PRIVACY, SECURITY AND ETHICS

Chapter 9

CHAPTER 9

PRIVACY **SECURITY** **ETHICS**

LEARNING OBJECTIVES

1. Identify the most significant concerns for effective implementation of computer technology.
2. Discuss the primary privacy issues of **accuracy**, **property**, and **access**.
3. Describe the impact of large **databases**, **private networks**, the **Internet**, and the **Web** on privacy.
4. Discuss online identity and major laws on privacy.
5. Discuss cybercrimes including creation of malicious programs such as viruses, worms, Trojan horse, and zombies as well as denial of service

attacks, Internet scams, identity theft, cyberbullying, rogue Wi-Fi

hotspots, and data manipulation.

6. Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
7. Discuss computer ethics including copyright law, software piracy, digital rights management, the Digital Millennium Copyright Act, as well as

plagiarism and ways to identify plagiarism.

INTRODUCTION

- A lot of users nowadays using technology as their daily life tasks.
- The use of personal data and our right to privacy.
- This chapter covers issues related to the impact of technology on people and how to protect ourselves on the Web.

Technology has had a very **positive** impact on people, but some of the impact could be **negative**.

What we need to be concern?

- **Privacy** – What are the threats to personal privacy and how can we protect ourselves?
- **Security** – How can access to sensitive information be controlled and how can we secure hardware and software?
- **Ethics** – How do the actions of individual users and companies affect society?

PRIVACY

- Privacy – concerns the collection and use of data about individuals
- Three primary privacy issues:

1. **Accuracy** – responsibility of those who collect data

   Must be secure and correct
2. **Property** – who owns data and who has rights to software
3. **Access** – responsibility of those who control data and use of data

LARGE DATABASE

◦ Did you know……

- Large organizations compile information about us daily
- Big Data is exploding and ever-growing

90% of the data collected has been collected over the last 2 years

- Data collectors include : -

. Government agencies
. Telephone companies
. Credit card companies
. Supermarket scanners
. Financial institutions
. Search engines
. Social networking sites
. **Information Reseller/Brokers**
    1.Collect and sell personal data
    2. Create electronic profile

Actually……

- **Personal Information** is a marketable commodity which raises many issue :

- Spreading Information without personal consent , leading to identity theft
- Spreading inaccurate information

- **Freedom of information Act**

- Entitlement to look at your records held by government agencies

What is private network?

- Private network is a computer network that uses private IP addresses space.
- E.g.: Employee Monitoring Software

  - Employee Monitoring Software is a technology that allows employers to gain valuable insight into employee's computer activities in the work space .

  -A proposed law could prohibit this type of electronic monitoring or get permission from the employee first.

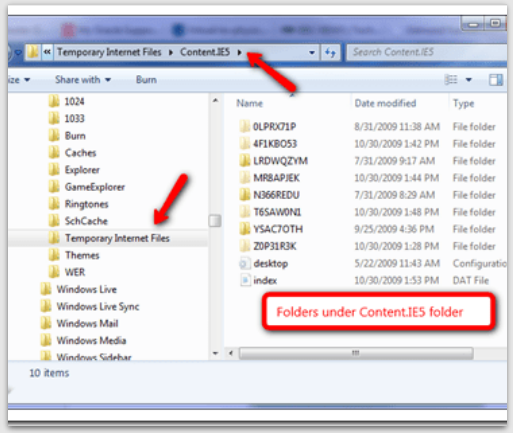
Illusion of anonymity

- Many people believe that, while using the web, little can be done to invade their privacy. This is the illusion of anonymity.
- In fact, while browsing the web, critical information stored in hard drive
  - History file
  - Temporary Internet file
  - Cookies
  - Privacy mode
  - Spyware (Privacy threats)

History File

All the location and addresses of sites that you have recently visited

Temporary internet files



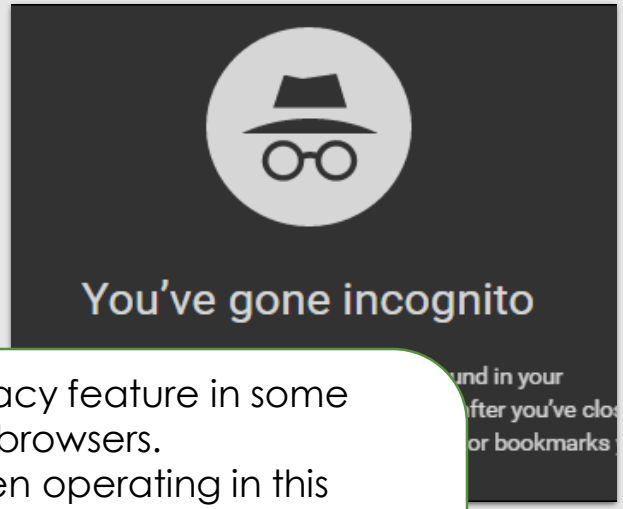
- known as browser cache is a folder on Microsoft window which save file from visited websites.

- This will allow such websites load more quickly for the next time they visited.

Spyware

- Unwanted software that infiltrate your computer device, steal internet usage and sensitive information.
- Wide range of programs that are designed to secretly record and report Internet activities, add Internet ad cookies.

Privacy mode



- Privacy feature in some web browsers.
- When operating in this mode, your browsing activity are not recorded in your hard drive.
- Eg: Incognito mode in Google Chrome and Safari on iPhone.

Cookies

-Cookies are small data files that deposited on your hard disk from the websites you have visited.
- 2 types of cookies is
* **Traditional cookies**
* **Ad network cookies**

- **Traditional cookies**: Provide info to a single site, a cookie is deposited with the information that identifies specifically.
- **Ad network cookies** (Adware cookies): Third party tracking cookies that stored in user's computer without their knowledge or record your activities across different sites.

PRIVACY THREATS

Web bugs

- Used by 3rd parties to monitor the activity of users at a website.
- Invisible images or HTML code hidden within an email message or web page.

Spyware

- Unwanted software that infiltrate your computer device, steal internet usage and sensitive information.
- Wide range of programs that are designed to secretly record and report Internet activities, add Internet ad cookies.

Computer Monitoring Software (Keystroke Logger)

- Invasive and dangerous
- Watches what you do

PRIVACY THREATS

Anti-Spyware Program

- Detect web bugs and monitoring software
- Detect files and remove privacy threats

ONLINE IDENTITY

- The information that people volunteering post about themselves online.

Major Law of privacy

E.g. : - Gramm-Leach-Bliley Act: Protects personal financial information

- Health Insurance Portability and Accountability Act (HIPAA): Protects medical records
- Family Educational Rights and Privacy Act (FERPA): Resists disclosure of educational records

SECURITY

What is security?

- The protection of computer systems and information from harm, theft, and unauthorized use

Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment, namely, serial numbers, doors and locks, and alarms

- We need to protect from:
    1. **Hacker**
    2. **Cybercrime**

HACKER

- a person who uses computers to gain unauthorized access to data

  Gain unauthorized access with malicious intent

- Not all hackers are illegal

CYBERCRIME

- Criminal offense that involves a computer and a network
- Effects over 400 million people annually

EXAMPLES OF CYBERCRIME

•**Malicious Programs or Malware** -Designed by crackers, computer criminals, to damage or disrupt a computer system

3 examples :

1.Virus 

2. Worm 

3. Trojan horse 

•**Denial of service** - attack attempts to slow down or stop a computer system or network by flooding it with requests for information or data

•**Rogue wi-fi or hotspot** - Imitate free Wi-Fi networks and capture any and all information sent by the users to legitimate sites including usernames and passwords

•**Data manipulation** -Finding entry into someone's computer network and leaving a prankster's message

•**Internets scams** -A fraudulent or deceptive act or operation to trick someone into providing personal information or spending money for little or no return

•**Cyber bullying-** Use of the Internet, cell phones, or other devices to send or post content intended to harm

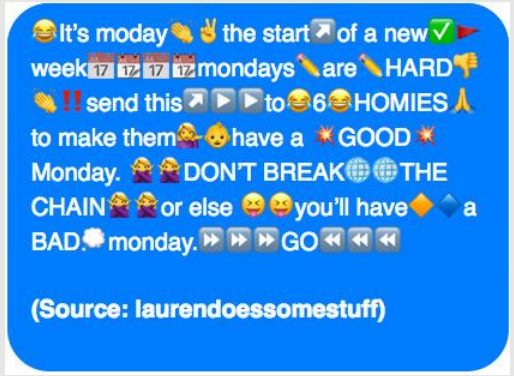
EXAMPLES OF INTERNET SCAMS

1.**Chain letter** – An unsolicited e-mail containing false information for the purpose of scaring, intimidating, or deceiving the recipient

2.**Auction fraud** – Payment is sent but merchandise not delivered

3.**Vacation prize** - "Free" vacation voucher is given but when arrive, they need to pay

4.**Advance free loan** – Give free loan but actually need to pay back



MEASURES TO PROTECT COMPUTER SECURITY

RESTRICTING ACCESS

- Limit access

1.Biometric scanning
- •Fingerprint/iris scanner

2.Passwords
- -but must aware of dictionary attack

AUTOMATED SECURITY TASK

- Ways to perform and automate important security tasks
- •**Password Managers** - Helps to create strong passwords
- •**Security Suites** - Provide a collection of utility programs designed to protect your privacy and security
- •**Firewalls** - Security buffer between a corporation's provide network and all external network

ENCRYPTING DATA

- Coding information to make it unreadable, except to those who have the encryption key

1.**E-mail encryption** protects emails
2.**File encryption** protects files
3.**Web site encryption** uses HTTPS protocol
4.Virtual private networks (**VPNs**)
5.**Wireless** network encryption restricts access to authorized users
-WPA

ANTICIPATING ACCESS

-prepare for disaster
1.**Physical Security** protects hardware
2.**Data Security** protects software and data from unauthorized tampering or damage
3.**Disaster Recovery** Plan describes ways to continue operating in the event of a disaster

PREVENTING DATA LOSS

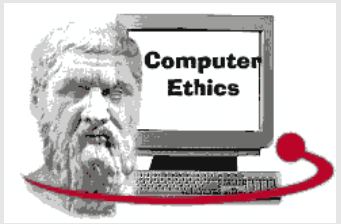
-routinely copy data and store it in a remote storage
- •Redundant data storage - Store off-site in case of loss of equipment
- •Cloud-based backup services such as Carbonite provide cloud based backup services

ETHICS

- What is Ethics?

  - Ethics is standard moral conduct

  - But for computer Ethics , it is a guidelines for morally acceptable use of computers



Example of unmorally use of computer :-

➢ **Copyright**

- Gives content creator the right to control the use of their work
- 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.
- Painting , books, music and films

➢ **Software Piracy**

- Unauthorized copying and distribution of software

  - Digital right management (**DRM**) control access to electronic media

  - Digital Millennium Copyright Act protect against piracy

➢ **Plagiarism**

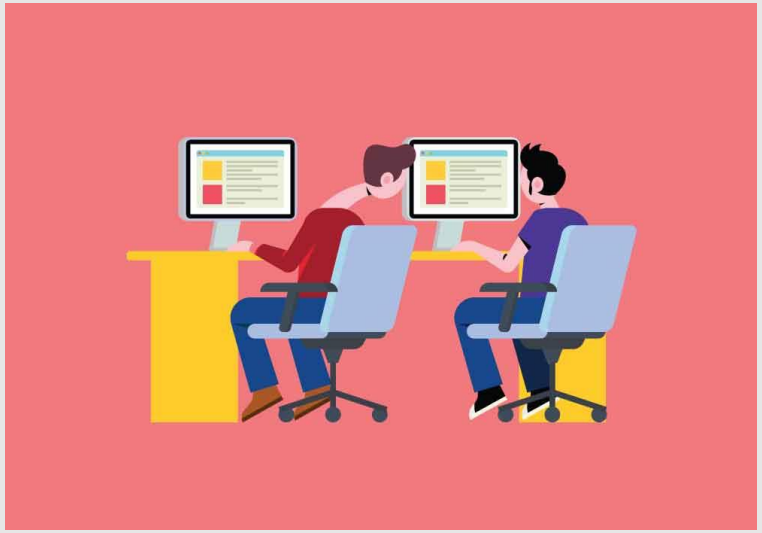
- Representing some other person's work and ideas as your own without giving credit to the original person's work and ideas

<u>Ways to prevent from plagiarism</u>

1. Give unique task

   - tasks that require a creative and individual approach

2. Use plagiarism checkers



THANK YOU

- - LAI LENG SHUEN (Clan Leader)
- - MUHAMMAD SHAWALUDDIN BIN SHAARI (Co-Leaders)
- - MUHAMMAD FADTHUN AMIERRUN BIN MD NORAZAM (Co-Leaders)
- - MUHAMMAD FAKHRULLAH BIN KAMAL BAHRIN (Co-Leaders)