Computer crimes

[Mohamed jowjary]

objectives

List types of computer crime and cybercrime.

List types of computer criminals.

Discuss how technology develops effect , privacy and anonymity.

Discuss security risks of using computer.

Describe how to protect your computer ,yourself

Define encryption and explain how it moves online information secure

Describe the issues the government face when balancing the weed for describing data and the public right to privacy

Distinguish between electronic discovery and computer forensics

Q1- List types of computer crime and cybercrime.

Examples of computer crime and cybercrime include

- identity theft
- malware
- including spyware
- viruses
- worms - Botnets - zombies - Trojan horses
- other rogue programs such as time bombs, logic bombs
- fraud theft and piracy - password theft
- salami shaving and data diddling forgery - blackmail
- cyberstalking and cyberbullying
- Internet crimes like shilling, rip and tear, pump and dump, and bogus goods

Q2List types of computer criminals

These actions are performed by computer criminals that include

- hackers
- crackers
- cyber gangs
- virus authors
- swindlers
- shills
- cyber stalkers
- cyberbullies
- sexual predators

Q3 Discuss how technology develops affect privacy and anonymity.

Technologies that jeopardize online anonymity include :

1-Cookies

2-Globally Unique Identifier

3-Ubiquitous Computing

4-Radio Frequency Identification

cookies are small text files that are written to your computer's hard disk by many of the Web sites you visit, they can

- Track your browsing habits
- Gather personal information without your consent
- Can be disabled

A globally unique identifier (GUID) is an identification number produced by software or a piece of hardware .

- Web serves can read the GUID
- Users are not always aware of the GUID
- If used companies allow users to opt out
- Civil liberties groups and public concern have decreased the use of GUIDS

Interacting with multiple networked devices is called **Ubiquitous Computing**

- An example is the adjustment of heat or light in an environment based om signals sent by monitors built into clothing
- An **active badge** can transmit infrared signals to create an electronic
- Current devices such as smartphones hold private information that can be exploited if the device is lost or stolen

Radio Frequency Identification

The use of radio waves to track a chip or tag

- Used for inventory control in stores
- Recognizes microchip in pets
- May compromise anonymity and privacy if information stored on RFID tags attached to U.S passport is misused

Q4 Discuss security risks of using computer

• A computer security risk is any event, action, or situation—intentional or not—that could lead to the loss or destruction of computer systems or the data they contain.

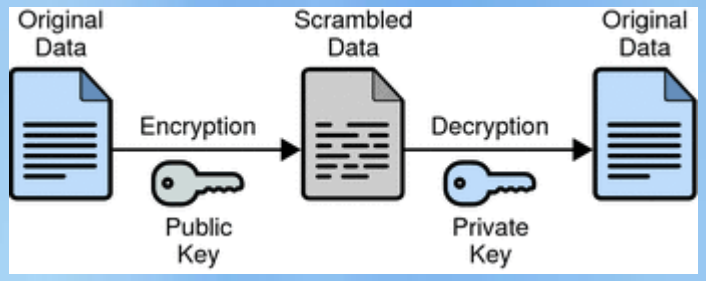
Q5 Describe how to protect your computer and yourself

No computer system is totally secure, but you can do several things to cut down on security risks

Safe surfing guides should always be followed in addition to utilizing some software and hardware deterrents, including an uninterruptible power supply (UPS), strong passwords, know-and have authentication, biometric authentication, encryption of sensitive data, and an installed firewall

Q6 Define encryption and explain how it moves online information secure

Encryption, essential for e-commerce and online banking, makes use of encryption keys to encode and decode information traveling over a network. This process guarantees that a message is unreadable by anyone except the intended recipient, who possesses the key to decode the encoded message



Q7 Describe the issues the government face when balancing the need for describing data and the public right to privacy

- 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

Q8 Distinguish between electronic discovery and computer forensics

- Electronic discovery is the exchange of electronic Documents.

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

Both facilitate the detection,
Apprehension and conviction of cybercriminals

http://portal.limu.edu.ly/pluginfile.php/22664/mod_resource/content/1/Computers%20Are%20Your%20Future

THANK YOU