ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Cybercrime is a Global Problem: Increasingly Social and Mobile

Abdulla Shaik[1], Sajida Banu Shaik[2]

Assistant Professor, Department of CE, Nuva College of Engineering & Technology,Nagpur. Maharashtra, India[1]

Assistant Professor, Department of MCA, Nuva College of Engineering & Technology,Nagpur. Maharashtra, India[2]

Abstract : With so much of our everyday communication and commercial activity now taking place via the Internet, the threat from cybercrime is increasing, targeting citizens, businesses and governments at a rapidly growing rate. The EU in particular is a key target because of its advanced Internet infrastructure and increasingly Internet-based economies and payment systems. The scale of cybercriminal activity represents a considerable challenge to law enforcement agencies and the total cost of cybercrime to society is significant.

Everyone agrees cybercrime affects everyone—governments, corporations, the public—but to what extent? And while vast sums are spent on security to protect against the evildoers, why is it so difficult to determine the amount of the damage they have done?

A recent report suggests that victims lose around €290 billion each year worldwide as a result of cybercrime, making it more profitable than the global trade in marijuana, cocaine and heroin combined. "It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion," After surveying more than 13,000 consumers in 24 countries, the researchers found that the numbers of online adults increased by 20 percent from last year, and that cybercrime impacted just under ½ of them in the previous 12 months. The total direct consumer cost was calculated to be $110 billion, slightly down from last year's $114 billion (USD), with the average cost per victim down approximately 20 percent. The reason the overall cost remains so high is that the pool of victimized online adults grew more rapidly - in other words, less money, but from more victims. In this paper we are going to give idea about how this can be possible and what we should do.

Key words: Cyber Crime, Email, Exe joiner, IP Camera, Phishing, Root kit, SIM Card, Sniffers, SMS Spy, Spoofing, Zombies

I. INTRODUCTION

Many organizations that have been cybercrime victims do not want to report the problem because they perceive it as bad for business. Organizations that have not detected losses may be more likely to respond to cybercrime surveys than those that have. Or those that have had very public large losses may be more prone to reply than those with moderate unreported losses. Sometimes downtime is figured into the mix. Sometimes the cost of buying new equipment or upgrades or security services or outside consultants is included in the total. There is no agreement on what and what not to include. Often organizations are not even aware they have had losses or the full magnitude of the crime is not known. "Many organizations simply don't want to report to the government that they have had losses because they don't trust how that information will be used."

Many cybercrimes are committed by a small number of people. For example, in 2010, a third of all the spam in the world was sent. So it would be a lot more efficient to just arrest the bad guys and put them in jail than to expect several hundred million users worldwide to run anti-virus and anti-spam software. Of course the anti-virus and anti-spam companies don't agree." A large part of the true cost of cybercrime is the money the world spends on anti-virus software, he maintains, adding "in fact, the anti-virus companies make much more money out of spam than the bad guys do. Let see how it happen in our real life how someone can hack our information.

II. CYBER CRIME ISSUES

A. Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

B. Child Pornography

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India. It explosion has made the children a viable victim to the cyber crime. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles.

The easy way to access the pornographic content readily and freely available over the internet lowers the inhibitions of the children. Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age, and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

In physical world, parents know the face of dangers and they know how to avoid & face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways. But in case of cyber world, most of the parents do not themselves know about the basics in internet and dangers posed by various services offered over the internet. Hence the children are left unprotected in the cyber world. Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is wrong and what is right for them while browsing the internet

C. How do they operate?

a. Pedophiles use false identity to trap the children/teenagers
b. Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
c. Befriend the child/teen.
d. Extract personal information from the child/teen by winning his confidence.
e. Gets the e-mail address of the child/teen and starts making contacts on the victimâ€™s e-mail address as well.
f. Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
g. Extract personal information from child/teen
h. At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

D. Phishing

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. The Web site, however, is bogus and set up only to steal the users information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately. Phishing, also referred to as brand spoofing or carding, is a variation on phishing, the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

E. Denial of service Attack

This is an act by the criminal, who floods the bandwidth of the victims network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

F. Virus Dissemination

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. A new virus threat through a E-mail attachment called ‘cabnote’ which could damage and destroy the hard disk and other computer data as well. The word ‘cabnote’s a disguise and it has nothing to do with Union or state cabinet notes or notings. You can advise your subordinates accordingly.

G. 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.

H. IRC Crime

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other.

I. Credit Card Fraud

The unauthorized and illegal use of a credit card to purchase property.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

J. Net Extortion

Copying the companyâ€™s confidential data in order to extort said company for huge amount

III. SOCIAL AND MOBILE ISSUES

3.1 SIM CARD

First off a little introduction about SIM CARD Our sim cards contain two secret codes or keys called (imsi value and ki value) which enables the operator to know the mobile number and authenticate the customer, these codes are related to our mobile numbers which the operators store in their vast data base, it is based on these secret keys that enables the billing to be made to that customer. Now what we do in sim cloning is extract these two secret codes from the sim and programme it into a new blank smart card often known as wafer, since the operator authentication on sims is based on these values, it enables us to fool the operators in thinking that it's the original sim,this authentication is a big flaw concerning GSM technology.

Now which sim cards can be cloned Sim cards are manufactured on the basis of 3 algorithms COMP128v1,COMP128v2 and COMP128v3 now an important note currently only COMP128v1 version sim cards can be cloned ,since this is the only algorithm which has been cracked by users, bear in mind that 70% of all the sim cards we use are COMP128v1 .

A. How to Clone a SIM Card?

1. First you'll need the IMSI (International Mobile Subscriber Identifier) number. This string of numbers is usually imprinted on the SIM card itself. This is an example of an IMSI number:

IMSI:329011334667899

An IMSI is usually 15 digits long, but can be one or two digits shorter.

2. Now you have your IMSI number you'll need the authentication key (Ki), which is unique to your SIM. This number can only be discovered electronically using a SIM duplicator, which is an external device that you will slot the SIM card into. A SIM duplicator is relatively inexpensive - they can be found at around the $10 mark - and can be purchased at multiple locations. A Google search for 'Super SIM' will turn up at least several online outlets.

3. When the SIM duplicator is connected to your PC and your SIM card, it will attempt to acquire the Ki number and copy the entire contents. When a new SIM card is placed into the duplicator after this process is complete, that data will be copied and, for all intents and purposes, the new SIM will be identical to the old.

During November 2008, the Indian police by a strange co-incidence stumbled upon the technology of SIM card cloning while investigating the Assam blasts. Since the SIM cloning is an illegal activity, the police in their defence said that they had no expertise in the area and SIM card cloning was a "technological surprise".

However, in other parts of the world, SIM cloning has been a major part of research since GSM mobiles claimed the markets. Phone cloning is, basically, a transfer of identity between two mobile phones. It involves placing a chip in the target mobile and allowing the electronic serial number (ESN) to be altered. ESN is the information used by the telecom operators to find if a person is the legitimate user of a particular SIM card. Mobile Identification Number (MIN) alteration together with changing ESN makes it easier to make fraudulent mobile calls as the information can be utilised to make the target mobile, a clone of the legitimate mobile. Cracking a telecom company or even eaves dropping in a cellular network can be used to obtain the ESN or MIN. All one needs to carry out the operation is a SIM card reader, a blank silver wafer card or smartcard, software to extract authentication keys etc, Wafer card programmers and some software to write PIC and EEPROM files to the blank card.

So the next time you feel that your mobile bills are a tad high, relax. If the trend does not continue, it is probably just you!

3.2. Caller ID spoofing

Caller ID spoofing is the practice of causing the telephone network to display a number on the recipient's Caller ID display that is not that of the actual originating station. The term is commonly used to describe situations in which the motivation is considered malicious by the speaker or writer. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, Caller ID spoofing can make a call appear to have come from any phone number the caller wishes. Because of the high trust people tend to have in the Caller ID system; spoofing can call the system's value into question. Many people have claimed that, after answering a spoofed call, the charge for the call is larger than it would be for a legitimate call.

Caller ID is spoofed through a variety of methods and different technology. The most popular ways of spoofing Caller ID are through the use of VoIP or PRI lines.

According to a report from the India Department of Telecommunications, the Government of India has taken following steps against the CLI spoofing Service Providers:

• Websites offering caller-ID spoofing services are blocked in India as an immediate measure.

• ILDOs, NLDOs and Access Service Providers have been alerted to the existence of such spoofing services, and shall collectively be prepared to take action to investigate cases of caller-ID spoofing as they are reported.

In the U.K., the spoofed number is called the "presentation

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

number". This must be either allocated to the caller, or if allocated to a third party, it is only to be used with the third party's explicit permission.

B. Valid reasons to spoof caller ID

There are reasons for modifying the caller ID sent with a call which are motivated by legitimate concerns. Differing opinions do exist on whether these reasons justify allowing modifications to the caller ID sent.

1. A company with a toll-free telephone number may prefer the caller ID to display this number.
2. A call center making calls on behalf of many clients may prefer the caller ID to display a different number for each client's calls.
3. Commercial answering-service bureaus which forward calls back out to a subscriber's cell phone, when both parties would prefer the caller ID to display the original caller's information.
4. Most calling-card companies display the caller ID of the calling-card user to the called party.
5. Business owners have been known to use caller ID spoofing to display their business number on the caller ID display when calling from outside the office (for example, on a mobile phone).
6. Google Voice displays its users' Google Voice number when they place calls through the service using their landline or cell phone.
7. Gizmo5 (now defunct) sent the user's Gizmo5 SIP number as outbound caller ID on all calls. Because Gizmo5 IDs were in the format 747NXXXXXX, it was possible to confuse calls made from Gizmo5 with calls made from area code 747.

3.3. SMS spoofing

SMS spoofing is a relatively new technology which uses the short message service (SMS), available on most mobile phones and personal digital assistants, to set who the message appears to come from by replacing the originating mobile number (Sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company, product).

Examples of SMS spoofing

- Messages sent from Google are sent with the Sender ID "Google".
- Messages sent from Facebook are sent with the Sender ID "FACEBOOK".
- Skype sends messages from its users with the mobile number they registered with. Note that when a user attempts to "reply" to the SMS, the local system may or may not allow the replying message to be sent through to the spoofed "origin."

The legality of SMS spoofing has been brought to our attention numerous times. We have heard that a lot of countries across Europe and Asia have actually passed laws making it illegal to spoof text messages. Unfortunately, we're not sure of the details and specifically which countries have made this illegal, but we're doing research and hope to have more info soon. We are confident that text message spoofing is NOT illegal under any existing laws in the United States.

Sites That Offer Text Message Spoofing

Here are some sites that have, or currently do, offer SMS spoofing services:

SMS Spoofing - http://www.smsspoofing.com
SpoofCard (New for 2011) - http://www.spoofcard.com
SpoofTexting - http://www.spooftexting.com
Fake My Text - http://www.fakemytext.com
The SMS Zone - http://www.thesmszone.com

Protecting users from SMS spoofing

If a user can prove that their SMS sessions have been spoofed, they should contact both law enforcement and their cellular provider, who should be able to track where the SMS messages were actually sent from. A user may also modify the phone's settings so that only messages from authorized numbers are allowed. This is not always effective since hackers could be impersonating the user's friends as well.

SMS Interceptor is a fun application that allows you to read messages from any cell phone! Just enter the phone number you are interested in and press Catch SMS. For all your spying needs. This is subscription service priced $9.99 per month 6 credits equaled 6 calculations. You must be the account holder or have permission from the account holder. This is an auto renewing subscription service that will continue until cancelled anytime by texting STOP to short code 91970. Available to users over 18 for $9.99 per month charged on your wireless account or deducted from your prepaid balance for 6 alerts per month on Sprint, Alltel, AT&T, Boost, T-Mobile, Virgin Mobile USA, U.S. Cellular and Cellular One. For support: text HELP to 91970.

SMS Message Reader if any one want to read someones SMS message the SMS Message Reader is a fun application that allows you to read messages from any cell phone! Just enter the phone number you are interested in and press Catch SMS. For all your spying needs. Like hackers can use different techniques to grab your data and personal information.

3.4. E-mail spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

retaliation. However, spoofing anyone other than yourself is illegal in some jurisdictions. Many of internet hackers send this type of mail which is redirect to home page and when user enter the login and password which is hack by the hacker. Your email account may use for illegal purpose. So be careful before entering your username and password.

3.5. Internet protocol camera

An Internet protocol camera, or IP camera, is a type of digital video camera commonly employed for surveillance, and which unlike analog closed circuit television (CCTV) cameras can send and receive data via a computer network and the Internet. Although most cameras that do this are webcams, the term "IP camera" or "netcam" is usually applied only to those used for surveillance. This type of devises can fix any and record your data.

3.6. Example: Salami attack

A salami attack is when small attacks add up to one major attack that can go undetected due to the nature of this type of cyber crime. It also known as salami slicing. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well .The attacker uses an online database to seize the information of customers that is bank/credit card details deducting very little amounts from every account over a period of time. The customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

Salami Attack Incidents: In January 1993, four executives of a rental-car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. In Los Angeles, in October 1998, district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. In 2008, a man was arrested for fraudulently creating 58,000 accounts which he used to collect money through verification deposits from online brokerage firms a few cents at a time. While opening the accounts and retaining the funds may not have been illegal by themselves, the authorities charged that the individual opened the accounts using false names (including those of cartoon characters), addresses, and social security numbers, thus violating the laws against mail fraud, wire fraud, and bank fraud.

Identifying the salami attack

The only way to detect salami attack according to me is to perform rigorous white box testing by checking each and every line of code which is exhaustive but that's the only way.

a) The corporate has to update the security of the system as high as possible so that if the attacker is taking advantage of any loophole than that bug is patched and attack is avoided.

b) Also those banks should advise customers on reporting any kind of money deduction that they aren't aware that they were a part of. Whether a small or big amount, banks should encourage customers to come forward and openly tell them that this could mean that an act of fraud could very well be the scenario.

c) Most Important according to me is that Customers should ideally not store information online when it comes to bank details, but of course they can't help the fact that banks rely on a network that has all customers hooked onto a common platform of transactions that require a database. The safe thing to do is to make sure the bank/website is highly trusted and hasn't been a part of a slanderous past that involved fraud in any way.

This attack is not only on the banks but also on any entity where slicing can be performed and people are made unaware of the crime.

3.7. EXE Joiner

EXE Joiner is a small program that allows you to easily join (bind) two or more files (no matter their type) into one single executable. That executable (the one into which the files are included) is a simple compiled program that, when opened, will automatically launch the included files one by one.

EXE Joiner features:

• Can join any file type that is needed by the executable for a properly run
• Unlimited files can be joined
• Option to encrypt the joined files
• Option to change the icon of the joined file (either with one of the icons included in EXE Joiner or another one of your choice)
• Option to drag and drop the files into EXE Joiner
• EXE Joiner is compatible with Windows 2k, XP, Vista, Windows 7 and Windows 8 (32-bit and 64-bit systems) and it doesn't need .Net Framework or other dependencies
• The joiner "stub" is undetectable when scanned with major antivirus products (Norton, Kaspersky, McAfee, Panda, AVG, Avast, TrendMicro)

EXE Joiner purposes:

• To distribute your program as a single executable
• To hide files
• To open/run more files from the same program/executable

3.8. Rootkit

A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

malware.
Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system (i.e. exploiting a known vulnerability, password (either by cracking, privilege escalation, or social engineering). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root/Administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.
Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.

3.9. Key logging or Keyboard Capturing
Keystroke logging, often referred to as keylogging or Keyboard Capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It also has very legitimate uses in studies of human-computer interaction. There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis.

Software-based keyloggers these are computer programs designed to work on the target computer's operating system.From a technical perspective there are five categories: Packet analyzers, Hypervisor-based, Kernel-based, API-based /Form grabbing based, Memory injection based keyloggers.

Let consider Sniffer as example may refer as packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

Analyze network problems
• Detect network intrusion attempts
• Detect network misuse by internal and external users
• Documenting regulatory compliance through logging all perimeter and endpoint traffic
• Gain information for effecting a network intrusion
• Isolate exploited systems
• Monitor WAN bandwidth utilization, Monitor network usage and Monitor data-in-motion
• Monitor WAN and endpoint security status
• Gather and report network statistics
• Filter suspect content from network traffic
• Serve as primary data source for day-to-day network monitoring and management
• Spy on other network users and collect sensitive information such as login details or users cookies
• Reverse engineer proprietary protocols used over the network
• Debug client/server communications
• Debug network protocol implementations
• Verify adds, moves and changes

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system. Firmware-based, Keyboard hardware, Wireless keyboard sniffers, Keyboard overlays Acoustic keyloggers, Electromagnetic emissions, Optical surveillance, Physical evidence

3.10. Buffer overflow
In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety.

zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

Skimming is a method of rapidly moving the eyes over text with the purpose of getting only the main ideas and a general overview of the content.
A. Skimming is useful in three different situations.
• Pre-reading--Skimming is more thorough than simple previewing and can give a more accurate picture of text to be read later.
• Reviewing--Skimming is useful for reviewing text already read.
• Reading--Skimming is most often used for quickly reading material that, for any number of reasons, does not need more detailed attention.

IV. PREVENTING CYBER CRIMES

4.1. Preventing credit/debit card fraud
By taking certain precautions, a user can prevent their credit or debit card from being misused both online and offline.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

1. Do not provide photocopies of both the sides of the credit card to anyone. The card verification value (CVV) which is required for online transactions is printed on the reverse of the card. Anyone can use the card for online purchases if the information is available with them.

2. Do not click on links in email seeking details of your account; they could be phishing emails from fraudsters. Most reputed companies will ask you to visit their website directly.

3. While using a credit card for making payments online, check if the website is secure The CVV will also be required.

4. Do not give any information to persons seeking credit card information over phone

5. Notify your bank / credit card issuer if you do not receive the monthly credit card statement on time. If a credit card is misplaced or lost, get it cancelled immediately.

4.2. Online Safety Tips

We all know that the Internet is a cool place to hang with friends and check out new things. But don't forget about the Internet's risks and dangers. If you're going to use the Web, do it safely! Here are some suggestions on what you should and shouldn't be doing online to help protect you against the bad stuff.

Never reveal personally – identifiable information online. A lot of creeps use the Internet to take advantage of other people, especially kids and teens. Never reveal any personally-identifiable information online, whether it's on your profile page or in a blog, chatroom, instant messenger chat or email.

• Always use a screen name instead of your real name.
• Never give out your address, telephone number, hangout spots or links to other websites or pages where this information is available.
• Be careful about sending pictures to people you do not know very well.
• Never tell people personal or private information about your friends or family.
• Never assume you're completely anonymous online. Even if you don't put personal information online, there are different ways that people can still figure out who you are and where you live.

Never share your password with other people (except for your parents). Your passwords to websites, email accounts and instant messenger services should not be shared with friends or strangers. Your friends may not be as safe as you are and may unknowingly subject you to danger. You should, however, share your passwords with your parents if they ask so they can make sure you're using the Internet safely.

Never arrange meetings with strangers.

Just because you've seen a person's picture and read his or her profile, does not mean you know them. Many people online lie about who they are and what their intentions are. Just because someone seems nice online, does not mean they really are. They could be trying to hurt you. Never arrange a meeting with a stranger you've met online. Even meeting a stranger in a crowded place could be dangerous as he could follow you home. If you wish to meet an online friend in person, talk to your parents and arrange a time and place where your friend can meet your parents first, just in case. If you are worried about your parents meeting one of your online friends, you probably shouldn't be friends with them in the first place.

Don't believe everything you read or see online.

Be wary of everything you see online unless it is from a trusted source. People lie about their age, who they are, what they look like, where they live, how they know you and what their interests are. Also, a lot of websites and emails contain information that is misleading or just plain untrue. If a person or deal sounds too good to be true, it probably is. Ask your parents to help you figure out what information is really true.

Don't download files or software without your parents' permission.

There are a lot of files on the Internet that are unsafe to download to a computer. Some files will bombard you with pop-up ads all day long. Some files will actually track everything you and your family does on your computer, including your logins, passwords and credit card information, which criminals then use to steal money from you and do other harm. There is no easy way to tell which files are bad and which are ok to download. That free desktop wallpaper you want to download might also steal your parents' credit card information. Ask your parents before you download any files or software from the Internet.

Don't respond to inappropriate messages or emails.

Some people send inappropriate messages just to see if you will respond. If you do, you are simply encouraging them to send more inappropriate material to you. Don't respond to inappropriate messages. Instead, talk to your parents about how to report them to the right place.

Don't post inappropriate content.

If you post information about tennis, you will attract people who are interested in tennis. If you post inappropriate content or pictures, you will attract people who have inappropriate interests. If you post jokes, photos or other content that contain sexual references you will probably attract people who are only interested in talking about sex. Be mindful of what you are communicating to the rest of the online world through the content you put onto the Internet.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Be leery of personal questions from strangers.
People you don't know who ask personal questions are often up to no good. Don't continue communicating with strangers who ask you personal questions. Talk to your parents about how to block them from communicating with you and report them to the right place.

Don't be bullied into fights.
People tend to say things online that they would never say in person. Some people even say rude and malicious things, sometimes just to see if you will respond. Don't respond to these people. Instead, talk to your parents about how to block them from communicating with you and report them to the right place.

Don't use adult sites.
There are some websites that kids just should not use. Don't use websites that contain adult content or that facilitate communication with older adults. No matter how much you think you know about the Internet, there are some people and places you just aren't ready to deal with. Enjoy websites that are designed for people your own age.

Understand what you put online will be there forever.
Assume that everything you put online—- every email you write, every picture you post, every blog or journal entry you post—- will be accessible on the Internet forever. Many search engines copy Internet pages and save them for viewing even after the pages are no longer online. Think about that before you post anything online. Do you really want pictures or blog entries to be seen 10 years from now?

Are You A Safe Cyber Surfer?

Fortunately, there are steps you can take to protect your computer, your information and your peace of mind from computer creeps who try to slow down a network operation, or worse yet, steal personal information to commit a crime. Here are some tips to help you, from the Mumbai Police

Make sure your passwords have both letters and numbers, and are at least eight characters long. Avoid common words: some hackers use programs that can try every word in the dictionary. Don't use your personal information, your login name or adjacent keys on the keyboard as passwords-and don't share your passwords online or over the phone.

Protect yourself from viruses by installing anti-virus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically.

Prevent unauthorized access to your computer through firewall software or hardware, especially if you are a high-speed user. A properly configured firewall makes it tougher for hackers to locate your computer. Firewalls are also designed to prevent hackers from getting into your programs and files. Some recently released operating system software and some hardware devices come with a built-in firewall. Some firewalls block outgoing information as well as incoming files. That stops hackers from planting programs called spyware-that cause your computer to send out your personal information without your approval.

Don't open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

When something bad happens-you think you've been hacked or infected by a virus,e-mail a report of the incident to your Internet provider and the hacker's Internet provider, if you can tell what it is, as well as your software vendor.

Take a test before opening e-mail attachment
• Is the email from someone that you know?
• Have you received email from this sender before?
• Were you expecting email with an attachment from this sender?
• Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense?
• Does this email contain a virus? To determine this, you need to install and use an anti-virus program.
Safety Tips

4.3. Wi- Fi Security Tips
• Change Default Administrator Passwords (and Usernames) of the WiFi Router.
• Change Password after regular interval.
• Position the Router or Access Point Safely.
• Turn Off the Network / WiFi routers if it is not in use.

4.4.Online Banking Tips
• Never use unprotected PCs at cyber cafes for internet banking.
• Never keep your pin and cards together.
• Never leave the PC unattended when using internet banking in a public place.
• Register for Mobile SMS , Email Transaction Alerts.
• Never reply to emails asking for your password or pin.
• Visit banks website by typing the URL in the address bar.
• Log off and close your browser when you have finished using internet banking.
• Memorize your PIN. Never carry your PIN.
• Report lost or stolen card immediately.

10 steps that can protect you from loss
• Register for transaction alert s via SMS and E- Mail.
• If you change your mobile number, update with the bank.
• Reduce the limit on your credit card if you use it sparingly.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

• Use virtul cards for online shopping.
• Make use of the virtual keyboard wherever possible.
• Instead of going to the banks website using the link in E-Mail, type the web address directly.
• Memorise 3 digits CVV number at the back of the card and scratch it out.
• Do not leave unwanted photocopies of essential documents at the photocopier.
• If you lose your phone, deactivate all banking services linked to that number.

V. CONCLUSION

This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation.
We can minimize the threat of cyber attack or cyber crime by getting a little aware and conscious while using social media platforms. It is possible to ensure the security of your personal data of those social media platforms with a very minimal effort. Do not share your password with any of your friends or colleagues or even on any online form. It is also suggested avoiding share information about your debit or credit card over these social media networks in order to avoid credit/debit card fraud, as well. The way to overcome these crimes can aware of Cyber Laws, Education and Policy making.

ACKNOWLEDGMENT

I am grateful to thank my Brother Mr. Mohammad Shaik, and my friends Miss. Nisha Rode and Mr. A. Hasheem Babu for giving precious inputs.

REFERENCES

[1.] http://cybercellmumbai.gov.in/
[2.] Internet Crime Complaint Center – www.ic3.gov/preventiontips.aspx
[3.] Norton Cyber Crime Prevention Tips – us.norton.com/prevention-tips/article
[4.] National White Collar Crime Center – www.nw3c.org/services/ic3/complaints
[5.] State of Texas Cyber Security Tips Monthly Newsletter, January 2013, Volume 7, Issue 1
[6.] Cyber-Crimes and their Impacts: A Review, IJERA, Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209 [7.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml,
[8.] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm,
[9.] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/
[10.] Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm
[11.] The Impact And Effects Of Cybercrime On The Society. December 12, 2011
[12.] http://socialmediatoday.com/freelancewriter/995206/impact-cyber-crime-and-security-social-media
[13.] http://www.hanyang.ac.kr/home_news/H5EAFA/0002/101/2012/29-3.pdf

BIOGRAPHIES

Abdulla Shaik working as Assistant professor in Department of MCA, Nuva College of Engineering and Technology. He worked as a lecturer in Joginapally B R Engineering College, Hyderabad. He completed his MCA in 2008, M.Tech(CSE) in 2010 from Acharya Nagarjuna university, Guntur with distinction. Till now he has published SIX international research papers. His area of interest is Operating Systems, Data Structures and the Software Testing Methodologies.

Mrs Sajida Banu Shaik working as Assistant professor in Department of MCA, Nuva College of Engineering and Technology. He worked as a lecturer in Joginapally B R Engineering College, Hyderabad. He completed his MCA in 2008, M.Tech(CSE) in 2010 from Acharya Nagarjuna university, Guntur with distinction. Till now he has published SIX international research papers. His area of interest is Operating Systems, Data Structures and the Software Testing Methodologies.