1- list type of crime and cybercrime ?

Types of cybercrime

- Identity theft
- blackmail; cyber-stalking and cyber-bullying
- Internet crimes like:
- shilling: ebay
- rip and tear: The action of accepting payment for goods that you have no intention of delivering.
- pump and dump: The use of Internet stock trading sites, chat rooms, and e-mail to sing false praises of worthless companies in which an individual holds stock. Once the false hype drives up the share prices, that individual makes a hefty profit.
- bogus goods: The deliberate selling of goods that do not perform the advertised function.

Types of computer 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 criminal ?

- Identity Thieves.
- Internet Stalkers.
- Phishing Scammers.
- **Cyber** Terrorists .

3- the effect of technology develops on privacy and 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 ?

Data encryption translates data into anotherform, or code, so that only people with access toa secret key (formally called a decryption key) orpassword can read it.

Encrypted data iscommonly referred to as ciphertext, whileunencrypted data is called plaintext.

There are steps to secure your onlineinformation:

1-Avoid clicking on links or attachments:

Cybercriminals do a good job of tricking people intoclicking on links supposedly from their bank, telecomoperator, electric or gas company, tax service and otherlegitimate organisations.

2- Think before you click-spelling errors, email addresses that don't seem right,Passwords are the keys to your digital kingdom:Use unique, complex passwords with a combination oflower and upper-case letters, numbers and symbols anddo not use the same password across your accounts.

3-Keep your identity safe:

Don't share passwords or choose one that can be easilyguessed. Make sure to change them often.

And wherepossible, use two-factor or strong authentication whichcombines something you know.

4-Back-up your data:

If your computer is infected by ransomware, malware orit crashes, the only way to definitely ensure that you willbe able to retrieve your lost data is by backing it up anddoing so on a regular basis.

5-Verify the web site you are on is safe:

before entering your payment details into any web site,check that the URL begins with https the "s" stands for"secure.

Reference :-

Computers are your future 12th edition by : Catherine LaBerta

BY : Osama Mohamed (3011)