PHENIKAA UNIVERSITY

Faculty of Computer Science

Introduction to Computing

Lecture 8: Social and Ethical Issues

Objective

- After studying this chapter, the student should be able to:
  - Define three ethical principles related to the use of computers.
  - Distinguish between physical and intellectual property and list some types of intellectual property.
  - Define privacy as related to the use of computers.
  - Give the definition of a computer crime and discuss types of attacks, motivation for attacks, and how to protect against attacks.
  - Define hackers and the damage done by them.

Ethical Principles (Code of Ethics)

- 1st principle: Moral rules
  - We should avoid doing anything if it is against universal morality
- 2nd principle: Utilization
  - An act is ethical if it brings about a good result
- 3rd principle: Social contract
  - An act is ethical if a majority of people in society agree with it

Intellectual Property

- Physical property: A person owns a physical object
- Intellectual property: The right of owning intellectual things
    - An author should be given the right to benefit from his/her written book
    - An artist should be given the right to benefit from his/her artwork.

Types of Intellectual Property

- Trademarks
  - A trademark identifies a company’s product or service.
- Trade secrets
  - A trade secret is the information about a product that is kept secret by the owner.
- Patents
  - A patent is a right to a monopoly to use and commercially exploit a piece of intellectual property for a limited period of time.
- Copyright
  - A copyright is a right to a written or created work.

Privacy

- Protecting personal information
  - Personal information is collected by private and public agencies
- Codes of ethics related with collecting personal data (in some countries)
  - Collect only data that are needed.
  - Be sure that the collected data are accurate.
  - Allow individuals to know what data have been collected.
  - Allow individuals to correct the collected data if necessary.
  - Be sure that collected data are used only for the original purpose.
  - Use encryption techniques to accomplish private communication.

Computer Crimes

- A computer crime is an illegal act, called an attack, involving any of the following:
  - A computer
  - A computer network
  - A computer-related device
  - Software
  - Data stored in a computer
  - Documentation related to the use of computers

Computer Crimes – Types of Attacks

- ❖ Penetration attack: Break into a system to get access to the data stored in a computer or in a computer network
  - ○ Viruses: unwanted programs that are hidden within other programs (host)
  - ○ Worms: an independent program which can copy itself and which travels through the network.
  - ○ Trojan horses: a computer program that does perform a legitimate task, but which also contains code to carry out malicious attacks such as deleting or corrupting files.
- ❖ Denial of service attack (DoS):
  - ○ Reducing the capability of a computer system to function correctly or bring the system down altogether by exhausting its resources.
- ❖ Motives: terrorism, espionage (gián điệp), financial gain, or hate.

Computer Crimes – Attact protection

- ❖ Physical protection
  - ○ The computer can be physically protected to allow physical access only to trusted individuals.
- ❖ Use protective software
  - ○ Software can be used to protect your data, such as data encryption or the use of strong passwords to access the software.
- ❖ Use strong anti-virus software
  - ○ Strong anti-virus software can control access to the computer when installing new software or accessing Internet sites.

Computer Crimes – Attact protection

- ❖ Preventing Crime on the Internet
  - ○ Develop effective Internet and security policies
  - ○ Use a stand-alone firewall with network monitoring capabilities
  - ○ Monitor managers and employees
  - ○ Use Internet security specialists to perform audits

Hackers

- Hacker (in the past)
  - A person with a lot of knowledge who could improve a system and increase its capability.
- Hacker (today)
  - Someone who gains unauthorized access to a computer belonging to someone else in order to copy secret information.
- Most countries impose heavy penalties for both harmless and harmful hacking
  - Accessing government computers without authorization is a crime
  - Heavy punishment for hackers who access the computers of private institutions, and the simple act of obtaining information from somebody else’s computer is a crime, whether the information is used or not.

Reading Materials

❖ All students in computing fields should read, understand and apply the ACM Code of Ethics and Professional Conduct:

- Code of ethics: https://www.acm.org/code-of-ethics#h-2.-professional-responsibilities.
- Professional Responsibilities: https://www.acm.org/code-of-ethics - h-2.-professional-responsibilities.
- Professional Leadership Principles: https://www.acm.org/code-of-ethics#h-3.-professional-leadership-principles.
- Details in the “Social_Ethical_Risk_Impacts.pdf” file
- Social and Ethical Case Studies

PHENIKAA UNIVERSITY

Faculty of Computer Science

Q & A