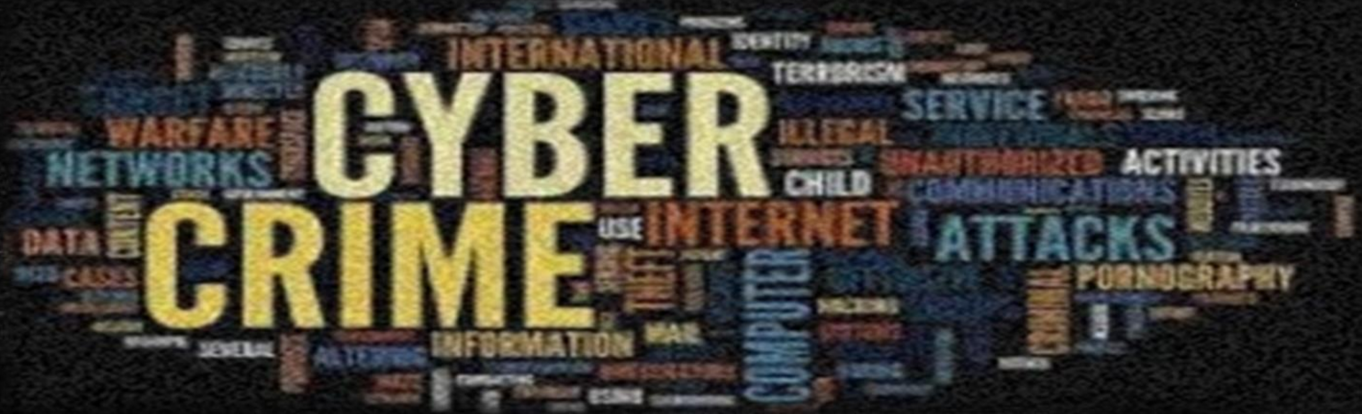
Problem based learning

By: Abdullah Ali

الجامعة الليبية الدولية للعلوم الطبية
LIBYAN INTERNATIONAL MEDICAL UNIVERSITY
LIMU

1- define cybercrime ?

- *Cybercrime or computer oriented crime is a crime that involves a computer and network*
- *The computer may have been used in the commission of a crime or it might be the target Cybercrime may threaten a person , company or a nations security and financial health*



list types of them ?

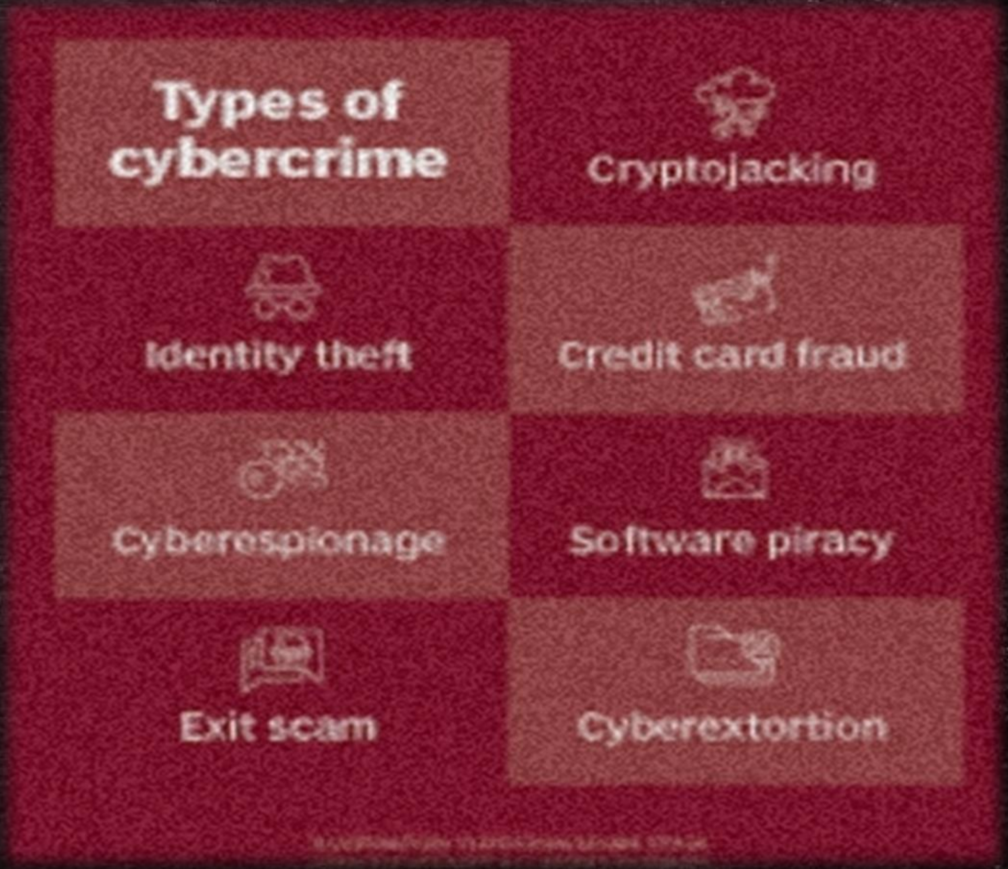
1. Hacking ▪

2. Virus dissemination ▪

3. Logic bombs. ▪

4. Phishing ▪

.5 Cyber stalking ▪



Types of cybercrime

Cryptojacking

Identity theft

Credit card fraud

Cyberespionage

Software piracy

Exit scam

Cyberextortion

2- define computer crimes? Types of them?

- *Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.*

List types of them ?

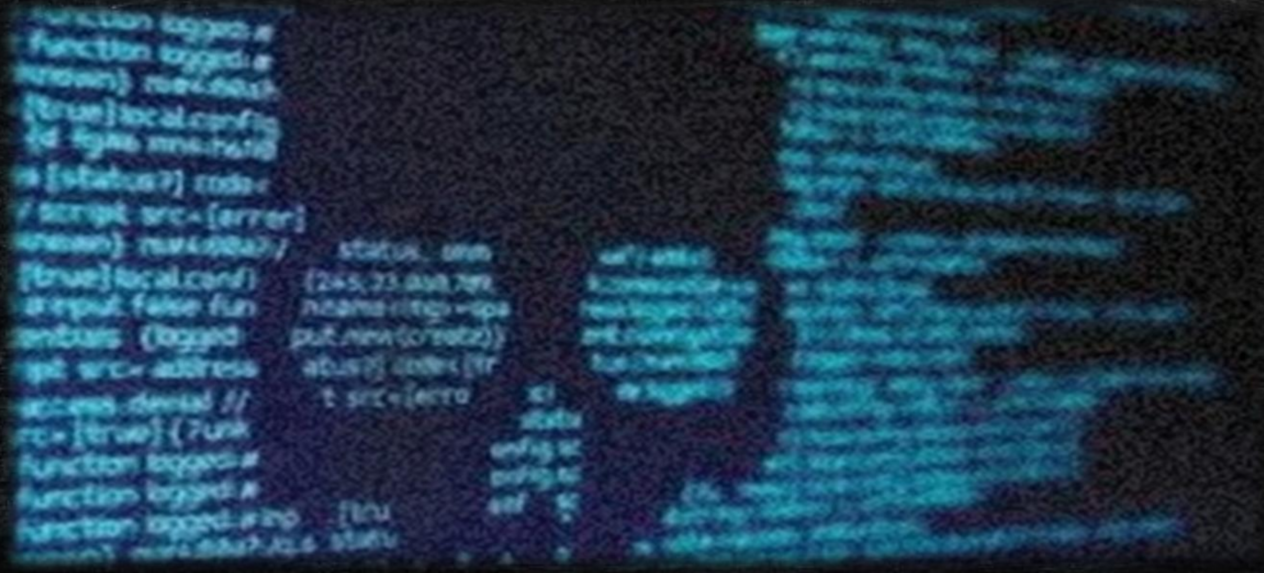
- *1--Copyright violation - Stealing or using another person's Copyrighted material without permission.*
- *2- cracking Breaking or deciphering codes designed to protect data.*
- *3-Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.*
- *4- Cyber bully - Harassing or stalking others online.*
- *5-Cyber squatting - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.*

3- list types of computer criminals ?

- 1- identity thieves
- 2- internet stalkers
- 3- phishing scammers
- 4- cyber terrorists

4- describe computer security risks ?

- A computer security risk is really anything on your computer that may damage or steal your data or allow someone else to access your computer without your knowledge or consent .
- There are a lot of different things that can create a computer risk , including malware .



5- discuss how computer develops effects on your privacy ?

- There has been written a lot about the Internet of Things and how it is going to change the world and societies for the better. We probably still cannot imagine the full potential of smart solutions that the future is going to unlock. For sure, the Iota will bring about great technological advancements, wonderful things, new insights and new ways of living. Soon enough, everything will be connected to the Internet: our homes, household appliances, cars, medical devices, clothes. It is just a matter of time before such technological solutions become our every-day reality.

6- discuss how to protect your computer and yourself?

- **Install Firewall**

- *Install Firewall A firewall enacts the role of a security guard. There are of two types of firewalls: a software firewall and hardware firewall. Each serves similar, but different purposes. A firewall is the first step to provide security to the computer. It creates a barrier between the computer and any unauthorized program trying to come in through the Internet. If you are using a system at home, turn on the firewall permanently. It makes you aware if there are any unauthorized efforts to use your system.*

Use Complex and Secure Passwords:

- *The first line of defense in maintaining system security is to have strong and complex passwords. Complex passwords are difficult for the hackers to find. Use a password that is at least 8 characters in length and include a combination of numbers, letters that are both upper and lower case and a special character. Hackers use certain tools to break easy passwords in few minutes. One recent study showed that a 6 character password with all lower case letters can be broken in under 6 minutes!*

SHALL USE STRONG PASSWORDS.
I SHALL USE STRONG PASSWORDS.
I SHALL USE STRONG PASSWORDS.
I SHALL USE STRONG PASSWORDS.
I SHALL USE STRONG PASS
I SHALL USE STRONG PAS
I SHALL USE STRONG PA
I SHALL USE STRONG PAS
I SHALL USE STRONG P

install Antivirus Software:

- *Antivirus is one other means to protect the computer. It is software that helps to protect the computer from any unauthorized code or software that creates a threat to the system. Unauthorized software includes viruses, key loggers , Trojans etc. This might slow down the processing speed of your computer, delete important files and access personal information. Even if your system is virus free, you must install an antivirus software to prevent the system from further attack of virus.*

- *Antivirus software plays a major role in real time protection, its added advantage of detecting threats helps computer and the information in it to be safe. Some advanced antivirus programs provide automatic updates, this further helps to protect the PC from newly created viruses.*

- *Antivirus for Windows 8 software may include advanced features such as email protection, blocking of pop-ups and identity theft.*

Check on the Security Settings of the Browser:

Browsers have various security and privacy settings that you should review and set to the level you desire. Recent browsers give you ability to tell web sites to not track your movements, increasing your privacy and security.

7- define encryption and how to secure your online information ?

- *Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.*
- *In computing, unencrypted data is also known as plaintext , and encrypted data is called cipher text. The formulas used to encode and decode messages are called encryption algorithms, or ciphers*

How to secure your info ?

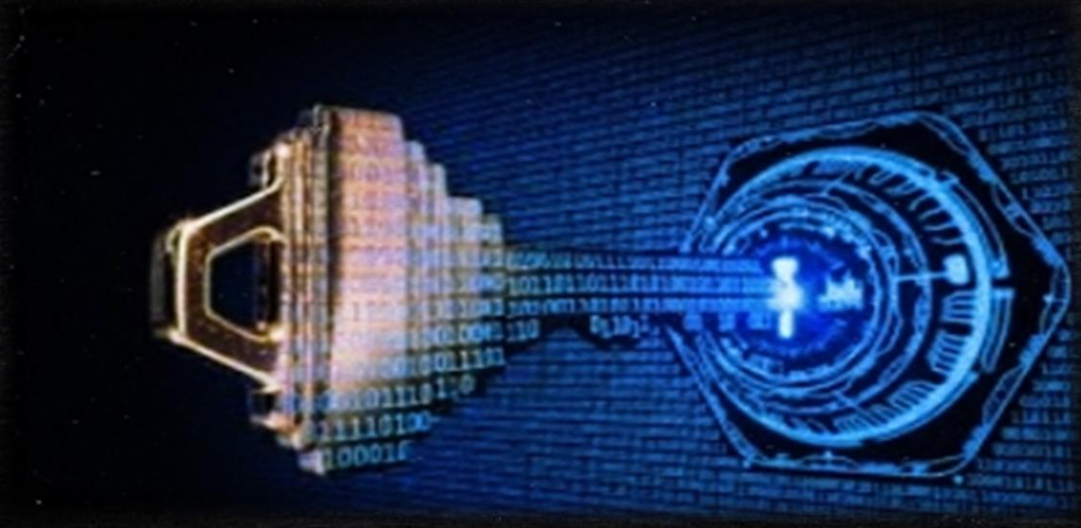
- *Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.*
- *Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor's office.*
- *Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.*
- *Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.*
- *Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.*
- *Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold on your mail.*
- *When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.*

8- discuss issues that faces govermentinal and legal agencies while decrypt info?

1-Spread use of robust unbreakable key

2-Common used of pretty good privacy

Is an encryption program that provides cryptography privacy and authentication for data communication



9- distinguee the different between electronic discovery and computer forensics ?

- ELECTRONIC DISCOVERY

- *Data collection involves identification and preservation as well as collecting, analyzing, and reporting data. Electronic discovery utilizes all those processes and generally collects active data. Active data is classified as information and data that is easily available through file storage and program managers utilized by a business or individual.*

- *When collecting data through electronic discovery, the data usually goes to the legal counsel who then performs his or her own review on the data. The professionals collecting this data are simply transferring information and do not discuss the intent of the user or business. They also do not provide legal advice.*

- *Electronic discovery is useful when the only information needed involves easily accessible files such as email, calendars, documents, and databases. A computer forensics expert is needed to further analyze the data if it has been deleted or if someone has tampered* with it.

DIGITAL FORENSICS

- *A forensic analysis of data is needed when the litigation requires a deeper look at the data. A digital forensic specialist sorts through data in search of hidden files or deleted data to help provide more-reliable evidence. Here are some examples of data that could be discovered using digital forensics:*

- *Data being stored automatically. After many years of digital backups, automatically stored data may have been removed from a server. Forensics can discover this data typically located on a hard drive.*

- *Deleted data. Any files that have been deleted from the system will usually remain on the computer's hard drive. Forensics will be used to locate this information as long as the hard drive has not been overwritten or wiped.*

- *Wiping software. Most computer forensic specialists can determine if any hard drive wiping software was used on a computer. This can help make a case that data was destroyed purposely.*

- *Digital forensic experts are brought in to produce more than data for a case. They analyze that data in hopes of finding evidence that can be used for a client. Typically, they partner with a legal team to determine what type of data they are seeking. These experts are more active with the case and can be called on in legal proceedings to defend their claims about the information.*

- *Computers are your future*