CYBERSECURITY

BY AHMED ALTARHONY

OBJECTIVES

- List the types of computer crimes , cyber crimes and computer criminals
- explain how privacy and anonymity become more at risk as technology develops
- Define encryption and explain how it makes online information secure
- Explain the issues the government faces when balancing between the need to access encrypted data and the public right to privacy
- Describe how to protect your computer and yourself
- Distinguish between electronic discovery and computer forensics

LIST THE TYPES OF COMPUTER CRIMES , CYBER CRIMES AND COMPUTER CRIMINALS

Types of computer crimes

- **identity theft**
- **phishing**
- **Spear phishing**
- **Malware**
  - **Spyware**
    - **Adware**
    - **Keyloggers**
- **computer virus**
  - **file infectors**
    - **macros**
    - A **boot sector virus**
- **rogue program**
  - Logic bomb
  - Time bomb
  - Worm

LIST THE TYPES OF COMPUTER CRIMES , CYBER CRIMES AND COMPUTER CRIMINALS

Types of computer crimes

- **denial of service (DoS) attack**
- **distributed denial of service (DDoS) attack**
  - Botnet
  - syn flooding
- **Trojan horse**
- **Rootkit**

Types of cybercrimes

- **Cyberstalking**
- **Cyberbullying**
- **Cybergaming**

Types of computer criminals

- **Hackers**
- **Crackers**
- **Cybergangs**

EXPLAIN HOW PRIVACY AND ANONYMITY BECOME MORE AT RISK AS TECHNOLOGY DEVELOPS

Cookies

- Contain our personal information written by website we visited, stored in user 's hard disk
- Used by internet ad network to track user browsing and preference
- It threats our anonymously and privacy

Radio Frequency Identification

- Chips or tags that uses radio wave for transmitting data and storing information
- Chips or tags can track our movement
- Some chips uses encrypted transmission of data which can be interfere by thief easily and stole the information
- Used in passport card **, pets for tracing and for individual to store health records and personal details**

Ubiquitous Computing

- It is concept of using technology implicit, built in things we use
- Such as active badge which used for track our movement and forward e-mail , phone call , message so on

EXPLAIN HOW PRIVACY AND ANONYMITY BECOME MORE AT RISK AS TECHNOLOGY DEVELOPS

Ubiquitous Computing

- **And other devices such as pcs , smart phones and digital music players**
- **Which contain such as a playlist, records of incoming or outgoing calls, or a list of recently viewed media**
- **stolen of these devices violate our privacy or can exhibit our privacy to danger**

Globally Unique Identifiers A globally unique identifier

- (GUID) is an identification number that is generated by a hardware component or a program
- **Can be read by web server** or embedded in various documents identifying the computer
- **Also** color laser printers embed printer tracking dots nearly invisible yellow dots
- these dots can identify the serial number and manufacturing code of the printer well as the time and date the document was printed.

DEFINE ENCRYPTION AND EXPLAIN HOW IT MAKES ONLINE INFORMATION SECURE

Definition of Encryption

- **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext

How encryption makes online information secure

- In encryption process a message such as ‘hello world ’ in plaintext subject to an encryption logarithm for each character in message substitutes the letter that is 13 positions to the right in the 26-letter alphabet (When you reach the end of the alphabet, start counting from the beginning.) the message will appear ‘tquua iadup’ in ciphertext un unreadable message this encryption logarithm is called encryption key
- In short encryption is the process of subjecting plaintext readable code to an encryption key which convert it to ciphertext or unreadable code

EXPLAIN THE ISSUES THE GOVERNMENT FACES WHEN BALANCING BETWEEN THE NEED TO ACCESS ENCRYPTED DATA AND THE PUBLIC RIGHT TO PRIVACY

- The use of unbreakable encryption will allow drug lords, spies, terrorists, and even violent gangs to communicate about their crimes and their conspiracies with impunity because is encoded and unreadable code or data
- Which provide secure way for them to communicate exchange data or message
- The use of unbreakable encryption will decrease or devastate the ability of government to fight crime and prevent terrorism. .

EXAMPLE : Pretty Good Privacy (PGP)

- And the use of breakable encryption will create backdoor and a vulnerability that could enable someone to crack the code, compromising the security of this encryption tool so threat the privacy or the security of information for the public

DISTINGUISH BETWEEN ELECTRONIC DISCOVERY AND COMPUTER FORENSICS

Computer forensics

- Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law related to computer crimes such as electronic fraud, cyberstalking, cyberbullying, phishing, or hacking

Electronic discovery

- the electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation including e-mails, voicemails, instant messages, e-calendars, audio files, data on handheld devices, animation, metadata, graphics, photographs, spreadsheets, Websites, drawings, and other types of digital data for noncomputer-related crime like hit-and-run or murder

DESCRIBE HOW TO PROTECT YOUR COMPUTER AND YOURSELF

Protecting computer

- **Power-Related Problems**
  - Power outages can destroy sensitive electronic components and carry the threat of data loss.
  - **Using application that backup work** at a specified interval
  - equip system with an **uninterruptible power supply (UPS)**
- **Controlling Access**
  - **By using strong password , pin code and biometric authentication** and the use of a physical trait or behavioral characteristic to identify an individual
- **Firewalls**
  - A **firewall** is a computer program or device which limits the ability of outsiders to access internal data

DESCRIBE HOW TO PROTECT YOUR COMPUTER AND YOURSELF

Protecting yourself

Avoiding Scams

- Do business with established companies that you know and trust
- Read the fine print. In situation of ordering something, make sure it's in stock or company promises to deliver within 30 days.
- Don't provide financial or other personal information or passwords to anyone
- Don't trust anyone in internet chat room

Preventing Cyberstalking

- Don't share any personal information
- Be extremely cautious about meeting anyone you've contacted online
- contact the police immediately if a situation you've encountered online makes you uncomfortable or afraid