HUM141
Computer Law

Lecture 2: Examples (Types) of Computer Crime

Dr. Fayza Nada

What is computer crime

- Computer Crime, E-Crime, Hi-Tech Crime or Electronic Crime is a crime in which a computer plays an essential part.
- This type of crime is the illegal exploitation of computer technologies, usually involving the Internet, to support crimes such as fraud, identity theft, sharing of information, and embezzlement.
- What is illegal varies greatly from territory to territory.
- The growth of international data communications and in particular the Internet has made these crimes both more common and more difficult to police.
  - Luckily there are people fighting computer crime and it is taken very seriously by government agencies.

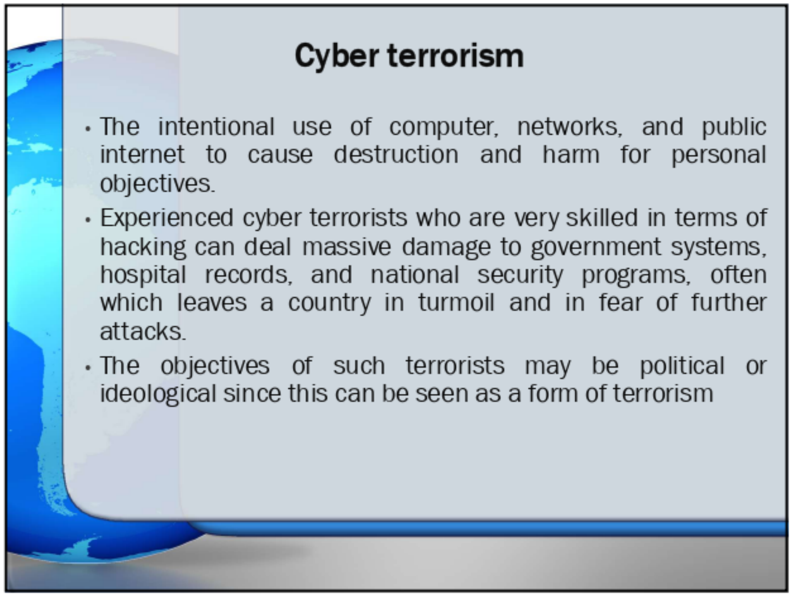
Examples (Types) of Computer Crime

Below is a listing of the different types of computer crimes today

- Cyber terrorism
- Cyber bully or Cyber stalking
- Creating Malware
- Denial of Service (DoS) attack
- Espionage
- Fraud
- Harvesting
- Identity theft
- Intellectual property theft
- Phishing

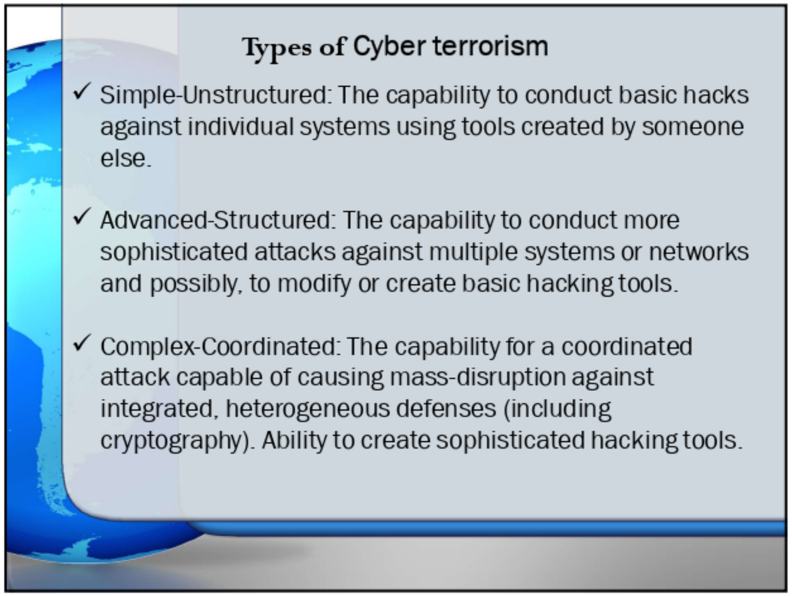
Examples of Computer Crime - Cont

- Salami Slicing
- Scam
- Spamming
- Spoofing
- Unauthorized access
- Wiretapping



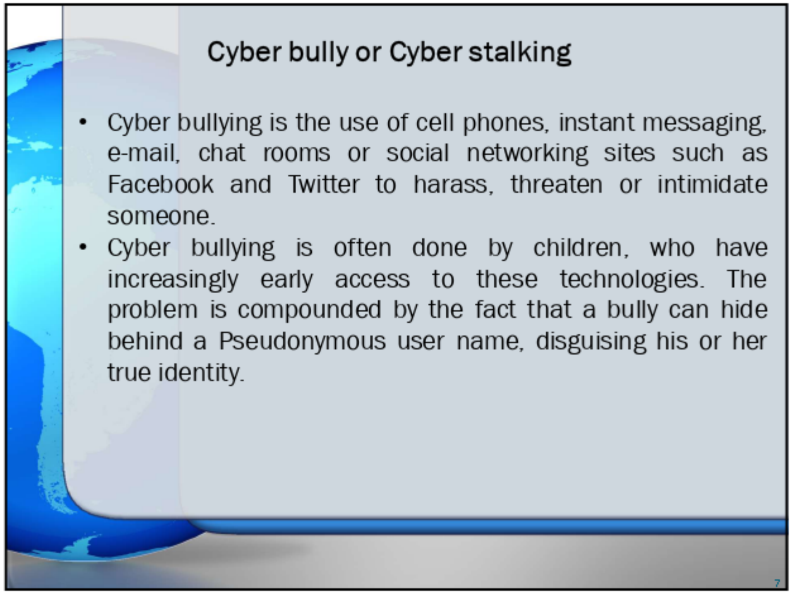
Cyber terrorism

- The intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.
- Experienced cyber terrorists who are very skilled in terms of hacking can deal massive damage to government systems, hospital records, and national security programs, often which leaves a country in turmoil and in fear of further attacks.
- The objectives of such terrorists may be political or ideological since this can be seen as a form of terrorism



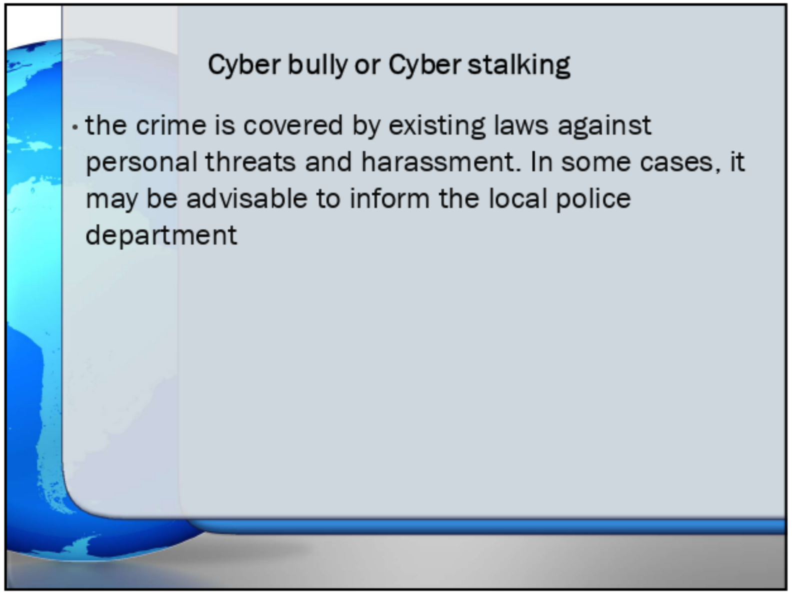
Types of Cyber terrorism

- ✓ Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else.
- ✓ Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools.
- ✓ Complex-Coordinated: The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools.



Cyber bully or Cyber stalking

- Cyber bullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone.
- Cyber bullying is often done by children, who have increasingly early access to these technologies. The problem is compounded by the fact that a bully can hide behind a Pseudonymous user name, disguising his or her true identity.



Cyber bully or Cyber stalking

- the crime is covered by existing laws against personal threats and harassment. In some cases, it may be advisable to inform the local police department

Creating Malware

- **Malware** is malicious software designed to change your settings, delete software, cause errors, watch browsing habits, or open computer to attacks.
- A computer can be infected by malware by visiting an infected website, downloading infected software, or installing infected software.

Denial of Service (DoS) attack

- is a method of attacking a networked computer by sending it an abnormally high number of requests, causing its network to slow down or fail.
- Since a single individual cannot generate enough traffic for a DoS attack, these attacks are usually run from multiple computers infected by worms.

Espionage

- **Espionage** (colloquially, **spying**) is the obtaining of information considered secret or confidential without the permission of the holder of the information.
- Espionage can be committed by an individual or a **spy ring** (a cooperating group of spies), in the service of a government or a company, or operating independently.
- It is by definition unwelcome and in many cases illegal and punishable by law.

Fraud

- **Computer fraud** is defined as any act using computers, the Internet, Internet devices, and Internet services to defraud people, companies, or government agencies of money, revenue, or Internet access.
- There are many methods used to perform these illegal activities.
- Phishing, viruses, and Dos attacks are some examples used to disrupt service or gain access to another's funds, but this list is not inclusive.

Harvesting

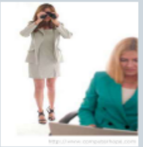
- A **harvester** is a software program designed to parse through large amounts of data, such as web pages on the Internet, to extract specific information.
- For example, a harvester may be designed to grab accounts, addresses, E-mail addresses, names, and phone numbers.
- With **account harvesting** a person or program records login and password information from a legitimate user to illegally gain access to their account(s).

Identity theft

- **Identity theft** is the act of a person obtaining information illegally about someone else.
- Thieves try to find such information as full name, address, date of birth, social security number, passwords, phone number, e-mail, and credit card numbers.
- The thief can then use this information to gain access to bank accounts, e-mail, cell phones, identify themselves as you, or sells your information.

intellectual property theft

- Stealing another persons or companies intellectual property.
- involves robbing people or companies of their ideas, inventions, and creative expressions—known as "**intellectual property**"
- **intellectual property** can include everything from trade secrets and proprietary products and parts to movies, music, and software.



Phishing

- Describe a malicious individual or group of individuals who scam users.
- They do so by sending E-mails or creating web pages that are designed to collect an individual's online bank, credit card, or other login information.
- Because these e-mails and web pages look like legitimate companies users trust them and enter their personal information.

Salami Slicing

- Stealing tiny amounts of money from each transaction.
- taking tiny fractions of every transaction that builds into a large sum of illegally gained money.
- If you stole fractions of a penny on a transaction it could go unnoticed and if you were to steal this small amount from thousands of transactions it can quickly add up.

Scam

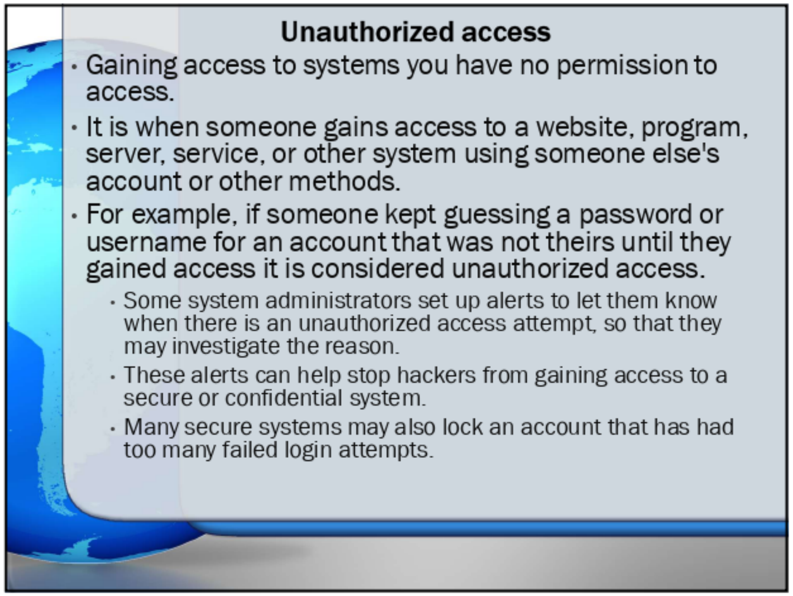
- Tricking people into believing something that is not true.
- Describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person. With the world becoming more connected thanks to the Internet, online scams have increased, and it's often up to you to help stay cautious with people on the Internet.

Spamming

- Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- referred to as **UCE (Unsolicited Commercial Email)** and **bulk e-mail**, **spam** is used to describe junk e-mail on the Internet.
- Spam is e-mail sent to thousands and sometimes millions of people without prior approval, promoting a particular product, service or a scam to get other people's money.

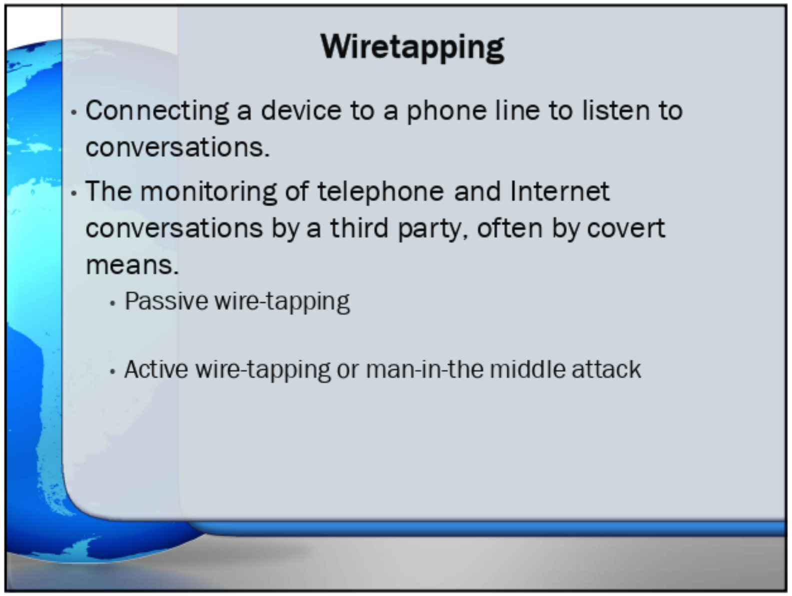
Spoofing

- Deceiving a system into thinking you are someone you really are not.
- the term **spoof** refers to hacking or deception that imitates another person, software program, hardware device, or computer, with the intentions of bypassing security measures. One of the most commonly known spoofing is IP spoofing.



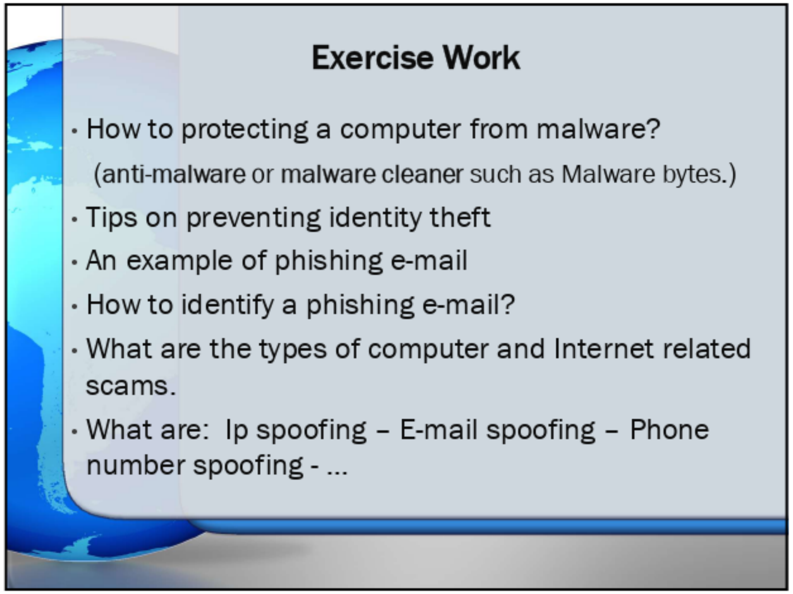
Unauthorized access

- Gaining access to systems you have no permission to access.
- It is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods.
- For example, if someone kept guessing a password or username for an account that was not theirs until they gained access it is considered unauthorized access.
  - Some system administrators set up alerts to let them know when there is an unauthorized access attempt, so that they may investigate the reason.
  - These alerts can help stop hackers from gaining access to a secure or confidential system.
  - Many secure systems may also lock an account that has had too many failed login attempts.



Wiretapping

- Connecting a device to a phone line to listen to conversations.
- The monitoring of telephone and Internet conversations by a third party, often by covert means.
  - Passive wire-tapping
  - Active wire-tapping or man-in-the middle attack



Exercise Work

- How to protecting a computer from malware?

  (anti-malware or malware cleaner such as Malware bytes.)
- Tips on preventing identity theft
- An example of phishing e-mail
- How to identify a phishing e-mail?
- What are the types of computer and Internet related scams.
- What are: Ip spoofing – E-mail spoofing – Phone number spoofing - …