ICT in Business

Computer Threats & Basic Security Measures

Learning Objectives

In this chapter you will learn about:

- Basic Concept of Threat
- Types of Threats
- Threats to the User
- Threats to Hardware
- Threats to Data
- Security Measures for Threats

Threats

- Computer security threats are constantly evolving. These threats are masters of disguise and deception, always evolving new ways to irritate, steal, and harm.
- A threat is any scenario or occurrence that has the potential to harm the computer through unauthorized access, destruction, disclosure, data manipulation, and/or denial of service.
- Basically, a computer threat is a term that relates to the security of a computer system being compromised. This is possible dangers that can affect the smooth functioning of a computer.
- This threat can lead to cyber-attacks and data being stolen, lost, or manipulated. Damage can be irreparable in some cases.

Threats

- A computer threat can be "intentional" such as hacking or "accidental" such as malfunctioning or physical damage.
- If a user can gauge the degree of harm that different threats can cause, they can prioritize them and take countermeasures.
- Regularly backing up users data is a countermeasure against the treat of data loss. A firewall is a countermeasure against hackers.
- In the present age, computer security threats are constantly increasing as the world is going digital.

Types of Threats

Computer threats can be classified into:

- **Threat to the User**
  - ✔ Identity Theft
  - ✔ Loss of Privacy
  - ✔ Computer Related Injuries
  - ✔ Online Spying Tools
  - ✔ Email Spam
- **Threat to Hardware**
  - ✔ Power Related Threats
  - ✔ Theft and Vandalism
  - ✔ Natural Disasters
- **Threat to Data**
  - ✔ Malware, Viruses and Malicious Programs
  - ✔ Cybercrime
  - ✔ Cyber Terrorism

Threat to the User

Identity Theft

- Identity theft is a form of crime in which someone's personal information is used without permission.
- Public profiles on social networks or other popular online services can be used as the source of data, helping criminals to impersonate their targets.
- Affected individuals can suffer financial loss due to unauthorized withdrawals and purchases made in their names.
- However, identity theft can also be done to damage the victim's reputation.

Threat to the User

Methods of Obtaining Information

Criminals obtain information by using various methods, such as;

- **Shoulder Surfing;** Shoulder surfing means watching someone while entering personal ID information for a private transaction.
- **Snagging;** A thief can try to snag information by listening through a telephone extension, through a wiretap while the victim gives credit card information to a legitimate agent.
- **Dumpster Diving;** Dumpster diving is looking for treasure in someone else's trash. In the world of information technology (IT), dumpster diving is a technique used to retrieve information that could be used to carry out an attack or gain access to a computer network from disposed items.
- **Social Engineering;** Social engineering is the art of manipulating people so they give up confidential information such as passwords or bank information by disguising as something legitimate.
- **High Tech Methods**; The ID thieves can get information using a computer and Internet connection. A person's identity may be snagged from unsecured internet sites.

Threat to the User

Loss of Privacy

- People are disclosing their personal information while transactions and that information are being generated and reaching the hands of other parties. Thus, privacy could be lost.
- Social media records that are open to the public are another way of losing privacy.

Threat to the User

Computer Related Injuries

- Computer use can cause physical injuries to the user.
- Prolonged mouse and keyboard use, staring at a monitor for long time, and poor seating conditions are the primary cause of such injuries.
- It can cause especially eyesight problem and other health related problems.

Threat to the User

Online Spying Tools

Software developers have created a number of ways to track user's online activities using internet. Many of these tools, which may pose a threat to users, are discussed further below;

- **Cookies**

Cookies are regarded as a significant threat to privacy, despite their beneficial purpose. This is because they can be used to store and report many types of information, like user online activity history, visited sites, passwords, etc. Later, these can be used against the user's wishes.

- **Web Bugs**

A web bug can record what pages user view, key words user type into a search engine, personal information user enter in a form on a web page, and other data. Because Web bugs are hidden, they are considered by many to be eavesdropping devices.

Threat to the User

- **Spyware**

Spyware is installed on a computer without the user's knowledge and collects information without the user's consent. Spyware can record individual keystrokes, Web usage, e-mail addresses, personal information, and other types of data. Besides, spyware can also refer to legitimate software that monitors your data for commercial purposes like advertising. However, malicious spyware is explicitly used to profit from stolen data.

Threat to the User

Email Spam

- Email spam, also referred to as junk email or simply spam, is unsolicited messages sent in bulk by email.
- Most email spam messages are commercial in nature. Whether commercial or not, many are not only annoying as a form of attention theft, but also dangerous because they may contain links that lead to phishing web sites or sites that are hosting malware or include malware as file attachments.
- Spammers collect email addresses from chat rooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers.

Threats to Hardware

Power Related Threats

- Power problems affect computer in two ways:
  - ✔ **Power fluctuations**, when the strength of your electrical service rises or falls, can cause component failures.
  - ✔ **Power failure**, when power is lost altogether, causes systems to shut down.
- Both power failures and fluctuations can result in a loss of data. Uninterruptible Power Supplies (UPS) can be a countermeasure to this threat.

Threats to Hardware

Theft and Vandalism

- Thieves can steal the entire computer or cause hardware vandalism, which is the act of intentionally or unintentionally breaking or destroying computer hardware.
- In both cases, the system and the data stored were completely destroyed.
- Keep the PC in a secure area, lock the computer to a desk, do not eat near the computer, handle equipment with care, etc. can be countermeasures to this theft and vandalism.

Threats to Hardware

Natural Disasters

- Disaster may be natural and manmade.
- This disaster could result in a total loss.
- Natural disaster (flood, fire, and earthquake) is difficult to protect. Because natural disasters vary by location.
- User has to take preparation and have to be aware about the natural disaster.
- User can take steps to protect his/her computer from manmade disasters.

Threats to Data

Malware, Viruses and Malicious Programs

- The term malware describes viruses, worms, Trojan horses etc.
- These virulent programs represent the most common threat to user's information.
- Viruses are pieces of a computer program that attach themselves to host programs.
- Worms are particular to networks, spreading to other machines on any network you are connected to and carrying out preprogrammed attacks on the computers.
- Trojan horses, like their namesake, introduce malicious code under the guise of a useful program

Threats to Data

Cybercrime

- The use of a computer to carry out any conventional criminal act, such as fraud, is called cybercrime and is a growing menace.
- Cybercrime is growing so rapidly, in fact, that the federal government has created a handful of agencies to deal with computer related crimes.
- Hacking remains the most common form of cybercrime and it continues to grow in popularity.
- A hacker is someone who uses a computer and network or internet connection to intrude into another computer or system to perform an illegal act.
- At one time, a hacker was just a person who understood computers well; however, hacking now refers to criminal or antisocial activity.

Threats to Data

Cyber Terrorism

- Cyber warfare and cyber terrorism are new forms of warfare; they attack the critical information infrastructure of the nation.
- The conventional goal in the case of cyber terrorism is to harm or control key computer systems, or digital controls.
- It is done to accomplish an indicator aim such as to disrupt a power grid or telecommunications.
- Typical targets are power plants, nuclear facilities, water treatment plants, and government agencies.

Security Measures

The basic security measures for various threats are;

- Use Strong Passwords
- Use Password Manager
- Limit & Control Access to Critical Data
- Put Up a Firewall
- Use Security Software
- Update Programs and Systems Regularly
- Secure the Portable Devices
- Secure Wi-Fi Network
- Monitor for Intrusion
- Schedule Backups
- Be Smart with Emails and Surfing the Web
- Turn Off Computer and Disconnect from the Internet
- Raise Awareness

End of Chapter