed in an attachment.

Forensics experts use review tools to make copies of and search through e-mails and their attachments looking for incriminating evidence using keyword searches. Some programs have been advanced to the point that they can recognize general threads in e-mails by looking at word groupings on either side of the search word in question.

Thus cuber forensic pertains to legal evidence found in computers and digital storage media. Some of the important cyber forensic tools are

1. Win-LiFTImager

USB based tool for First Responders, Investigators and IT Security Professionals to collect volatile data, which will be lost once the computer system is shutdown

2. TrueBack

TrueBack is a cyber forensics software tool for digital evidence seizure and acquisition (Disk imaging).

3. F-DAC- Forensic Data Carving Tool

Data Carving is a technique used in the field of Cyber Forensics when data cannot be identified or extracted from media by any simple procedure due to the fact that the desired data no longer has file system allocation information available to identify the sectors or clusters that belong to the file or data.

4. F-RAN- Forensic Registry Analyzer Tool The Windows Registry is an important source of evidence for examiners in the field of computer and digital forensics.

5. Mobile Check Analyzer

Mobile Check Analyzer is a digital forensic imaging tool for WinCE/Pocket PC/ Windows Mobile/ Blackberry/Symbian and Palm OS PDAs/ Mobile Phones and Smartphone.

6. NeSA- Network Session Analyzer

The importance of Network Forensics tools are increasing as the cyber crimes related to computer network are increasing at a rapid rate.

References :

http://www.cyberforensics.in/?AspxAutoDetectCookieSupport=1

http://www.cyberlawsindia.net/computer-forensics2.html

http://en.wikipedia.org/wiki/Computer_forensics

http://cdac.in/index.aspx?id=cs_cf_cyber_forensics

Pratima Trivedi is
Chief Faculty at PNBIIT Lucknow

SECURITY USING DIGITAL CERTIFICATE

Raman Verma

Digital Certificate is one of the foundations of a public key infrastructure (PKI). It is the electronic equivalent of a passport or driver's license, and may be used to identify and authenticate someone making online transactions.

What is a Digital Certificate?

In cryptography, a digital certificate (also known as public key certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity and the digital signature of an entity that has verified the certificate's contents are correct.If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner(a self-signed certificate) or other users("endorsements") whom the person examining the certificate might know and trust.

Certificates are an important component of Transport Layer Security (TLS), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications such as email encryption and code signing.

Contents of a typical Digital Certificate:

» Serial number: Use touniquely identify the certificate.

» Subject: The person or the entity identified.

» Signature Algorithm: The algorithm used to create the signature.

» Issuer: The entity that verified the information and issued the certificate.

» Valid-From: The date, the certificate is first valid from.

» Valid-To: The expiration date of

certificate.

» Key-usage: Purpose of the public key (e.g. encipherment, signature, certificate signing)

» Public key: A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

» Thumbprint Algorithm: The algorithm used to hash the public key certificate.

» Thumbprint (also known as fingerprint) The hash itself, used as an abbreviated form of the public key certificate.

Verisign (Internet Services Company) uses the concept of classes for different types of digital certificates:

» Class-1 for individuals, intended for email.

» Class-2 for organizations, for which proof of identity is required.

» Class-3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.

» Class-4 for online business transactions between companies.

» Class-5 for private organizations or governmental security.

Other vendors may choose to use different classes or no classes at all as this is not specified in the PKI standards.

Certificate authority:

A certificate authority (CA) is a trusted third-party, trusted by both the subject (owner) of the certificate and by the party relying upon the certificate.

Certificates and website security:

The most common use of certificates is for HTTP-based websites. A web browser validates that a TLS (Transport Layer Security) web server is authentic so that the user can feel secure that his/her interaction with the web site has no eavesdroppers and that the web site is who it claims to be. This security is important for electronic commerce. In practice, a web site operator obtains a certificate by applying to a certificate provider (a CA that presents as a commercial retailer of certificates) with a certificate signing request. The certificate provider signs the request thus producing a public certificate. During web browsing, this public certificate is server to any web browser that connects to the web

site and proves to the web browser that the provider believes it has issued a certificate to the owner of the web site.

Before issuing a certificate, the certificate provider will request the contact email address for the web site from a public domain name registrar, and check that published address against the email address supplied in the certificate request.

A certificate provider can opt to issue three types of certificates, each requiring its own degree of vetting rigor. In order of increasing rigor(and naturally, cost) they are: *Domain Validation, Organization Validation and Extended Validation.* These rigors are loosely agreed upon by voluntary participants in the CA/ Browser Forum.

Domain Validation:

A certificate provider will issue a Domain Validation (DV) class certificate to a purchaser if the purchaser can demonstrate one straightforward vetting criterion: the right to administratively manage the domain name in question. For example, a domain name registrar might sell (or more accurately, resell) DV certificates through their domain name management system.

Organization Validation:

A certificate provider will issue an Organization Validation (OV) class certificate to a purchaser if the purchaser can meet two criteria: the right to administratively manage the domain name in question, and perhaps, the organization's actual existence as a legal entity. A certificate provider publishes its OV vetting criteria through its Certificate Policy.

Extended Validation:

To acquire an Extended Validation (EV) certificate, the purchaser must persuade the certificate provider of its legitimacy by surviving a battery of complex vetting criteria, the majority of which are manually performed. As with OV certificates, a certificate provider publishes its EV vetting criteria through its Certificate Policy.

Note: Browsers will generally offer users a special visual indication when a site presents an EV certificate. For example, it might change the background color of the URL bar from neutral to green. In this way, the user can decide whether or not to more readily trust the site as being legitimate.

How does a Digital Certificate work?

When sending message over the Internet, the

public key encryption may be used.

Public key encryption is the use of complex mathematical formulas to make data unreadable. Under public-key encryption, two different keys are used, one for encrypting the data and a second key to decrypt it.

Someone wanting to send a message would request the recipient's digital certificate, which contains the public key, from a trusted directory, and use the public key to encrypt the message before sending. Once the message is encrypted it can only be decrypted using the intended recipient's private key.

The sender can also digitally sign the message using their own private key to prove that the message originated from them. If the message has been digitally signed the recipient would verify the sender by obtaining the sender's digital signature.

The effectiveness and reliability of the digital certificate is based on the confidence all parties to a transaction have in the structure, policies and procedures surrounding the PKI system.

References

» Book - IT Audit

» Banking & Technology –R.K. Uppal.

» www.anz.com

» www.slideshare.net/mobile/omidazg/session7-securing-information-systems

» www.wikipedia.org

Raman Verma is B Tech and student of ADBT Batch 8th of PNBIIT

"If you don't like something, change it.

If you can't change it, change your attitude. Don't complain."

MOBILE BANKING SECURITY

Rupal Srivastava

A compromised mobile device provides easy entry to a wealth of personal information apps, contact lists, email, call history and social media accounts are all readily accessible to anyone with physical or programmatic control of the device. Couple this with the natural tendency of humans to snoop around when they find something that isn't theirs, and we have a security risk that stems not only from professional criminals but also the "average Joe." In a recent experiment, Symantec purposefully "lost" 50 smartphones in public areas. Of those lost smartphones, 96% were accessed by their finders, and 80% of the finders tried to access files clearly marked with sensitive corporate or personal information.

Threats to Mobile Banking :

Combine the effectiveness of these brute force attacks with the fact that passwords are often forgotten, easy toguess, and habitually reused, and you can see the fallacy in thinking user names and passwords alone are enough to keep your banking application safe if you happen to lose your Smartphone or tablet.

As with most types of online security, risks often come down to customer behavior. It is impossible to prevent customers from choosing easy passwords to guess or reusing them across multiple sites. It is also impossible to control what they search for on the internet using their mobile device, what sort of applications they download, and where they download these applications from. As it has been said time and time again, end-user browsing behavior is the Achilles' heel of fraud prevention.

Cybercriminals trick unsuspecting Smart-phone and tablet owners into inadvertently and voluntarily downloading Malware *(Criminalshave a number of tools at their disposal to infect a customer's computer with malicious software or Malware)* onto their device.

Third-party app stores are particularly susceptible to having Malware embedded in applications. Though both iOS and Android systems have their vulnerabilities, Juniper

Research found that 92% of all the malware they discovered was directed at the more open Android platform. in 2012, an application called "Android Security Suite Premium" was one such application identified as malware. Posing as a security product, the application was actually used to intercept and steal text messages. Considering one time passwords are often sent as text messages to mobile phones, these types of malware are particularly disconcerting.

Downloading an app disguised as malware, However, is just one method cybercriminals are turning to in order to infect mobile devices. Fictitious SMS text messages, malicious links that are cleverly designed to take advantage of smaller screens, exploiting open Wi-Fi networks, and "Jailbroken" devices – those that have had theirunderlying operating system tampered with toenable the use of SIM cards from other providers, are just a few of the many threats mobile users face as outlined by the Anti-Phishing Working Group report. As these threats emerge the black market for mobile malware is starting to take shape, and organizations should prepare now to protect their mobile banking applications.

Mobile Fraud Prevention :

As with any fraud prevention strategy, the only true way to protect customers is to have multiple layers of fraud protection.

Safe Browsing for Mobile -

While it is impossible to control the browsing and download behavior of end users, one possibility to reign in the untamed is to adopt a safe browsing solution, such as Easy Solutions' Detect Safe Browsing (DSB) for mobile. DSB for mobile provides a protected channel to web sites that mobile users frequently access. Both end users and mobile banking application managers can set up exactly which sites are to be protected. Customers simple open the DSB application, click on the link they wish to visit, and are directed to the bank site passing through Easy Solutions' protected servers first. This means that even if malware exists on a machine, the banking sessionthrough DSB will be safe.

Device Authentication with the Detect ID Mobile SDK -

It is critical to maintain a high level of security on the mobile channel without adding unnecessary complexity for customers. The mobile channel createsunique security

concerns, but will soon be subjected to the same FFIEC regulations as other channels. Detect ID's Mobile SDK (software development kit) is a library designed to be integrated into any custom mobile banking application for iOS, Android, or Blackberry. Any time a customer download banking application their Smartphone or tablet becomes a mobile authentication credential based on hardware and software variables used to create a unique finger print.

Professional Security Services for Mobile Applications -

Easy Solutions' expert IT team will help to conduct a risk assessment and review the technology used to create the mobile application platform. Some security professionals view the mobile revolution as a chance for the industry to get things right with a clean slate. As with any effective security approach a layered defense is the best and most successful way to keep these new devices malware free. Threats will no doubt emerge and consistently threaten mobile devices, but this is a unique opportunity to get a jump start in protecting your business and customers.

Some Tips :

» Always use a secured Wi-Fi connection, where you have a unique user name and password, before sending any sensitive information over your mobile phone.

» Download your bank's mobile application from a legitimate app store associated with your phone and use it every time, so you can be sure you are visiting the real bank every time and not a copycat site.

» Install anti-malware technology, and back up data regularly.

» Configure your device to auto-lock after a period of time with a password of six-to-eight alphanumeric characters.

» Keep your apps and device software up-to-date.

Rupal Srivastva is B Tech and student of ADBT 8th Batch of PNBIIT

TOOLS TO CURB CYBER FRAUDS

Shubham Saxena

Abstract

This paper examines the issue of frauds from the perspective of banking industry. The study seeks to evaluate the various causes that are responsible for banks frauds. It aims to examine the extent to which bank employees follow the various fraud prevention measures including the ones prescribed by Reserve Bank of India. It aims to give an insight on the perception of bank employees towards preventive mechanism and their awareness to wards various frauds. The study signifies the importance of training in prevention of bank frauds. A strong system of internal control and good employment practices prevent frauds and mitigate losses. The research reveals that implementation of various internal control mechanisms are not up to the mark. The results indicate that lack of training, overburdened staff, competition, low compliance level (the degree to which procedures and prudential practices framed by Reserve bank of India to prevent frauds are followed) are the main reasons for bank frauds. The banks should take the rising graph of bank frauds seriously and need to ensure that there is no laxity in internal control mechanism.

Banks these days are being duped of crores of Rupees, thus destabilizing investor's confidence. The year2005 witnessed the wiping of Rs. 1134.4 crores from the banking industry in India due to bank frauds, which was about 2.5 times the amount lost in the previous year. Banks are dealing with public's money and hence it is imperative that employees should exercise due care and diligence in handling the transactions in banks. Recent rise in bank frauds calls for tightening of security mechanism. A strong system of internal control is the most effective way of fraud prevention. The banks should increase their efforts to raise the level of security awareness in their organizations to combat frauds.

A comparative picture (Table 1) of total number of fraud cases and amount involved as on March 31, 2013 for scheduled commercial banks, NBFCs, Urban Cooperative banks, and Financial Institutions is as under:

Table 1: No. of frauds cases reported by RBI regulated entities

(No. of cases in absolute terms and amount involved in Rs. crores) Category	No. of Cases	Amount Involved
Commercial Banks	169190	29910.12
NBFCs	935	154.78
UCBs	6345	1057.03
FIs	77	279.08
	176547	31401.01

Broadly, the frauds reported by banks can be

divided into three main sub-groups:
a) Technology related
b) KYC related (mainly in deposit accounts)
c) Advances related

A closer examination of the reported fraud cases has revealed that around 65% of the total fraud cases reported by banks were technology related frauds (covering frauds committed through /at internet banking channel, ATMs and other alternate payment channels like credit/ debit/prepaid cards) while the advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds. Table 4 below shows that relatively large value advances related frauds (> Rs. 1 crores) have increased both in terms of number and amount involved over the last four years.

» Identity Theft – The most broadly defined of the three types of online banking fraud, identity theft gets the most attention from the media and is of highest concern to consumers. For example: A collection agency calls and tells a customer that she owes $5,000 in credit card debt. After doing some research, the customer finds that her identity was stolen and that the thief opened several credit card and checking accounts at different banks, passed bad checks, and accessed her online account and transferred the money out via bill pay.

» Friendly Fraud – This kind of fraud, also known as "civil fraud" or "family fraud,"refers to fraud committed using information that belongs to a trusted friend or family member. As much as financial institutions, independent

Table 2: Bank Group wise Advance Related Frauds (Rs. 1 Crores& above in value)
(No. of cases in absolute terms and amount involved in Rs. Crores)

	2009-10		2010-11		2011-12		2012-13		Cumulative total (As at end March 2013)	
Bank Group	**No. of cases**	**Amount Involved**	**No. of cases**	**Amount Involved**	**No. of cases**	**Amount Involved**	**No. of cases**	**Amount Involved**	**No. of cases**	**Amount Involved**
Nationalized Banks including SBI Group	152	736.14	201	1820.12	228	2961.45	309	6078.43	**1792**	**14577.28**
Old Private Sector Banks	16	99.10	20	289.31	14	63.31	12	49.87	149	767.75
New Private Sector Banks	10	63.38	18	234.18	12	75.68	24	67.47	363	1068.18
Sub-total	**26**	**162.48**	**38**	**523.49**	**26**	**138.98**	**36**	**117.34**	**512**	**1835.93**
Foreign Banks	4	45.26	3	33.20	19	83.51	4	16.75	**456**	**277.05**
Grand Total	**182**	**943.87**	**242**	**2376.81**	**273**	**3183.94**	**349**	**6212.51**	**2760**	**16690.26**

Technology related frauds (only online banking included)

Online banking fraud is divided into three categories, each of which poses a unique threat to customers and institutions. The three categories are:

organizations and the media communi-cate to consumers that they should not share confidential data, many people do share their information with close friends and family. A

growing number of identity theft cases indicate that some close friends and family members will pretend to be the customer and steal from that individual. These are very time-consuming cases to research, but they can present a lower risk to the institution if the case is referred back to the customer to handle in a civil (rather than criminal) manner. For example (how friendly fraud occurs):

- A customer calls the financial institution's call center because he can't access his account online. While the call center representative is talking with him, there presentative can see someone is accessing the customer's account on the Internet. When the representative asks if anyone might know his password, the customer explains that he shared it with his daughter; the password is the same as his ATM password, which he had given to her so she could withdraw money. It turns out that the daughter just left home, not on good terms, and took all of her father's money.

» Internal Fraud – This type of fraud is not new, but online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. Another option is to truncate account numbers and customer data and limit employee access to the full numbers. Of the three types of fraud, internal fraud can be the most costly to financial institutions.

In order to mitigate risk associated with online banking, financial institution policies and systemic controls should create an environment in which fraud can be prevented, detected, monitored and benchmarked against industry standards. These policies and controls should:

» Require “reasonable efforts” to be made to ascertain the true identity of individual customers and/or the stated business purpose of each commercial enterprise with which the bank conducts business.

» Have to know your customer (KYC) policy that includes the following for personal account opening:

1.Proper identification of the customer;

2.Validation of the customer's residence or place of business;

3.Consideration of the source of funds used to open an account; and

4.Checking with a service bureau, if applicable, for undesirable customer behavior such as insufficient funds or check kiting.

» Have adequate ongoing monitoring systems in place to identify suspicious transactions, such as structuring, transactions inconsistent with the nature of a customer's stated business purpose, and unusual wire activities. Various operational controls are available to mitigate fraud risk, including:

1.Monitoring transactions coming in and going out of deposit accounts using reports that identify a certain threshold and history of the activity over a specific time frame;
2.Creating reports that monitor large dollar deposits; and
3.Tracking ATM activity based on dollar thresholds over a certain time frame.

Combining technology and sound banking practices can help maintain the security and integrity of financial transactions. When enrolling online banking customers or opening accounts via the Internet, operational controls and software can be used together to mitigate risk. Because most online transactions occur in real time, validation and monitoring should whenever possible be conducted in real time, rather than overnight or through batch processing.

Financial institutions should establish policies and train call center represen-tatives to recognize customer imperson-ation or "pretext" calls. When these types of calls are identified, the representative should deny the caller access to information and report the incident. In establishing policies related to caller identification, financial institutions should consider the impact of denying access to legitimate customers, as well as of granting access to someone imperso-nating a customer. Each institution must determine how much risk it is willing to accept and establish policies accordingly.

Responsible for Fraud Detection

While senior management and the board are ultimately responsible for a fraud management program, internal audit can be a key player in helping address fraud. By providing an evaluation on the potential for the occurrence of fraud, internal audit can show an organization how it is prepared for and is managing these fraud risks.

In today's automated world, many business processes depend on the use of technology. This allows for people committing fraud to exploit weaknesses in security, controls or oversight in business applications to perpetrate their crimes. However, the good news is that technology can also be a means of combating fraud. Internal audit needs to view technology as a necessary part of their toolkit that can help prevent and detect fraud. Leveraging technology to implement continuous fraud prevention programs helps safeguard organizations from the risk of fraud and reduce the time it takes to uncover fraudulent activity. This helps both catch it faster and reduce the impact it can have on organizations. The following analytical techniques are effective in detecting fraud:

» Calculation of statistical parameters (e.g., averages, standard deviations, high/low values) – to identify outliers that could indicate fraud.

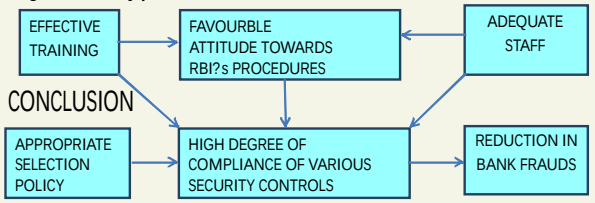
» Classification – to find patterns amongst data elements.

» Stratification of numbers – to identify unusual (i.e., excessively high or low) entries.

» Digital analysis using Benford's Law – to identify unexpected occurrences of digits in naturally occurring data sets.
» Joining different diverse sources – to identify matching values (such as names, addresses, and account numbers) where they shouldn't exist.
» Duplicate testing – to identify duplicate transactions such as payments, claims, or expense report items.
» Gap testing – to identify missing values in sequential data where there should be none.
» Summing of numeric values – to identify control totals that may have been falsified.
» Validating entry dates – to identify suspicious or inappropriate times for postings or data entry.

This shows a proper system is not developed to abreast the bank employees of various frauds that perpetrate in banks every now and then, or the reason could be that the circulars that are circulated among various banks by either their respective head office or the RBI, containing information about the modus operandi of frauds committed remain at the desk of manager. The manager neither communicate the information to his staff members, nor does he himself give due attention to it. The result of hypothesis testing revealed that there was a significant difference in the awareness level among the three categories of employees at three different hierarchal levels. It can be attributed to the fact that managers get more opportunity to read news / circulars circulated from the head office and RBI to them, since circulars go directly to them first. There was a significant difference among the awareness level of employees of various banks. This may be due to the reason that organization culture; training status and communication process differ for different banks.

Figure 1: Hypothesized Bank Fraud Reduction Model



The bank employees do not give due importance to the problem of frauds. The awareness level of bank employees regarding bank frauds is not very satisfactory, and majority of them do not dispose favorable attitude towards RBI procedures as they find difficulty in following them due to workload and pressure of competition. Moreover employees are not well trained to prevent bank frauds. Training positively affects the compliance level of employees and improves the attitude towards RBI's procedure.

Managerial Implications

In order to solve the problem of frauds it becomes imperative to train staff in prevention of bank frauds. It is also important to provide adequate staff so that guidelines and instructions lay down by the RBI can be

followed strictly. The communication process between the manager and staff should be improved so that proper information about frauds is disseminated. The attitude towards RBI procedures should be improved through proper communication. The bank employee should be educated as to why a particular procedure is followed and what can be the implication if it is not adhered to strictly. A policy of compulsory leave in a month should be introduced so as to unveil the unscrupulous deeds performed by corrupt officer in charge. The personal life style of the employee should also be checked from time to time in order to see any discrepancy between his income and expenses. Signature is always vulnerable to forgery and thumb impression should be introduced along with signature.

In relation to banking industry, there is need for greater sharing of information between financial institutions on trends and practices of fraudster and fraud topologies, especially those frauds that are committed in computerized environ-ment.

Shubham Saxena is B Tech and a student of ADBT 8th Batch of PNBIIT

"Whoever saves one life saves the world entire."

It's a True story of one of the student of ABDT 8th batch studying at PNBIIT Lucknow. On 15th May she was heading towards her Institute to attend class. Near Munshipulia Chauraha she saw an accident, where an old man was lying on the road bleeding profusely. Many people were staring at him but no one was helping him out. She was in the tempo and was already late for the class, but seeing the condition of the old man, she couldn't resist herself. She stopped the tempo, went to the old man and tried to carry him to the hospital. At that time two boys also came to help her in picking him. Finally they took him to nursing home nearby. But doctor asked her to stay back for police investigations. She had to rush for class so she requested for allowing her to go. But they then asked her to give some original id proof. She had driving license. They insisted her to deposit original driving license with them for treating the old person. She had no other option but to deposit her license and to go for the class. Because of quick and brave response of her, the old person was saved and is happily living. Her brave act is an example for the society.

LATEST BANKING TECHNOLOGY AND IT NEWS

PNB Rupay platinum card
Punjab National bank launched PNB Rupay Platinum card for the convenience of High Net worth individuals on National Payment Corporation of India (NPCI) platform. It has following features:
1. Per day cash withdrwal limit of Rs 50000/ from ATM
2. Merchant shopping up to Rs 125000through POS or E Commerce
3. Register online for retail internet facility / mobile banking facility

Source : PNB Knowledge Centre

National Payments Corporation of India (NPCI) and JCB International Co. Ltd, a subsidiary of Japan's JCB Co. Ltd., are entering into a partnership for payment cards issuance and acceptance.
Under the pact, JCB cards will be accepted at all NPCI locations in India. The partnership will also include the issuance of RuPay/JCB international cards by NPCI member banks that will be globally accepted through the JCB network,

Source : Business Today June 29, 2015

Novopay, a Bengaluru-based company whose banking solution is linked to the online biometric authentication of the Aadhaar programme at its backend, pushes the financial inclusion or the Jan Dhan Yojna agenda further. In the coming years, 30,000 points of service will be available all over India. After teaming up with Bank of India, Novopay, incubated by Khosla Labs, is concentrating on semi-urban and rural market by transforming kirana stores into bank branches which can open bank accounts and log transfers of money with their device. Novopay is opening accounts for migrant workers and of those who have no access to banking facilities to send money back home every month. Mumbai-based prepaid payment solution provider ItzCash has issued more than 80 million prepaid accounts of which nearly 40 per cent is in the semi-urban and rural areas. Amongst the 292 unbanked regions classified by the Reserve Bank of India, ItzCash is present in 255.

Source : economic times January1 2015

Private sector lender Axis Bank on Wednesday launched a new debit card, which can be switched off for specified time periods, and has also put in fraud protection cover personal accidental. The card named 'Secure+' can be switched off by using a mobile phone application or Internet banking gateway or through the phone banking application

Source : Business today June 15,2015

Researchers develop mobile Tech to make blind user see: Researchers at the University of Lincoln are looking to create an effective visual aid system, leveraging the spatially-aware capabilities of devices like Project Tango which have started to appear in the market. These devices have a multitude of cameras and sensors, enabling them to get a 3-dimensional view of their surroundings. The Lincoln Centre of Autonomous Systems previously made progress in the field of indoor mapping and object recognition, and these findings have been helpful in the creation of this new visual-aid system. The researchers have developed an interface that recognizes the objects around it, and relays this information to the user with the help of vibration, sound or a spoken hint, depending on the user and the object. Basically, the interface learns over time and understands how the user responds to certain actions, enabling it to better convey information to the user. The key difference between this interface and similar visual aid devices is that it dynamically adapts to the user and the object, enabling recognition to be faster and better.

Source : http://www.digit.in/mobile-phones/researchers-develop-mobile-tech-to-help-blind-users-see-26461.html

A parliamentary panel has recommended making at least 15 per cent Public Sector Banks (PSBs) branches all-women offices to provide safe and convenient work environment to women in the banking sector.

It has also recommended flexible working hours for women employees to help them balance their professional and family responsibilities. In a report on 'Working Conditions of Women in Public Sector Banks', the panel said that PSBs should be instructed by the Finance Ministry to open at least 15 per cent of their branches as all-women units, especially in those parts of the country where discrimination against women has traditionally been on the higher side than the rest of the country.

Source : http://www.businesstoday.in/money/banking/par-panel-asks-finmin-to-make-15percent-of-psb-branches-all-women-offices/story/222570.html

2,590 post offices have core banking services As the Reserve Bank of India is expected to give Department of Posts (DoP) payment bank licence by September, there are 2,590 post offices in the country with core banking facilities. Profile of post office shall change as facility will be offered to poorer section of the population.

source : http://www.moneycontrol.com/news/current-affairs/2590-post-offices-have-core-banking-services-ravi prasad 1927821.html?utm_ source=ref_article

BSNL launches mobile wallet with cash withdrawal option

State-run operator BSNL on Friday launched a pre-paid card linked mobile wallet service which would allow its customers to transfer money, pay for services as well as withdraw cash of up to Rs 1 lakh. The wallet service, Speed Pay, allows a customer to load money even if he does not have a bank account.

Source: http://www.moneycontrol.com/ news/business/bsnl-launches-mobile-walletcash-withdrawal-option_1785761.html?utm_ source=ref_article

Digitally Speaking: The bank is where the customer is

Putting a model sailing ship in a bottle seems a bewildering kind of art. Writing an entire book on a grain of rice is another difficult art form. But how about keeping a copy of one's bank, complete with all of its applications and services, in one's ultraportable mobile phone? So one can bank comfortably out of one's palm – anytime, anywhere, and in a safer way. Cloud, mobile and virtualization technologies, as well as high-performance nano chips, are turning not only one's mobile, but every possible screen close to him – tablet, touch-banking screen, etc. – into one's bank. Distance is no longer a limiting factor and the banking activity can be carried out almost anywhere in the world. The “bank is where the customer is” phenomenon is driven, in particular, by an increase in the number of users in the 35-45 age group.

Source: http://www.moneycontrol.com/news/advertising/digitally-speaking-the-bank-is-wherecustomer-is_1270774.html?utm_ source=ref_article

Smarter retail banking/ smarter money

The banking industry has to fundamentally reorient their business models, by moving from product-centric silos to customer-centric strategies.

Financial organizations around the world are looking ahead. New challenges and new obstacles loom large, but as the global economy evolves, many new opportunities present themselves.

But first, the challenges. They include a host of new regulations aimed at reducing risks in the system; increasing capital reserves; growing revenue in recession-wrecked economies of mature markets; competing and partnering with non-traditional players; rebuilding trust across the global financial system; and, finally, competing to attract and retain increasingly demanding customers. Just to name a few.

With that in mind, the opportunities are there for those who want to change the conversation from one about problems to one about possibilities. The global economy is expected to show a growth rate of 5.8% compounded over the next 15 years. Global assets are expected to quadruple within the same time frame to $1,264 trillion1 and 2.5 billion unbanked or under-banked people worldwide constitute a large untapped customer pool.

Much of that movement will happen in emerging markets. A recent survey by the IBM Institute for Business Value (US) shows tomorrow's banks must become more client centric by leveraging sophisticated insights to improve risk management, pricing, channel performance and client satisfaction.

Source : http://www.ibm.com/smarterplanet/in/en/banking_technology/ideas/

CI Bank to Focus on Leveraging Technology

ICICI has a strong presence in social media through banking on Facebook, which is further strengthened by becoming the first bank in Asia to introduce payment services on Twitter.

Source : http://profit.ndtv.com/news/banking-finance/article-icici-bank-to-focus-on-leveraging-technology-chanda-kochhar-769554

Mobile banking users to double in four years: Study

The number of mobile banking users globally is likely to double (1.8 billion) in the next four years with adoption rate reaching to about 60-70 percent in India and China, a study has suggested. The report "Global mobile banking report done by KPMG , a global consultancy firm, also suggests that mobile banking and payment systems are increasingly being integrated with other technologies, driving an era of "open banking"

Source : http://www.bgr.in/news/mobile-banking-users-to-double-in-four-years-study/

A beautiful speech by Sundar Pichai - an IIT-MIT Alumnus and Global Head Google Chrome:

The cockroach theory for self development. At a restaurant, a cockroach suddenly flew from somewhere and sat on a lady. She started screaming out of fear. With a panic stricken face and trembling voice, she started jumping, with both her hands desperately trying to get rid of the cockroach. Her reaction was contagious, as everyone in her group also got panicky. The lady finally managed to push the cockroach away but ...it landed on another lady in the group. Now, it was the turn of the other lady in the group to continue the drama. The waiter rushed forward to their rescue. In the relay of throwing, the cockroach next fell upon the waiter. The waiter stood firm, composed himself and observed the behavior of the cockroach on his shirt. When he was confident enough, he grabbed it with his fingers and threw it out of the restaurant. Sipping my coffee and watching the amusement, the antenna of my mind picked up a few thoughts and started wondering, was the cockroach responsible for their histrionic behavior? If so, then why was the waiter not disturbed? He handled it near to perfection, without any chaos. It is not the cockroach, but the inability of those people to handle the disturbance caused by the cockroach, that disturbed the ladies. I realized that, it is not the shouting of my father or my boss or my wife that disturbs me, but it's my inability to handle the disturbances caused by their shouting that disturbs me. It's not the traffic jams on the road that disturbs me, but my inability to handle the disturbance caused by the traffic jam that disturbs me. More than the problem, it's my reaction to the problem that creates chaos in my life.

Lessons learnt from the story:

I understood, I should not react in life. I should always respond. The women reacted, whereas the waiter responded. Reactions are always instinctive whereas responses are always well thought of. A beautiful way to understand.....LIFE. Person who is HAPPY is not because Everything is RIGHT in his Life. He is HAPPY because his Attitude towards Everything in his Life is Right..!!,,,,,,,

SAILING SAFE IN CYBERSPACE
Protect Your Identity and Data

Author: Anjali Kaushik
Length: 292 pages
Publisher: SAGE Publications India Pvt Ltd Price:
ISBN-13:9788132111221

Sailing Safe in Cyberspace by Anjali Kaushik is an excellent resource on safe computing. It provides a comprehensive guide to the reader about how security of information might be compromised, how cybercrime markets work and measures that can be taken to ensure safety at individual and organizational levels. This book combines insights on cybersecurity from academic research, media reports, vendor reports, practical consultation and research experience.

This book is organised in four main sections. The first section of the book discusses motivation and types of cybercrimes that can take place with. The author cites variables like social, economical, biological and criminal justice system as being instrumental in promoting cybercrime. In the second sections the author discusses the major types of threats that users might encounter like spam, malware, phishing, in cloud computing, SQL injection etc, techniques in details and their trends. The third discusses the financial, non-financial and economic impact and trend of cybercrime and role of the government in combating it. The fourth section of the book tells the readers about ways to protect themselves and secure their data/information stored in computers and the cyberspace. It concludes by offering suggestions for building a secure cyber environment.

In this book Sailing Safe in Cyberspace the author discusses very important relevant issues related to operations in cyber space for individuals, organisations and nations and acknowledges the advantages the convergence of technology has brought about for users. The book includes in-depth analysis more than 50 global cybercrime incidents and their impact. Author says that a fundamental lack of awareness of protecting oneself has been said to be the cause of people becoming victims of cybercrime. The book is excellent resource giving in-depth exposure to various ways in which the security of the computers can be compromised, how cybercrime markets works and what is to be done to ensure their safety for sailing safe for individual computer users and practical suggestions for organization users. A definite good read for people who do not wish to be bogged by technical jargon and who wish to protect themselves against cybercrime.

Compiled by Sanjay Srivastva,
Librarian at PNBIIT Lucknow

Desirable qualification for IT officers in Banks & Financial Institutions

COURSES AT OUR CENTRE

Be a Techno banker

1. ADVANCED DIPLOMA IN BANKING TECHNOLOGY
2. CERTIFICATE COURSE IN BANKING TECHNOLOGY (CCBT)

OBJECTIVE : To create a well equipped pool of techno-bankers aspiring for jobs in Banking, I.T. & Financial Sectors.

PLACEMENT RECORD : (ADBT)

- ✓ Excellent track record of campus placement.
- ✓ Past recruitment include NPCI, ICICI Bank, HDFC Bank, PNB, Vijaya Bank, UBI, Dena Bank & HP, FSS etc. (Disclaimer: Institute does not guarantee placement)

GENERAL INSTRUCTIONS : For placement information, application form and prospectus visit institute's website: www.pnbiit.ac.in

पंजाब नैशनल बैंक
सूचना प्रौद्योगिकी संस्थान
विभूति खण्ड, गोमतीनगर, लखनऊ- 226010 (यू0पी)
फोन : 0522-2721172-73, फैक्स : 0522-2721439

punjab national bank
institute of information technology
Vibhuti Khand, Gomti Nagar, Lucknow - 226010 (U.P.)
Ph. : 0522-2721172-73, Fax : 0522-2721439

Contact : Mr. A.K. WAHI # 0522-4066760/Mr. Pramod Dixit # 09335925126, Mrs. Pratima Trivedi # 09450101334

PNBIIT, Established in 2002, is an independent society promoted by Punjab National Bank to promote training & education in BFI sector with focus on IT.