Chapter 6

Security Threats and Safety Measures

Learning Objectives

By the end of this chapter, learner will be able to:

- Name the different kinds of software licensing available
- Differentiate between freeware and open source software
- State how the use of shareware software is different from that of freeware software
- Differentiate between copyright and licensing
- Define cyberethics, cybersafety and cybersecurity
- State the purpose of cookies
- Tabulate the different phases of cyber ethics evolution
- List precautions that can be taken to ensure cyber safety
- Identify the different kinds of threats to cyber security
- State ethical behaviour to be followed as a cyber citizen
- Identify the different categories of cyber crime

INTRODUCTION

With the wide spread use of internet, networks and computers have become increasingly susceptible to threats. These threats destroy data as well the programs that computers use. The objective of these threats is to destroy the data and to steal the vital information stored in computers. This information is used by the attackers for their benefit. We occasionally hear about the data theft from credit card companies or banks, which lead to major financial losses. Also sometimes individual users are fooled in to giving their personal and sensitive information such as passwords or bank data leading to financial loss. This chapter shows various threats that computers and networks face.

1. VIRUSES

A computer virus is a program usually hidden within another simple program. It produces copies of itself and inserts them into other programs or files, in turn destroying the data and performing other malicious actions. Computer viruses are never naturally occurring; they are always man-made. Once created and released, however, their spread does not

remain directly under our control. While developing the viruses, programmers have specific target in mind such as data theft or destruction of software, which runs the computers. The virus can be transferred hidden in files, programs or even in disks. The viruses can be of different kind but a common virus is macro virus, which is discussed in detail here.

1.1 Macro Viruses

A simple macro is series of programming steps that are stored in a single location. Macro allows automation of many actions with only a single keystroke. These can be embedded in the program files. Many programs, such as Word and excel allow you to record a series of keystrokes and menu selections and then save them to a file. This helps eliminate doing the same action several times increasing efficiency. Macro viruses created with the intention of fooling the user can deceive them in sharing confidential information. This information can be used by the Macro to damage the computer data or software. The virus using macro files are most popular as they are:

- Easy to write.
- Can infect more people faster as they exchange documents and data frequently
- Can easily infect any computer capable of running Office and Internet

Macro viruses can corrupt data, create new files, move text, flash colors, insert pictures, send files across the Internet, and format hard drives. Macro viruses are increasingly used as transport mechanisms to drop off even nastier bugs. Macro viruses modify registries, forward copies of it through emails, look for passwords, copy documents, and infect other programs. Macro viruses can do a lot of different damage in a lot of different ways.

Example of macro Virus is Wazzo, W97M etc.

2. WORMS

Worms are very similar to viruses in the manner that they are computer programs that replicate copies of themselves (usually to other computer systems via network connections). Viruses often, but not always, contain some functionality that will interfere with the normal use of a computer or a program. Unlike viruses, however, worms exist as separate entities; they do not attach themselves to other files or programs. Because of their similarity to viruses, worms are also often referred to as viruses. Some examples of the worst Worms that impacted the web are as follows:

1. Jerusalem is one of the earliest worms that spread in 1987. It is also one of the most commonly known viruses. It used to delete files that were executed on each Friday the 13th. It was first detected in the city of Jerusalem.

2. In 1991, thousands of machines running MS-DOS were hit by a new worm, Michelangelo. The virus would overwrite the hard disk or change the master boot record of infected hosts.
3. In 2007 Storm Worm hit the computers. Once hit, your machine becomes part of a large botnet which performs automated tasks that range from gathering data on the host machine, to sending infected emails to others. About 1.2 billion emails were sent from the infected computers propagating infection.

Since Worms spread mostly through the email attachments, the best ways to avoid them is using caution in opening emails. If the email is from an unidentified source, it is always best to delete it. Most of the time worms attach themselves to email. Even the sender of email does not recognize what they have forwarded, as emails are sent automatically using all contact information in the user's profile.

3. TROJAN HORSES

A Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into the system. Since they look like sincere programs they are referred as Trojan like the Trojan horse of Greek mythology. The Trojan program does not attach itself to the files like a virus nor replicate itself like a worm but it does provide unauthorized access to user's computer.

They are mostly spread through internet downloads and online gaming programs. They mostly affect the targeted computers. The trojan program prompts you to do the normal functions such as inputting your email address or profile name. You do so, not knowing that, you have provided access to the malicious software. This software is capable of taking over the functionality of your computer. An infected computer will begin to operate slowly and will exhibit pop-ups from time to time. Eventually the computer will cease to operate, or crash.

The best way to avoid the Trojans is to adopt safe download practices. If you are not sure of the website safety, then it is probably best not to download any program from that source.

An example of the Trojan horse was "I love you" which infected several computers in USA and Asia, completely damaging the data of millions of computers

4. SPYWARE

A Spyware as the name suggest is a program used to spy on the computer system. This program will try to get all the confidential and sensitive information such as your bank

account numbers, passwords etc. Then this confidential data is misused to access user's accounts. Spyware can also change the configuration of your computer, generally without obtaining your consent first.

There are a number of ways Spyware or other unwanted software can get on to computer. A common trick is to covertly install the software during the installation of other software that is being downloaded such as music or video or a file-sharing program.

Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

SpyWare sends information back to the spy ware's home base via the user's Internet connection, thus it eats user's internet bandwidth. SpyWare applications running in the background can lead to system crashes or general system instability as they use memory and system resources of the user's computer.

SpyWare have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors. It also installs other SpyWare programs, read cookies, change the default home page on the Web browser. While doing so, it consistently relays this information back to the SpyWare author who will either sell the information to another party or use it for advertising/marketing purposes.

Some of the common Spywares are CoolWebSearch, Internet optimizer and Zango

5. MALWARE

Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. The intent of the malware is to damage the data or functionality of the computer or network. In fact all the threats mentioned above such as virus, Trojans etc are examples of Malware.

6. SPAMS

The term "spam" refers to unsolicited commercial email (UCE) or unsolicited bulk email (UBE). It is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. It is also referred as junk email. Unsolicited email mostly contains advertisements for services or products. However most of the spams are from marketers or user who are trying to deceive the users. The most commonly seen spam includes the following:

- Phishing scams, a very popular and dangerous form of email fraud
- Foreign bank scams or advance fee fraud schemes
- Other "Get Rich Quick" or "Make Money Fast" (MMF) schemes
- Quack health products and remedies

Spam emails is not only unwanted, it clogs your email accounts and uses unnecessary server space. This creates burden on servers in the businesses. Since Internet is a public platform, it is never possible to completely stop the Spam email. However precaution can be taken while looking at an unknown email addresses. Most of the email hosts can identify such users and help filter them.

Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender. It is because of these additional costs that most of the hosts are very keen that users use spam filters as well as report spams so they can be stopped.

7. HACKERS AND CRACKERS

Hackers and crackers are the software programmers who use dubious ways to get control over your computer and systems. The intent of both hackers and crackers is to gain control over your computer so that they can get the sensitive confidential information. They then use this information against you by stealing money, personal data, pictures, bank details and government military information, so on and so forth. This information can either be sold for money or hackers access account themselves to rob you directly. Originally hackers were the gifted programmers who gain access to the systems or network to show case the security loopholes to the administrators. Later the term cracker was coined for such activist who had intentions of doing malicious activities. Crackers have an end goal of destroying data and network for personal monetary gains.

8. ANTI VIRUS TOOLS

Anti Virus tools are the software programs that help us detect the virus in emails or files and hence protect our computers. These tools can detect virus, worms, Trojans as well as spyware and adware. They block us from visiting unsafe websites, and also downloading unsafe programs from such websites. They protect us from identity thefts and threats from phishing websites. There are several commercial antivirus softwares available such as Norton, Mcafee, K7, Quickheal etc.

9. DATA BACKUP AND SECURITY

As we discussed earlier, there are threats to the computers that are sometimes hard to avoid. Unknowingly we may open an email that may have virus attachments and can destroy all the program and data on our computer. That is why to protect ourselves from such unknown threat; we need to assure backing up the data. The basic principal on data back up is very simple, just make another copy of the data and keep it elsewhere than on the same computer. This guarantees that once the data on your computer gets corrupted due to a threat, you can reload the data again on your computer once it has been rectified. These days you have external hard drives which can back up data. Also most of the smart devices are also used to back up the data.

Before we discuss in detail how to use the security tools, here are some of the guiding principles to use the computers securely.

1. Using Security software such as Norton antivirus, Symantec etc.
2. Never share passwords
3. Beware of email attachments form unknown sources
4. Do not randomly download material from websites which has not been checked for security
5. Never propagate hoax or chain emails
6. Always logout your laptop or computer
7. Restrict remote access
8. Frequently back up important data and files
9. Use encryption or sites that use encrypted data

There are several security tools available which help us protect against all sorts of threats mentioned above. In brief, the tools are available for antispam, antivirus, firewalls, encryption tools, password managers and cleanup tools.

First Recorded Computer Crime

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and

livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Viruses

Case 1: Brain (in its first incarnation written in January 1986) is considered to be the first computer virus for the PC. The virus is also known as Lahore, Pakistani, Pakistani Brain, Brain-A and UIUC. The virus was written by two brothers, Basit and Amjad Farooq AM, who lived in Lahore, Pakistan. The brothers told TIME magazine they had written it to protect their medical software from piracy and was supposed to target copyright infringers only.

The virus came complete with the brothers' address and three phone numbers, and a message that told the user that their machine was infected and for inoculation the user should call them.

When the brothers began to receive a large number of phone calls from people in USA, Britain, and elsewhere, demanding them to disinfect their machines, the brothers were stunned and tried to explain to the outraged callers that their motivation had not been malicious.

They ended up having to get their phone lines cut off and regretted that they had revealed their contact details in the first place. The brothers are still in business in Pakistan as internet service providers in their company called Brain Limited.

Introduces or causes to be introduced any viruses or contaminant in that case, suit filed under Chapter IX of IT Act i.e. Section 43 as a Civil Wrongs under IT Act

Worms

Case 1: The 1988 Internet Worm was the first major worldwide computer security incident where **malware** (software that is malicious) propagated throughout the internet. This worm infected Unix servers, taking advantage of different types of vulnerability in installed code such as Sendmail and finger. The lessons from that incident are still valid and, surprisingly perhaps, the vulnerabilities identified that allowed the worm to cause such problems are still present in some modern software.

The perpetrator of the 1988 Internet worm (Robert Morris, a graduate student at Cornell University) meant no harm but was experimenting with what was possible. He is now a respected computer science researcher. Security authorities no longer accept such an excuse so you should not attempt any such security 'experiments'.

Case 2: Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Trojan horses

Case 1: Hacker sentenced to 21 months jail in TKBot Trojan horse case, Sophos reports

An American hacker has been sent to jail after using a Trojan horse to break into innocent internet users' computers.

Raymond Paul Steigerwalt, from Indiana, has been sentenced to 21 months in jail for his involvement in an international hacking gang which broke into computers around the world, including PCs at the United States Department of Defense, with a Trojan horse.

Steigerwalt, 21, was a member of the international "Thr34t-Krew" hacking gang which launched a Trojan horse designed to break into internet-connected computers. TheTroj/TKBot-A Trojan horse (also known as the TKWorm) exploited a **vulnerability** that is found on some Microsoft IIS web servers.

At least two computers belonging to the Department of Defense were infected and damaged by the malicious code. Between October 2002 and 7 March 2003, Steigerwalt and other members of the Thr34t-Krew gang were able to remotely control infected computers without the knowledge of the computers' owners.

Steigerwalt, who pleaded guilty to the charges, has been ordered to pay $12,000 to the Department of Defense for damage caused by the Trojan horse

Case 2: A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these 'friends' managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. An year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

Spyware

'Loverspy' Spyware Creator Now Most Wanted Internet Criminal on FBI's List

Carlos Enrique Perez-Melara, an ex-student of certain San Diego-situated college, was lately listed on Federal Bureau of Investigation's (FBI) list of Internet criminals, who were most wanted, because he had created "Loverspy" one notorious spyware also called "Email PI," published theverge.com dated November 7, 2013.

Perez-Melara, aged 33, had developed the malware valuing $89 such that it would catch a person who acted deceitfully while pretending to love. It dispatched one e-greeting card to the suspected deceiver which if viewed would plant one especially harmful Trojan capable of seizing e-mail ids, keystrokes, IM (instant messages) as well as movie from the victim's web-based camera. Following the Trojan's planting, the contaminated PC fully came under the control of the hacker.

Spams

Sanford Wallace, 43, also known as "Spamford Wallace" and "David Frederix", was arrested in Las Vegas on Thursday. Wallace is accused of hacking into 500,000 accounts to harvest friend lists between November 2008 and March 2009. He allegedly used the compromised lists to make more than 27 million unsolicited postings on Facebook walls that appeared to come from friends.

If targets clicked on links within the messages, they were presented with a website designed to fool them into handing over their full name, email address and password, prosecutors said. Finally they would be redirected to affiliate websites that would allegedly pay Wallace "substantial revenue" for traffic.

The scheme relied on vulnerabilities that Wallace discovered in Facebook's spam filters, according to the indictment.

"To accomplish his scheme, Wallace first tested his spamming capabilities between two Facebook accounts," it said.

"[He] used a fake Facebook account of 'David Frederix' and his legitimate 'Sanford Masterwb Wallace' account to test variations of spam messages in order to evade Facebook's filtering mechanisms.

"Once Wallace evaded Facebook's spam filters he employed an automatic scripting process to sign into a compromised Facebook user's account, retrieve a list of all the user's friends, and then post a spam message to each of the user's friend's Facebook walls."

Wallace is now indicted on a total of 11 charges of fraud, intentional damage to a protected computer, and criminal contempt.

The contempt charges relate to an earlier **civil case brought against Wallace by Facebook itself**.

A federal judge awarded the dominant social network $711m in damages in October 2009. The firm did not expect Wallace to pay, but the judge also ordered him not to log in to Facebook. According to Thursday's indictment he "wilfully and knowingly" breached that order.

Wallace, who first gained notoriety as a spammer in the 1990s and also lost a civil case brought against him by MySpace in 2008, was released on $100,000 bail. He faces up to three years in jail and a $250,000 fine for each of the six fraud charges and up to 10 years in jail for each of the three charges of intentional damage to a protected computer.

Facebook welcomed the arrest.

"We applaud the efforts of the US Attorney's Office and the FBI to bring spammers to justice,"

"Two years ago, Facebook sued Wallace and a federal court ordered him to pay a $711 million judgment for sending unwanted messages and wall posts to people on Facebook. Now Wallace also faces serious jail time for this illegal conduct."

Hackers and Crackers

An engineering dropout and global hacker, is in the CBI net. He is part of a global network of hackers and was arrested from Pune following a tip-off from the FBI. He was flown to New Delhi in the evening.

This is for the first time that a global network of cyber hackers has been traced to India. Investigating agencies of China, Romania and the United States collaborated with the CBI to pounce upon the 32-year-old professional hacker who, a source said, had compromised more than 1,000 internet accounts around the world.

The CBI claims that his hacking syndicate has been active in India since 2011, and that he has confessed to hacking 950 foreign email accounts besides 171 in India. He was arrested from his house in Pune and taken to New Delhi on a transit-remand for further questioning.

The CBI tracked him down after the FBI passed on information on the global network of cyber hackers. Simultaneous raids were conducted in Mumbai and Ghaziabad.

This is not the first time he has been arrested. In 2003, he was arrested by the Mumbai police for defrauding a Mumbai-based credit card processing company of nearly Rs9 lakh when he was only 21 and pursuing a degree in engineering in Pune. At that time, he was operating a website designing services start-up www.mafiaz.com. During investigation, police found several fictitious names of clients and bank account numbers in his computer.

"Though he has claimed to have hacked into the email accounts of over 900 people globally, the kind of clientele whom he was serving is still to be established. From identify theft to corporate rivalry, he was serving all types of clients," a CBI officer said. But he hacked only email accounts and not bank accounts.

CBI claimed that he was operating through two websites — www.hirehacker.net and www.anonymity.com — and was charging between $250-500 for his service. He was paid via Western Union money transfer and Paypal. He used to send the money to his father and girlfriend.

"As part of an international law enforcement operation, the CBI has registered two cases against suspected operators of hacking websites. Similar operations are being conducted in Romania, China and the US. It is suspected that the number of email accounts hacked may be much larger once the data is collected and the accused are interrogated," a CBI officer said.

The hacker's clientele included jilted lovers and corporate entities. After registering the cases, the CBI carried out searches in two locations in Mumbai and one each in Pune and Ghaziabad for violations of various sections of the IT Act and section 379 of the IPC.

Sections applicable in hacking

Hacking is punishable under section 66 read with section 43 of the Information Technology Act, 2000.

Punishment/Fine

The person can be punished with up to three years imprisonment or fine up to Rs5 lakh or both.

***Name of hacker Hidden purposefully

Summary of Sections Applicable for Cyber Crimes

Cyber Crime ITAA 2008 Act Section's -IPC Section's

Email spoofing 66D- 416,417,463,465,419

Hacking 66,43-378,379,405,406

Web-jacking 65 -383

Virus attacks 43,66

Logic bombs 43,66

Salami attacks 66

Denial of Service attacks 43

Email bombing 66

Pornography & Child Pornography 67, 67B -292,293,294

Bogus websites, cyber frauds 420

Forgery of electronic records 463, 465, 470, 471

Sending defamatory messages by email 66A- 499, 500

Sending threatening messages by email 66A -503, 506

Financial Crime 415,384,506,511

Cyber Terrorism 66F -153A, UAPA 15-22

Identity Theft 66C-417A, 419A

Website Defacement 65 -463,464,468,469

Summary

- A computer virus is a program usually hidden within another simple program.
- Macro viruses created with the intention of fooling the user can deceive them in sharing confidential information.
- Worms are very similar to viruses in the manner that they are computer programs that replicate copies of themselves.
- A Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into the system.
- A Spyware is a program used to spy on the computer system to get all the confidential and sensitive information such as your bank account numbers, passwords etc.
- Malware is any kind of unwanted software that is installed without your adequate consent.
- Spam emails is not only unwanted, it clogs your email accounts and uses unnecessary server space. It is also referred as junk email.
- Hackers were the gifted programmers who gain access to the systems or network to show case the security loop holes to the administrators.
- Cracker was coined for such activist who had intentions of doing malicious activities.

EXERCISE

A. Multiple Choice Questions

1. Which of the following is an anti-virus program
   (a) Norton (b) Quick heal
   (c) K7 (d) All of these

2. All of the following are examples of real security and privacy threats except:
   (a) Hackers (b) Spam
   (c) Virus (d) Worm

3. Trojan horses are very similar to virus in the matter that they are computer programs that replicate copies of themselves.
   (a) True (b) False

4. _____ monitors user activity on internet and transmit that information in the background to someone else.
   (a) Malware (b) Adware
   (c) Spyware (d) None of these

5. Viruses are _____.
   (a) Man made (b) Naturally occur
   (c) Machine made (d) All of the above

6. Firewall is a type of _____.
   (a) Virus (b) Worm
   (c) Security threat (d) None of the above

7. Unsolicited commercial email is known as _____.
   (a) Spam (b) Virus
   (c) Malware (d) Spyware

B. Match the following

(1) Virus	(a) "Get Rich Quick" Scheme
(2) Worm	(b) Cool Web Search
(3) Trojan Horse	(c) I Love You
(4) Spyware	(d) Jerusalem
(5) Spam	(e) Wazzo

C. Answer the following questions:

Q.1. While working on the computer, you notice that the system is working very slowly, files are corrupted, default home page on the web browser has changed, lot memory is consumed, and unnecessary pop-ups are coming. What can be the probable reason?

Q.2. You have very important data on your computer. How will you ensure that this data remains safe?

Q.3. Differentiate between virus, worms and Trojan horses.

Q.4. How is a hacker different from a cracker?

D. Lab Session

- Search the internet for various new viruses and worms that surfaced in last year.
- Research various email spams that are sent out these days. How many of these have you seen which are related to banks? Please visit bank websites and identify if they have messages about spams.
- Make a list of security tools available for your computer by researching on the internet and t ell what all threats they protect you from.
- Make a list of different anti-virus programs available today, along with their pricing and protection features.
- Scan your system to find out different security threats infecting your computer.
- Do a survey and find out how many people are comfortable making payments online. If they are not, find reasons for the same. Also suggest them the ways to make online payments safe.