Computer Security and Ethics

Tasmia
Jannat
Lecturer
Dept of CSE, RUET

Introduction

- **What is Ethics?**
  - Ethics refers to a set of moral principles that guide individual's/ group's behaviour.

- **What is Computer Ethics?**
  - Computer ethics are set of moral rules or guideline that regulates use of computer/ similar computing devices.

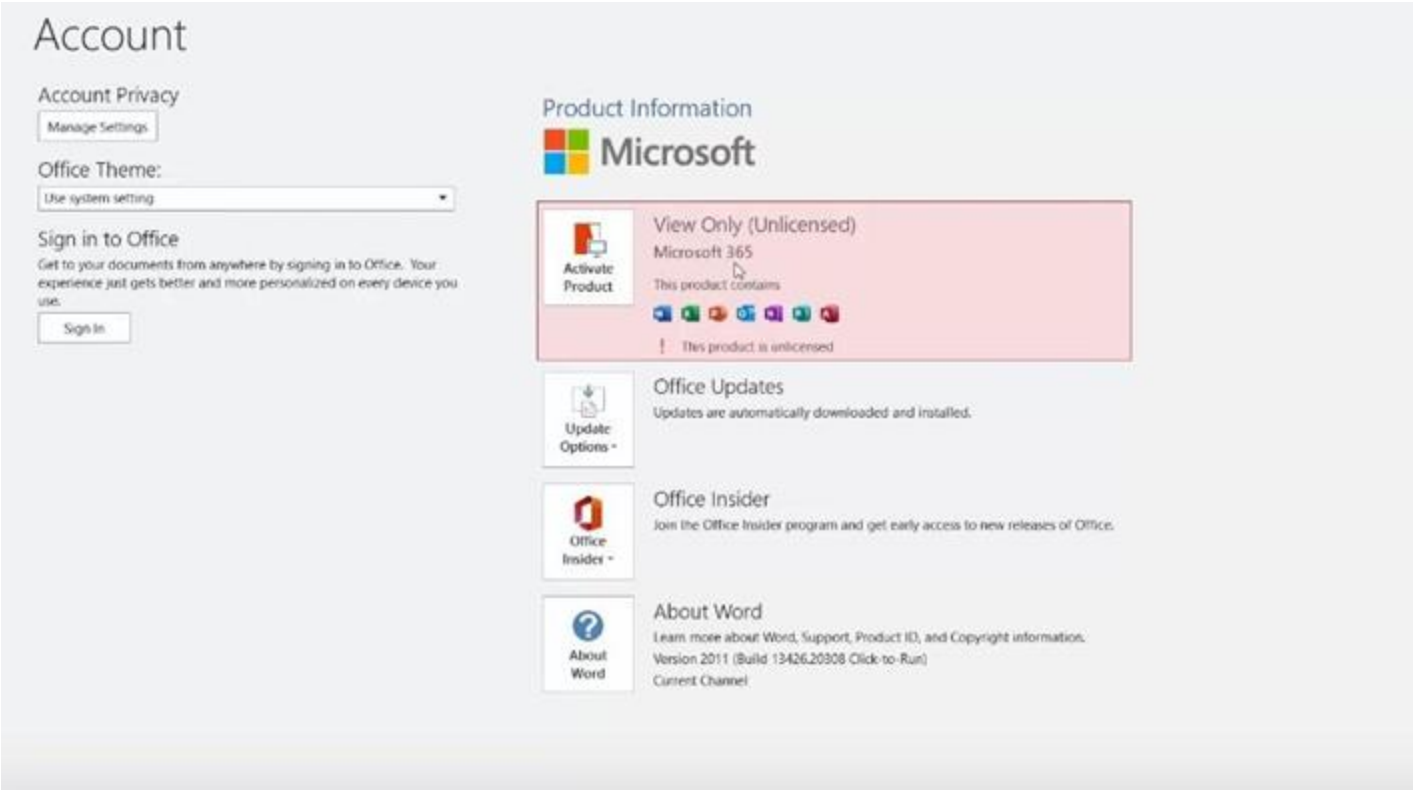
Common Terminology

❖ **Intellectual Property:**

Intellectual property is a category of property that includes comprehensible creations of the human intellect.

- **Copyright:** Copyright refers to the legal right of the owner of *intellectual* property. In simpler terms, copyright is the right to copy. This means that the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work. Some ways to ensure copyright:
  - **Copy guards** to prevent the duplication of works.
  - **DRM** (Digital Rights Management) to protect unauthorized redistribution of digital media. Like subscription in Netflix
  - **CPRM/CPPM (Content Protection for Recordable Media)** for controlling the copying, moving and deletion of digital media on a host device, such as a personal computer. It is a form of digital rights management (DRM)
  - **Activation** to require license registration before use.

Activation


Account
Account Privacy
Manage Settings
Office Theme:
Use system setting
Sign in to Office
Get to your documents from anywhere by signing in to Office. Your experience just gets better and more personalized on every device you use.
Sign In
Product Information
Microsoft
Activate Product
View Only (Unlicensed)
Microsoft 365
This product contains
This product is unlicensed
Update Options
Office Updates
Updates are automatically downloaded and installed.
Office Insider
Office Insider
Join the Office Insider program and get early access to new releases of Office.
About Word
About Word
Learn more about Word, Support, Product ID, and Copyright information.
Version 2011 (Build 13426.20308 Click-to-Run)
Current Channel

Common Terminology

- **Trademarks:** Trademarks usually refers to protection of the use of a company's name and its product names, brand identity (like logos) and slogans.

- **Difference between Copyright and Trademark:**
  Generally, copyrights protect creative or intellectual works, and trademarks apply to commercial names, phrases, and logos.

Common Terminology

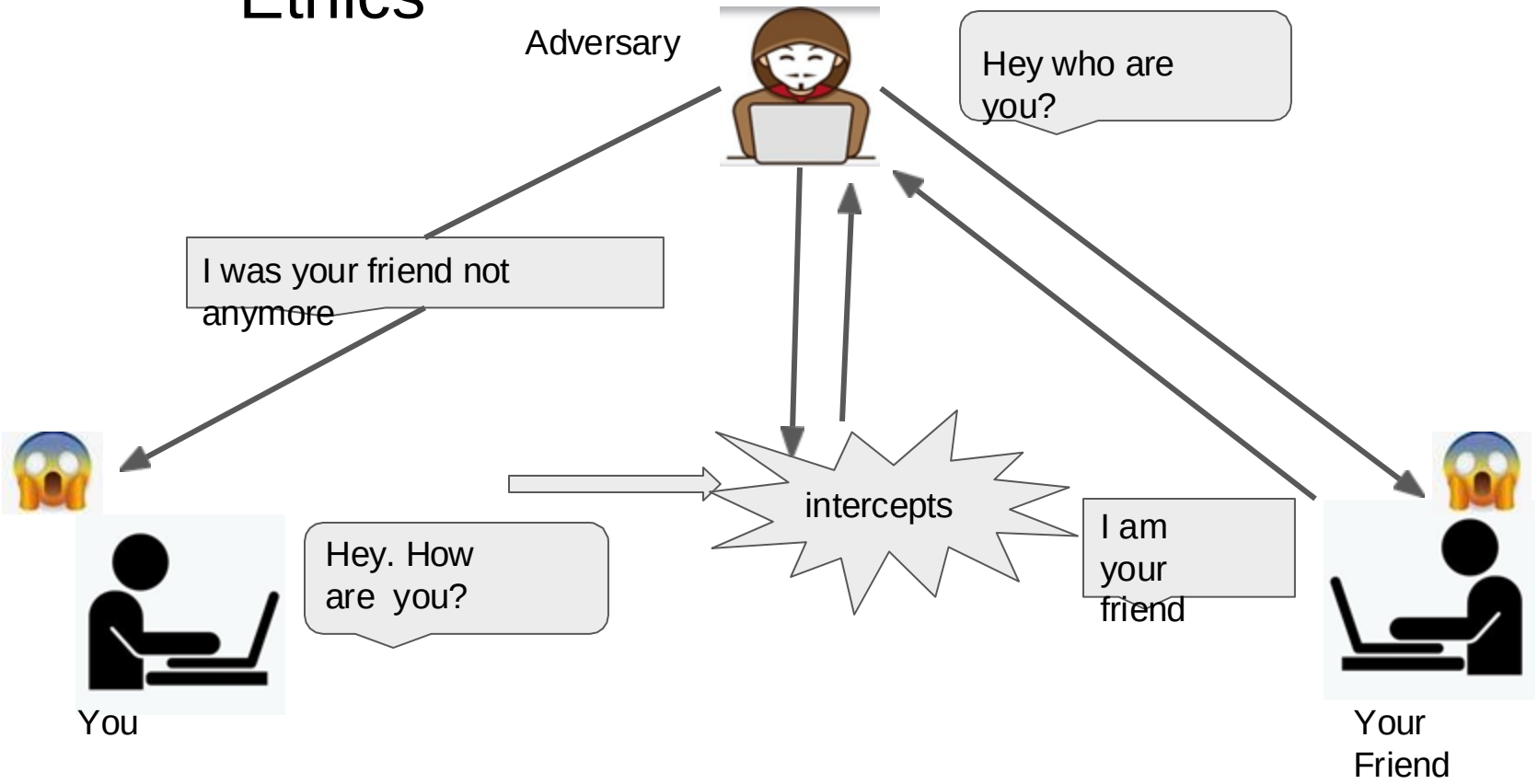
- **Patent:** A patent is the granting of a property right by a sovereign authority (Patent Office) to an inventor. This grant provides the inventor exclusive rights to the patented process, design, or invention for a designated period in exchange for a comprehensive disclosure of the invention.
- **License:**
  If a company wants to use any intellectual property for which they do not own a copyright or patent then they need to come up with a legal agreement with the owner of the intellectual property in form of a **license** that would allow them to use the intellectual property according to the agreement.

Common Terminology

Types of License:

- **Cross-licensing:** Agreement between two or more parties where each party grants rights to their intellectual property to the other parties
- **Patent pools:** Agreement between two or more **patent** owners to license one or more of their **patents** to one another or to third parties.
- **Licensing fees** are paid as part of an agreement that defines the terms under which tangible property is licensed for use by one party (a “licensor”) to another (the “licensee”).
- **Non-exclusive licenses:** A Non-Exclusive licence grants to the **licensee** the right to use the intellectual property, but means that the licensor remains free to exploit the same intellectual property and to allow any number of other licensees to also exploit the same intellectual property.
- **Exclusive license**: An exclusive Licence means that no person or company other than the named licensee can exploit the relevant intellectual property rights.

Common Violations of Computer Ethics



Common Violation of Computer Ethics

- **Intellectual Property Infringement**
  - **Copyright infringement:** Plagiarism, piracy, copying without consent/reference of the owner.
  - **Patent infringement:** Use of patented invention without permission from the patent holder
  - **Trademark infringement:** Copying the logo or motto of a business
- **Adversarial Attack on**
  - **Integrity**: Change/ manipulate original data.
  - **Authenticity**: Pretend to be the genuine source of data
  - **Confidentiality**: Exploit secrecy of data
  - **Availability**: Deprive of service.
- **Privacy Violation:** Violating any aspect of privacy can be referred to privacy violation. Like Hacking, Malware, **Anonymity** (keeping a user's identity masked through various applications)

Cybercrime

Cybercrime: Cybercrime is any type of illegal activity that takes place via digital means.

Targets of Cybercrime:

- Financial Data
- Intellectual Data
- Personal Data
- System Access
- Theft, Modification, Blackmail
- Modification, Sale
- Sabotage, Backdoor, Exploitation

Cyber Bullying : Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content.

Cyber Terrorism : Cyber Terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

Computer Security

- **Privacy:**
  Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. Privacy helps us establish boundaries to limit who has access to our personal property, places and things, as well as our communications and our information.

- **Privacy Aspects:**
  - **Right to be let alone:** Right to be immune from scrutiny or being observed in private settings, such as one's own home
  - **Limited access:** person's ability to participate in society without having other individuals and organizations collect information about them
  - **Control over information:** Rights to determine when, how, and to what extent information about oneself is to be communicated to others.

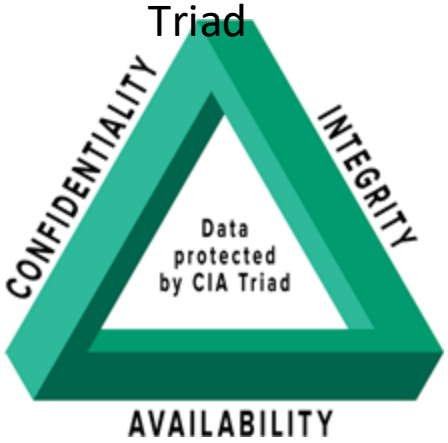
Common Terminology

Confidentiality: Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the authorized people who are allowed to do so can gain access to sensitive data.

Integrity: *Data integrity is the overall accuracy, completeness, and consistency of data.*

Availability: Data availability is about the timeliness and reliability of the access to and use of data. It includes data accessibility.

CIA Triad



Authenticity*: Data authenticity also means that a digital object is indeed what it claims to be.*

Adversary: An adversary is a malicious entity whose aim is to prevent the users of the from achieving privacy, integrity, and availability of data

Laws Concerning Cybercrime in Bangladesh

Although there might be some lackings in enforcement, Bangladesh Government has enacted adequate laws concerning cybercrime in Bangladesh which are:

- The Penal Code, 1860
- The Bangladesh Telecommunication Act, 2001 and
- Information and Communication Technology Act, 2006
- The Pornography Act, 2012
- The (Proposed) Cyber Security Act, 2015.

Different Cyber Crimes and Punishment

Cyber Crime	Definition / Mechanism	Punishment / Penalty	Technical and other measures
Phishing	**Phishing** is a type of social engineering attack where an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The main objective is to gather information	Section 54 (Not less than 7 years and more than 14 years or fine up to 1 crore Tk.)	● User awareness against phishing attacks. ● Verifying A Site's Security. Check url, site security certificate etc
Spoofing	**Spoofing** is an *identity theft* where malicious party impersonates another device or user on a network, in order to launch attacks	Section 54 (Not less than 7 years and more than 14 years or fine up to 1 crore	● Use an access control list ● Packet Filtering ● Use encrypted

Different Cyber Crimes and Punishment

Cyber Crime	Definition / Mechanism	Punishment / Penalty	Technical and other measures
Identity Theft	**Identity theft** is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases.	Section 54 (Not less than 7 years and more than 14 years or fine up to 1 crore Tk.)	● Safeguard your email id and password. ● Never share credit card information ● Be aware of phishing and spoofing
Cyber Stalking	Expressing or implying a physical threat/ harm that creates fear through the use to electronic medium.	Section 54, 55, 55 (Not less than 7 years and more than 14 years or fine up to 1 crore Tk.)	● Safeguard personal contact informations. ● Never share too many personal and family information. ● Avoid unknown person in social

Different Cyber Crimes and Punishment

Cyber Crime	Definition / Mechanism	Punishment / Penalty	Technical and other measures
Internet Time Theft	It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The unauthorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.	Section 54(1)(i) & 56 (Not less than 7 years and more than 14 years or fine up to 1 crore Tk.)	● Use strong password ● Check and block unidentified device in network
Planting Virus, Worms, Trojan etc	Expressing or implying a physical threat/ harm that creates fear through the use to electronic medium.	Section 54(1)(c) (Not less than 7 years and more than 14 years or fine up to 1 crore Tk.)	● Use strong antivirus ● Always enable firewall ● Never open suspicious executable file.

The people associated with computer crimes

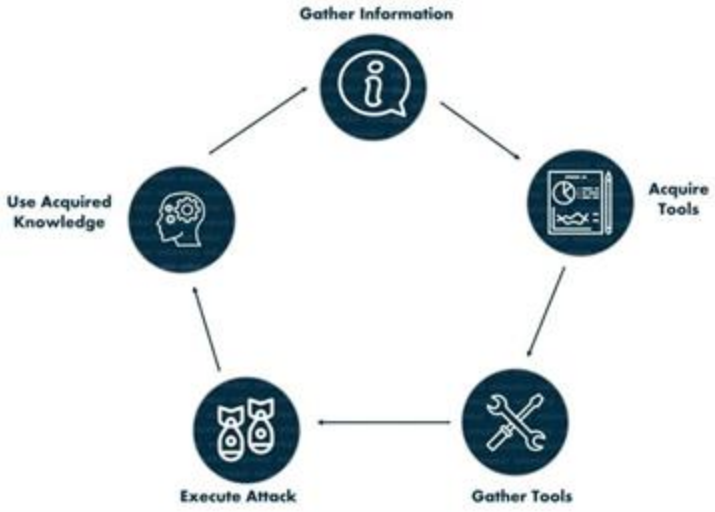
The people who are associated with computer crimes are often called **Hackers**, **Crackers**, **Virus programmers**, Breachers, Information Warriors, etc.

- A **Hacker** is a person who breaks into a computer system to get access to the information stored there. A hacker may not cause any harm to the system or organization, but hacking is still illegal and unethical.
- A **cracker** is a person who breaks into a computer system just like a hacker, with the intention to steal passwords, files, or programs for unauthorized use. They may sell this information to some other people for money. Crackers cause financial damage to an organization.
- **Virus programmers** are like crackers who breach the computer system, in order to steal information. They program dangerous viruses to get access to system. They cause harm to computer systems.

Ethical Hacking

In order to catch a hacker, one needs to have the mentality of a hacker, which is the fundamental of ethical hacking.

An ethical hacker serves as an organization by protecting their system and its information from illegal hackers as cyber-attacks and cyber terrorism is greatly growing.



Bug Bounty

Security flaws in software leave them open for attackers to exploit vulnerabilities and bypass security defenses. This is where the Bug Bounty programs come in. A bug bounty program is when an organization will pay a ransom to third-party security researchers when they find software security flaws that meet certain conditions in the software or on their sites, apps, or services.

Cybercrime Detection Techniques

- Auditing log file
- Firewall logs and reports
- Tracing domain name/IP addresses
- Spoof detection software

Malware

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

Common property of malware:

- **Permanence**: Some malware can affect more permanent system component such as master boot record. In that case, even if a computer is formatted the infected application or program can be still on a backup disk, thus virus can easily re-infect the computer.
- **Transmissible:** malware can be small software programs which can carry other similar malware, thereby making the malware dangerous.

Malware

- **Replication:** Replication is where a malware reproduces or duplicates itself to insure it has a method of spreading.
- **Stealth**: The stealth malware first attaches itself to files on the computer and then attacks the computer.
- **Memory or non memory resident:** A malware can be either memory resident where the malware is first loaded into memory and infects a computer subsequently or *non memory resident where the malware code runs each time a file is opened.*
- **Polymorphic**: Some malware have an ability to change their code. This means a malware can carry several amounts of similar variants.

Malware

- **Computer Virus:** A computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

- **Computer Worm:** Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.

Malware

- **Trojan:** It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses).

Malware

- **Ransomware:** Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

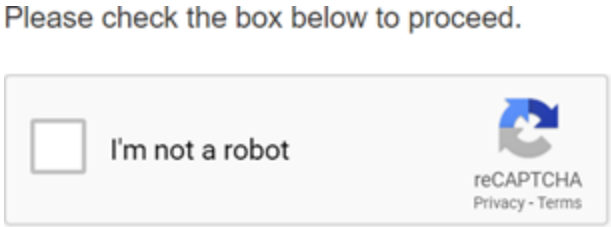
- **Spyware:** Cybercriminals use spyware to monitor the activities of users. By logging the keystrokes a user inputs throughout the day, the malware can provide access to user names, passwords, and personal data. Much like other malware, antivirus software can help you detect and eliminate spyware.

Malware

- **Bots :**

  A bot is a software program that performs an automated task without requiring any interaction. A computer with a bot infection can spread the bot to other devices, creating a botnet.

  One way to control bots is to use tools that help determine if traffic is coming from a human user or a bot. For example, you can add CAPTCHAs to your forms to prevent bots from overwhelming your site with requests. This can help you identify and separate good traffic from bad.



Personal Safety Steps

1. Change passwords regularly.
2. Keep log-in information secret. Always log off from your computer or your online accounts.
3. Install an updated anti-virus and fire-wall software.
4. Password protect your computer.
5. Do not share personal information, files, or computer access to strangers.
6. Do not leave your computer or devices unattended.
7. Avoid using the “auto-fill” function for online accounts and forms.
8. Use a primary email and secondary email.
9. Beware of online scams — never accept free gifts online.
10. Be wary of unexpected emails with attachments.
11. *Be mindful of which website URLs you visit*
12. Do a spyware scan often.
13. Invest in data backup (e.g. external drive or server).


Facebook - Log In or Sin
Secure | https://www.facebook.com
facebook
Facebook helps you connect and share with t
people in your life.
Real


Facebook - Log In or Sin
https://www.facebouk.com
facebook
Facebook helps you connect and shar
people in your life.
Fake