COMPUTER CRIME

1/LIST TYPES OF CRIME

Unauthorized access

malware, including spyware and viruses

rogue programs such as time bombs, logic bombs, worms, and Trojan horses

fraud and theft (password theft)

2/LIST TYPES OF COMPUTER CRIMINALS

Hackers : ethical hackers, or white hats + grey hats

Crackers: (black hats) are hackers who become obsessed (often uncontrollably) with gaining entry to highly secure computer systems. Their intent, however, is to destroy data, steal information, or perform other malicious acts

Cyber-gangs: groups of hackers or crackers working together to coordinate attacks, post online graffiti, or engage in other malicious conduct.

Virus authors

Swindlers

Shills

Cyber-stalkers

Cyber-bullies

3/THE EFFECT OF DEVELOPS ON PRIVACY ANONYMITY

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)

4/ UNDERSTAND COMPUTERS SECURITY RISKS OF USING COMPUTER AND THE INTERNET

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.

Vacation hacking : who create phony Wi-Fi hot spots, called evil twins, users believe they are legitimately connected to the airport, hotel, or airline. Unlike they're signing onto a fraudulent network. The information being entered is being captured by criminals.

Corporate Espionage: The unauthorized access of corporate information, usually to the benefit of 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).

5/DISTINGUISH BETWEEN E-DISCOVERY AND COMPUTER FORENSICS

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

Electronic discovery is the electronic aspect of identifying, collecting and producing electronically stored information in response to a request for production in a law suit or investigation.

6/DESCRIBE HOW TO PROTECT YOUR COMPUTER AND YOURSELF

Do not leave a secured account active on the monitor and walk away.

Create strong logins and passwords for each individual who uses a system. This provides each user with a section to store documents that no other user can see or utilize when logged in. A strong password should:

- Be difficult to guess.
- Be at least 14 characters or more in

length.

- Include uppercase letters, lowercase

letters, numbers, and special

characters.

- Not be a recognizable word or phrase.

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.

To protect yourself against cyberstalking, follow these tips:

- Don’t share any personal information, such as your real name, in chat rooms. Also, 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.

7/DESCRIBE THE ISSUES THE GOVERNMENT FACE WHEN BALANCING THE NEED FOR DECRYPTING DATA AND THE PUBLIC RIGHT TO PRIVACY

Privacy advocates agree that the key lies in giving citizens the right to be informed when personal information is being collected as well as the right to refuse to provide this information. In the European Union (EU), 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.

Protecting the privacy rights of U.S. citizens has been a controversial area for years. Most of us agree that our rights should be protected, but our definition of acceptable levels of protection varies widely.

8/DEFINE ENCRYPTING AND EXPLAIN HOW TO SECURE YOUR ONLINE INFORMATION

Encryption: refers to a coding or scrambling process that renders a message unreadable by anyone except the intended recipient. Until recently, encryption was used only by intelligence services, banks, and the military.

public key encryption (asymmetric key encryption) is a computer security process in which two different keys an encryption key (the public key) and a decryption key (the private key)—are used. The use of two different keys safeguards data and thus provides confidentiality. Additionally it allows a digital signature to be decoded or verified only by individuals that a have access to the sender’s public key, thereby proving that the sender is authentic and has access to the private key. The way it works is that people who want to receive secret messages publish their public key, for example, by placing it on a Web page or sending it to those with whom they wish to communicate. When the public key is used to encrypt a message, the message becomes unreadable. The message becomes readable only when the recipient applies his or her private key