Privacy, Crime, and Security

IT Foundation Report 8

By: Mustafa Jalal Fteita

Contents:

1- Define and list Cypercrimes

2- Define and list computer crimes.

3- List computer criminals.

4- Describe computer security risks.

5- Discuss how computer development effects privacy and anonymity.

6- Discuss how to protect your computer and yourself.

7- Define encryption and how to secure your Information.

8- Discuss the issues that faces governmental and legal agencies to decrypt information.

9- Distinguish the diffrence between electronic Discovery and computer forensics.

Cypercrimes:

- **Cybercrime:** describes crimes carried out by means of the Internet.

Types of Cybercrime:

- Identity theft
- Blackmail
- Cyberstalking
- Cyberbullying
- shilling
- Rip and tear
- Pump and-dump
- Bogus goods

Computer crimes:

- **Computer crimes**: computer-based activities that violate state, federal, or international laws.

Types of Computer crimes:
- Unauthorized access.
- Malware: including “spyware and viruses”.
- Rogue programs: such as “time bombs, logic bombs, worms, and Trojan horses”.
- Fraud and theft (password theft)

Computer criminals:

- **Computer criminals**: people who can cause security problems, ranging from pranksters to hardened criminals.

Types of Computer crimes:
- Hackers.
- Crackers.
- cybergangs.
- Virus authors.
- Swindlers.
- Shills.
- cyberstalkers.
- cyberbullies.
- Sexual predators.

Security risks:

- **Computer security risk:** is any event, action, or situation that could lead to the loss or destruction of computer systems or the data they contain.

- **Wireless Networks:** Wireless LANs pose challenges to security, especially hotspots that are designed for open access.
To break into a wireless network you must be within the proximity limits of the wireless signal. It is fairly easy to break into an unsecured wireless network and obtain confidential information.

- **Corporate espionage:** the unauthorized access of corporate information, usually to the benefit of a competitor.
The perpetrators are often ex-employees who have been hired by a competing firm precisely because of their knowledge of the computer system at their previous place of employment.

- **Information Warfare:** The use of information technologies to destroy an enemy's information ,or hacking the network infrastructure, including the electronic banking system) and structural sabotage (attacks on computer systems that support transportation, finance, energy, and telecommunications).

Technology development affection to privacy & anonymity:

Marketing firms, snoops, and government officials can use computers and the Internet to collect information in ways that are hidden from users. The same technology also makes it increasingly difficult for citizens to engage in anonymous speech.

- **Anonymity:** refers to the ability to convey a message without disclosing your name or identity.

Examples of technologies that threaten online anonymity include:

- **Cookies:** small text files that are written to your computer's hard disk by many of the Web sites you visit.

- **Global unique identifiers (GUID):** an identification number that is generated by a hardware component or a program.

- **Ubiquitous computing:** a trend in which individuals no longer interact with one computer at a time but instead with multiple devices connected through an omnipresent network, enabling technology to become virtually embedded and invisible in our lives.

- **Radio frequency identification:** The use of radio waves to track a chip or tag placed in or on an object is referred to as radio frequency identification (RFID).

Protecting your computer:

- **Power-Related Problems:** Power surges, which are often caused by lightning storms or fluctuations in electrical currents, and power outages can destroy sensitive electronic components and carry the threat of data loss. You can also equip your system with an **uninterruptible power supply (UPS),** a battery-powered device that provides power to your computer for a limited time when it detects an outage or critical voltage drop.

- **Controlling Access:** The most secure authentication approach is biometric authentication, the use of a physical trait or behavioral characteristic to identify an individual, For example, Gateway now offers a built-in biometric fingerprint sensor on its latest notebook that locks access to the computer unless the correct fingerprint is matched.

- **Firewall:** a computer program or device that permits an organization’s internal computer users to access the external Internet but severely limits the ability of outsiders to access internal data.

Protecting yourself:

It is important to protect your personal data from theft and yourself from a cyberattack.

- **Avoiding Scams:** To avoid being scammed on the Internet, follow these tips:
• Do business with established companies that you know and trust.
• Read the fine print. If you're ordering something, make sure it's in stock and that the company promises to deliver within 30 days.
• Don't provide financial or other personal information or passwords to anyone, even if the request sounds legitimate.
• Be skeptical when somebody in an Internet chat room tells you about a great new company or stock.

- **Preventing Cyberstalking:** To protect yourself against cyberstalking, follow these tips:
• Don't share any personal information, such as your real name, in chat rooms. Use a name that is gender- and ageneutral. Do not post a user profile.
• Be extremely cautious about meeting anyone you've contacted online. If you do, meet in a public place and bring friends along.
• If a situation you've encountered online makes you uncomfortable or afraid, contact the police immediately. Save all the communications you've received.

Encryption & how to secure your information:

- **Encryption:** refers to a coding or scrambling process that renders a message unreadable by anyone except the intended recipient.
This process guarantees that a message is unreadable by anyone except the intended recipient, who possesses the key to decode the encoded message.

Electronic discovery & computer forensics:

- **Electronic discovery:** is the obligation of parties to a lawsuit to exchange documents that exist only in electronic form, including e-mails, voicemails, instant messages, e-calendars, audio files, data on handheld devices, animation, metadata, graphics, photographs, spreadsheets, Web sites, drawings, and other types of digital data.

- **Computer forensics:** a branch of forensic science, examines hardware and software to detect cybercrime.

Issues that faces governmental and legal agencies to decrypt information:

The U.S. government continues to look for ways to balance the government's need to know with the public's right to privacy.

The government recently released a new
random-number standard: a critical component of encryption methods.

However, a backdoor was discovered that could enable someone to crack the code, compromising the security of this encryption and obtaining confidential information.
The U.S. government understands the importance of encryption and the need to collect information, but within the limits of retaining the privacy of its citizens.

a basic human rights declaration gives all citizens the following privacy rights:
- Consumers must be informed of exactly what information is being collected and how it will be used.
- Consumers must be allowed to choose whether they want to divulge the requested information and how collected information will be used.
- Consumers must be allowed to request that information about themselves be removed from marketing and other databases.

Resource:
Computers are your future
by: Catherine LaBerta
Chapter 9: Privacy, Crime,
and Security

Thank you for Watching!

By: Mustafa Jalal Fteita