

12

Data Protection


Outline

12.1 Introduction

We live in a world at a time which is often called information age where information is freely available from any part of the world. The Internet has revolutionised the world and people are getting used to having access to whatever information they want anytime, anywhere and from a wider and wider range of computing devices.

Unfortunately, this also has resulted in increased security concerns. Now, even if you ensure not to use any external media on your computers but if you are connected to the Internet, your computer and data on it is still vulnerable.

This chapter talks about the threats that are associated with online access and the measures to prevent and counter them, if ever they occur.

- 
- 12.1 Introduction
 - 12.2 Threats to Data
 - 12.3 Data Protection Solutions
 - 12.4 Firewall – An Important Solution for Computer Security

12.2 Threats to Data

A **threat** is a potential violation of security. When a *threat* is actually executed, it becomes **attack**. Those who execute such actions, or cause them to be executed are called *attackers*.

Some common threats the average computer user faces every day are being given below :

- ⇒ Viruses : ⚡ *Worms* ⚡ *Trojans*
- ⇒ Spyware
- ⇒ Adware
- ⇒ Spamming
- ⇒ PC Intrusion :
 - ⚡ *Denial of service*
 - ⚡ *Sweeping*
 - ⚡ *Password Guessing*
- ⇒ Phishing

Before we talk about various data threats, you should know that other than data threats, **regular computer maintenance** is required to keep your computer in a good working condition. You should maintain your computer by following these steps :

- ⇒ *Keep your computer hardware dust free.*
You should keep your computer hardware clean by keeping it in dust free environment and regular cleaning of accumulated dust, if any, using the appropriate devices such as blowers designed for the same.
- ⇒ *Keep your computer software clean.*
You should keep uninstalling unused /unwanted software and keep removing junk and temporary files from your computer's disk.

The above steps will ensure that your computer is clean and maintained and thus usable for a longer time. After this basic computer maintenance steps, let us talk about different data threats and ways to handle them.

12.2.1 Computer Viruses

Computer viruses are malicious codes/programs that cause damage to data and files on a system. Viruses can attack any part of a computer's software such as boot block, operating system, system areas, files and application-program-macros etc.

Two other similar programs also cause virus like effects. These are :

- (a) **Worms.** A worm is a self-replicating program which eats up the entire disk space or memory. A worm keeps on creating its copies until all the disk space or memory is filled.
- (b) **Trojan Horses.** A Trojan horse is a program that appears harmless (such as a text editor or a utility program) but actually performs malicious functions such as deleting or damaging files.

NOTE

Malware is a general term used to refer to viruses, worms, spyware, adware etc. In other words, it is unwanted software that someone else wants to run on your computer. Malware infects your computer, making it behave in a way, which you do not approve of.

DAMAGE CAUSED BY VIRUSES

Viruses can do the following if left unchecked :

- ◆ **Damage or delete files.** Some viruses may delete or damage random documents or specific files that are crucial to your operating system—for example, operating system files. This damage can range from rendering useless just a few files to affecting your entire computer, possibly requiring you to reinstall your operating system and start from scratch.
- ◆ **Slow down your computer.** Viruses can run in the background, without being seen, and may cause your computer to run extremely slow.
- ◆ **Invade your email program.** Some forms of viruses may wreak even more havoc by spreading themselves to the contacts in your address book.

NOTE

Not all computer problems are caused by viruses. Even though your computer, or a particular program, may not be running properly, this could be caused by other things, such as a bug (which is simply an error in the application's code), or misconfiguration of software or hardware.

12.2.2 Spyware

Spyware is a software which is installed on your computer to spy on your activities and report this data to people willing to pay for it. It tracks the user's behavior and reports information back to a central source. These are used to spy on someone either for legal or illegal purpose.

Spyware mostly get installed on your PC without your consent. Typically, spyware finds its way onto PCs by "piggybacking" onto a file, or gets downloaded from the Internet when you visit a particular website. Pests such as spyware can often lurk silently on your computer until someone or something sets them off, or until they are found and properly removed.

NOTE

Do you know that roughly 32% computers of the world are infected with some types of malware.

DAMAGE CAUSED BY SPYWARE

Spyware can act like a peeping tom or, at worse, a geeky thief.

For example, it :

- ◆ **Compromises your data, computing habits, and identity.** Spyware can monitor information about your computing habits, such as what websites you visit, or record your keystrokes, which in the end can lead to identity theft. For example, spyware can record the keystrokes that you use while keying in a credit card number and send this number to a "cyberthief."
- ◆ **Alters PC settings.** Some forms of spyware can also alter computer settings like your web browser home page setting or the placement of your desktop icons. This doesn't do much damage to your PC, but it's really annoying.
- ◆ **Slows down your PC.** Spyware can rob your PC or system speed and Internet access efficiency. This can become a big problem when you're trying to use the programs on your PC, watch videos online, or download large files.

12.2.3 Adware

These are the programs that deliver unwanted ads to your computer (generally in Pop-Ups form). They consume your network bandwidth. Adware is similar to spyware—however, it may be installed with your consent. So it is advised that you thoroughly read installation agreements before you allow installation of a software.

DAMAGE CAUSED BY ADWARE

Adware comes complete with the following disadvantages :

- ◆ **Adware tracks information just like spyware.** Adware tracks information about your data and computing habits to produce targeted advertising, such as pop-up ads, on your computer screen.
- ◆ **Displays arrays of annoying advertising.** When infected with adware, you will likely see frequent pop-up ads appear out of nowhere. This may even happen every time you open your web browser.
- ◆ **Slows down your PC.** The adware software working in the background and the bombardment of ads can slow your PC to a crawl.

12.2.4 Spamming

Spamming refers to the sending of bulk-mail by an identified or unidentified source. In non-malicious form, bulk-advertising mail is sent to many accounts. In malicious form (e.g., e-mail bombing), the attacker keeps on sending bulk mail until the mail-server runs out of disk space.

NOTE

You can't get a virus simply by reading email. It is activated only when you click a link in it or open an attachment.

DAMAGE CAUSED BY SPAMMING

Spamming comes complete with the following disadvantages :

- ◆ **Spam reduces productivity.** The billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance, and reduce overall productivity.
- ◆ **Spam eats up your time.** Deleting spam emails seems like the simple solution, but it eats up a significant amount of productivity.
- ◆ **Spam can lead to worse things.** Spam messages may contain offensive or fraudulent material and can even be used to spread viruses.

12.2.5 PC Intrusion

Every PC (personal computer) connected to the Internet is a potential target for hackers. Computers are under constant attack from cyber vandals. PC Intrusion can occur in any of the following form.

- (i) **Sweeper Attack.** This is another malicious program used by hackers. It sweeps *i.e.*, deletes all the data from the system.
- (ii) **Denial of Services.** This type of attack eats up all the resources of a system and the system or applications come to a halt. Example of such an attack is flooding a system with junk mail.
- (iii) **Password Guessing.** Most hackers crack or guess passwords of system accounts and gain entry into remote computer systems. And then they use it for causing damages in one or another form.

12.2.6 Eavesdropping

Eavesdropping is a passive attack in which an attacker gains access to the communication-medium through which some communication is taking place and then listens to the communication and gets information about the content of the message.

EAVESDROPPING

“ Unauthorised monitoring of other people’s communications is called **Eavesdropping** ”

Eavesdropping can be carried out through all communication devices and media of today—telephone systems, emails, instant messaging, other Internet services (e.g., chat rooms, social networking websites etc.), mobile devices etc. Eavesdropping activities do not affect normal operation of transmission and communication ; thus both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced.

For example, while sending emails, if the email message is not encrypted and digital signature has not been used, then the attacker can exploit these security loopholes. Because of these security lapses, the attacker can launch a *Man-in-the-Middle attack* on the network and intercept the message being transmitted. The attacker can then deface the message and send it to the recipient. The recipient is then deceived into believing the defaced message is the real message and may act as per the defaced message and may provide personal or sensitive information.

Similarly, sending or providing confidential information over insecure protocols like HTTP makes the information more prone to eavesdropping attack.

12.2.7 Phishing and Pharming

It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card information, account data etc. In Phishing, an imposter uses an authentic looking email or web-site to trick recipients into giving out sensitive personal information. For instance, you may receive an email from your bank (which appears genuine to you) asking to update your information online by clicking at a specified link. Though it appears genuine, you may be taken to a fraudulent site where all your sensitive information is obtained and later used for cyber-crimes and frauds.

Pharming (pronounced “farming”) is an attack in which a hacker attempts to redirect a website’s traffic to another, bogus website. Through pharming attack, the attacker points you to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

In this the attacker convinces you that the site is real and legitimate by spoofing or looking almost identical to the actual site down to the smallest details. You may enter your personal information and unknowingly give it to someone with malicious intent.

12.2.8 Cookies

A cookie, also known as a web cookie or a browser cookie, is a small piece of data sent from a website and stored in a user’s web browser (in a text file) while a user is browsing a website. Some cookies disappear after user closes his browser while others, known as tracking cookies, remain saved and load the next time user visits the same websites.

These cookies help track user’s browsing sessions and load information faster, but create some security and privacy concerns as well.

1. **Session Data.** When you visit a website on a regular basis, such as your email or online bank, you may not have to enter your username and password to get in. That's because the information is being pulled from a tracking cookie. While these cookies encrypt the information they store, if somebody found out the encryption key and acquired your cookies, he could discover your passwords. While the odds of this happening are extremely small, the risk does exist.

2. **Tracking Information.** When you visit certain websites with advertisements, those ads create cookies that store and track your online patterns. You may have noticed that if you go to a clothing store's website, for example, you'll see ads for that store when you click away to other websites. That's because tracking cookies have relayed this information back to the advertisers, who use it to target their ads. Sometimes, your information may be sold to other companies. Some people view this as an invasion of privacy.

3. **Public Computers.** While the same general threats exist for traffic cookies saved on public or shared computers as those saved on your personal computer, the much larger amount of people who have access to these computers makes saving traffic cookies more risky. When you finish using a public or shared computer, delete the cookies to ensure that the next people who use the same computer can't access the information.

12.3 Data Protection Solutions

The entire computer security is based on a system of actions and safeguards that are designed to protect a computer system from deliberate (or accidental) access and/or damage by these threats. In this section, we are going to categorize the solutions to these threats in *two* ways :

- ⇒ Active Protection
- ⇒ Preventive Measures

Active Protection

Installing and properly using an antivirus software that includes internet security—which includes protection against threats such as viruses, Spyware, and PC intrusion—is vital for proper protection against the hackers, intruders, and other wrongdoers.

Preventive Measures

Even though security programs may actively detect and eliminate any threats your PC encounters, you should always help to prevent these issues from ever arising.

Let us now move on to the real solutions to the threats that we have discussed so far.

12.3.1 Solutions to Viruses, Adware and Spyware

There are thousands of viruses, Spyware and other Malware currently "*in the wild*," and more appear each week, so protecting your systems against infection by viruses is an essential part of information security.

Protecting yourself against viruses involves the following safeguards :

Active Protection

- ⇒ Use Anti-Virus and Anti-Spyware software.
You need these programs help to detect and eliminate any malware that sneaks its way onto your PC.

If a virus somehow is found on a system on your network, you should do the following:

- ◆ Scan all your systems for evidence of the virus.
- ◆ Disconnect any infected systems immediately from your network.
- ◆ Restore the infected systems from a clean backup.
- ◆ Notify your antivirus vendor so it can ensure its signature database is up-to-date.

◆ **Download updates regularly.**

New viruses and other malware emerge everyday, and your security software needs to know about them in order to provide full protection. This is done through *signature file updates*, so that your anti virus is laden with all new emerging viruses.

To keep you antivirus, anti-spyware program updated, the best option is to set the program to *automatically update* when needed, so you don't have to worry— you'll always be fully protected.

◆ **Run frequent full-system scans.**

Even though most security software programs actively scan your PC for malware, you should also perform a full system scan at least once a month.

Preventive Measures

◆ **Keep your system up-to-date.**

Malware often takes advantage of security holes in operating systems and software programs. You should always install any available updates for your operating system, such as Windows, and any common software you use.

◆ **Use caution when downloading files on the Internet.**

Only download files from reputable websites by looking for signs, such as a privacy statement, full contact information, and SSL encryption of sensitive information, typically indicated by a padlock in the lower-right corner of your web browser.

◆ **Be careful with email.**

Email is a very convenient and useful communication method; however, it is also used by hackers, spammers, and criminals to get what they want. Follow these guidelines :

- ◆ Don't download or open unsolicited email attachments.

- ◆ Watch for Phishing scams. Be careful of an email that asks you to verify your personal details. Don't click on any link provided in the email. Rather type the address of concerned bank or site in browser and find out the truth.

- ◆ Check for security alerts.

- ◆ Review your web browser settings regularly *e.g.*, disable running of scripts and cookies etc.

- ◆ Disconnect from the Internet when you're away.

COOKIES

“ Cookies are small files created on client computers when these systems browse certain Web sites. These cookies can contain information about the user. ”

12.3.2 Solutions to Spam, Eavesdropping

Spam has become the bane of the Internet, and still there is no real solution in sight. Spam is usually defined as “unsolicited e-mail” and resembles the flyers from stores that clog your newspapers each morning, but it's much more than that.

Protecting yourself against Spam involves the following safeguards :

Active Protection

- ⇒ Use Anti-Spam software.

Following are two of the main methods used by anti-spam software to get rid of spam :

- (i) **Sender filtering.** This method allows only messages from your approved sender list to reach your inbox – all other mail is quarantined for later review. *Sender filtering* is done on the basis of *digital certificates* and *digital signatures*.

- ◆ **Digital Certificates**, specially formatted digital information issued to website, are used to verify the identity of the message sender to the recipient. Digital certificates are issued by a certificate authority (CA) that is trusted by both the sender and recipient.

- ◆ **Digital signatures** are a way of authenticating the identity of creators or producers of digital information. A digital signature is like a handwritten signature and can have the same legal authority in certain situations, such as buying and selling online or signing legal contracts.

- (ii) **Keyword filtering.** This method filters out email messages that contain certain keywords or phrases, which are defined by you or others.

DIGITAL CERTIFICATES

“ **Digital Certificates**, specially formatted digital information issued to website, are used to verify the identity of the message sender. ”

DIGITAL SIGNATURES

“ **Digital signatures** are a way of authenticating the identity of creators or producers of digital information. ”

Preventive Measures

- ⇒ Keep your email address private.

Be careful whom you give your email address to. Before giving your address out on an online form, check if there is a website privacy policy. This policy typically informs you of how they handle your personal information. Signing up for free offers seen online or by email may dramatically increase your chances of receiving spam messages.

- ⇒ Use encrypted connection always especially if you have to provide sensitive information. Encrypted connections are made possible through protocols like Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) and offer better security to data being transmitted.

- ⇒ Install personal firewall on computers connected to the Internet so as to keep a check on incoming and outgoing information and connections.

- ⇒ Always avoid conducting online transactions or using online banking services on public networks or public Internet facilities (e.g., public WiFi).

- ⇒ Install protection software such as **Internet security software** that also provides intrusion prevention system to detect and prevent further attacks by eavesdroppers.

12.3.3 Solutions to PC Intrusion

The combination of identification, authentication and authorization can control access to a system. This combination is very useful especially in network security. Various techniques used for network security are given below :

Active Protection

- ◊ Authorization

Asking the user a legal login-id performs authorization. If the user is able to provide a legal login-id, he/she is considered an *authorized user*.

- ◊ Authentication

Authentication is also termed as **password-protection** as the authorized user is asked to provide a valid password, and if he/she is able to do this, he/she is considered to be an *authentic user*.

- ◊ Firewall

A system designed to prevent unauthorized access to or from a private network is called **Firewall**. Firewalls are a mechanism to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

Preventive Measures

- ◊ Use proper File access permissions when sharing files on the Internet.

File access permissions refer to privileges that allow a user to read, write or execute a file.

- If a user has **Read permission** for a file, he/she can view and read the file.
- If a user has **Write permission** for a file, he/she can edit and write into the file.
- If a user has **Execute permission** for a file, he/she can execute the file.

File permissions are given for *three* sets of users : *owner*, *group* and *others*.

- **Owner** – the user who has created the file.
- **Group** – the group of users who are working with the owner as a group.
- **Others** – all other users.

So, you can decide upon the file permissions, so that an unknown user does not get write or execute permissions at all.

- ◊ Disconnect from the Internet when away

Using “always on” Internet connections such cable and DSL increases your chances of some infections and intrusions as your PC is always connected to the Internet. This doesn’t mean you should switch back to dial-up Internet— however, you may want to disconnect from your “always on” connection when you don’t plan on using it for a long period of time.

12.3.4 Solutions to Phishing and Pharming Attack

Phishing is the fishing for confidential information. It is a scam that encompasses fraudulently obtaining and using an individual’s personal or financial information. **Pharming** refers to the redirection of an individual to an illegitimate Web site through technical means. To counter these evil twins is a task where you need alertness and carefulness.

You can use following safeguards to counter these attacks :

Active Protection

If, somehow, you have become a victim of these attacks, then follow these guidelines :

- ◊ Take the computer offline

Disconnecting from the internet reduces the probability of infecting other devices in the same network with malware.

⇒ Backup all files on the hard drive

If backing up data is routinely done, it is only necessary to backup new files. Focus on capturing all sensitive data and irreplaceable files such as videos and family photos.

⇒ List the information given to phishing scammers

Depending on what was leaked, one may need to change passwords, or cancel credit cards etc. BUT here you need to be very very cautious. DO NOT USE THE COMPROMISED COMPUTER TO CONTACT AGENCIES because using the same device may open users to the risk of a freshly installed *keylogger*, which can record the new password as well.

⇒ Run anti-virus software.

Do not trust free anti-virus programs. They can be malware in disguise. It is advised to take the infected computer to a professional who specializes in malware removal.

⇒ Contact credit agencies to report any possibilities of identity theft

Reach out to credit bureaus that operate and manage the credit cards, as it will sound the alarm to potential creditors.

Preventive Measures

Phishing, and to a lesser extent, *pharming*, rely on tricking users rather than advanced technology, the best way to handle these threats is through vigilance.

- ⇒ Don't open emails from unknown sources or click on links embedded in suspect messages.
- ⇒ Check the security guidelines of websites such as PayPal so that you can distinguish between legitimate and bogus emails.
- ⇒ Also, rather than clicking on the link embedded in an email, you can type the general link in your web browser (e.g. <http://www.paypal.com>).
- ⇒ Most important, **when in doubt, do not click.**

Physically protecting systems

- ❖ Keeping important computers such as servers or mainframes in locked rooms.
- ❖ Posting security guards.
- ❖ Security locks, smart cards.
- ❖ Keeping sensitive data on stand-alone machines instead of networks.
- ❖ Using alarm systems and video cameras.

Using software to protect systems

- ❖ **Data encryption.** It is a method in which data is 'scrambled' before being transmitted through a network. Only the authorised recipient has the 'key'.
- ❖ **Firewalls.** A software to block access from outside (and to prevent data being sent out in some cases).
- ❖ **Activity or Audit logs** to track who has been doing what on the system.
- ❖ **User IDs and Passwords** – to authenticate users.
- ❖ **Access rights** – to ensure information safety.

12.3.5 Data Privacy vs. Data Protection

So far you have read that data protection is about securing data against unauthorized access. Data privacy is a related term that is about authorised access, *i.e.*, who can access and track the data of your organisation. As you must be aware that when you surf the Internet, websites tend to collect various types of data such that :

- ⇒ IP addresses of the user's computer (*user's location*).
- ⇒ Information about usage of website. *For example*, what users click on and how long they spend on a page.
- ⇒ Information about browsers and device used to access the sites.
- ⇒ Browsing activity across different sites.

Data privacy is about the users/sites/service providers who can use the collected data and what are their rights related to that. It involves assigning the rights to use data in a specific way, *e.g.*, only some sites are allowed in your local networks.

Data privacy rules of an organisation govern the decisions like :

- ❖ Which websites are blocked in the local network ?
- ❖ Which internet browsers are allowed on your network ?
- ❖ Which ISPs (Internet Service Providers) can access and tracking your information and your browser history ?
- ❖ And so on.

DATA PRIVACY

“ Data privacy refers to the rules about the authorised access of data, *i.e.*, which all users/sites/service providers etc. can access or track the data/ browsing information. ”

NOTE

Data protection is essentially a technical issue, whereas data privacy is trust based and has associated legality.

Safe Internet Surfing Rules

In nutshell if you follow the below given smart and secure internet surfing rules, your data and information will remain safe and keep the fraudsters away.

- (i) Download only from secure websites and official app stores
- (ii) Always type the URLs rather than using a webpage or email link.
- (iii) Avoid clicking on unknown links.
- (iv) Use regularly updated anti-virus software
- (v) Look for secure URLs (with https) while providing data or making payments.
- (vi) Avoid using the proxy site and proxy software

Check Point

12.1

1. Both email attachments and downloaded files can spread malware.
 - (a) True (b) False
2. What is a firewall ?
 - (a) A wall that is reinforced and cannot catch on fire.
 - (b) A program that protects against viruses.
 - (c) A filter for an Internet connection that monitors outgoing and incoming activity.
3. A strong password should contain :
 - (a) Both uppercase and lowercase letters.
 - (b) A word that is easy to remember, such as the name of a pet.
 - (c) At least 8 characters, and a combination of letters, numbers, and characters.
4. Which type of program can send out information about your web browsing activities or other personal details ? (a) Cookies (b) Spam (c) Spyware (d) Trojan.

12.4 Firewall – An Important Solution for Computer Security

An Internet firewall is a device or software that is designed to protect your computer from data and viruses that you do not want. A firewall is so called because of the real firewalls used to secure buildings. A physical firewall is a set of doors that closes in a building so as to contain a fire to one area, preventing the entire building from being destroyed. Likewise an Internet firewall is designed to shut off access to your operating system or to other computers that are connected to your network.

FIREWALL

“ A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. ”

Firewalls can be implemented in *two* forms :

1. Software Firewall

A software firewall is a special type of computer software running on a computer. It protects your computer from

outside attempts to control or gain access, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms.

2. Hardware Firewall

It is physical piece of equipment designed to perform firewall duties. A hardware firewall may actually be another computer or a dedicated piece of equipment which serve as a firewall. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network.

Firewalls keep out malevolent hackers and people who intended to do damage and take over other peoples' servers. Firewalls really serve no other purpose. Firewalls seek to limit the access to a server or computer and let in only the people who need to be there.

NOTE

Confidentiality of information ensures that only authorized users get access to sensitive and protected data.

LET US REVISE

- ❖ A **threat** is a potential violation of security. When a threat is actually executed, it becomes **attack**.
- ❖ Computer viruses are malicious codes/programs that cause damage to data and files on a system.
- ❖ A worm is a self-replicating program, which eats up the entire disk space or memory.
- ❖ A trojan horse is a program that appears harmless (such as a text editor or a utility program) but actually performs malicious functions such as deleting or damaging files.
- ❖ Spyware is a software which is installed on your computer to spy on your activities and report this data to people willing to pay for it.
- ❖ Adware are the programs that deliver unwanted ads to your computer.
- ❖ Malware is a general term used to refer to viruses, worms, spyware, adware etc.
- ❖ Spamming refers to the sending of bulk-mail by an identified or unidentified source.
- ❖ Phishing is the criminally fraudulent process of attempting to acquire sensitive information pertaining to a user.
- ❖ To keep a computer protected, one should use updated software, be cautious while handling mails and surfing Internet, scanning computer regularly etc.

Objective Type Questions

O T Q s

Multiple Choice Questions

1. A worm is...
 - (a) A slimy pink thing that lives in dirt.
 - (b) Pieces of malicious code that make copies of themselves and spread through computers without human interaction.
 - (c) An unsolicited email message.
2. If you receive an email claiming to need your username and/or password, what should you do?
 - (a) Report it as phishing/spam through your email provider
 - (b) Delete the message
 - (c) Reply to the message with your email and password