EBA SOUNNI

1845116

IA3

Cybercriminals are individuals who use computer, network, and the internet to perpetrate crime.

There are four common categories of complaints the (IC3) receives:

1- government impersonation scams involve people pretending to represent official organization such as FBI, to defraud.
2- **Nonaction/non-delivery** scams involve running auction of merchandise that does not really exist.
3- **Advance fee fraud** involve convincing individuals to send money as a good faith.
4- **Identity theft** involves the stealing of someone's personal information for financial gain.
identity theft occurs when a thief steals personal information such as your name, address, birth date, bank number account, and social security number.
Although most people are aware of spam, the (M3AAWG) found that half of e-mail users have opened spam.
Hacker anyone who unlawfully breaks into a computer system either an individual computer or a network.
    - **White-hat hackers** break in to system for nonmalicious reasons, such as to test system security or to expose undisclosed weaknesses.
    - **Black-hat hackers** break into systems to destroy information or for illegally gain.
    - **Gray-hat hackers** they often illegally break into system merely to flaunt their expertise to the administrator of the system they penetrated or to attempt to sell their services in repairing security breaches.

Packet analyzer is a program deployed by hackers that looks at (or sniffs) each packet as it travels on the internet.

Trojan horse is a program that appears to be something useful or desirable, like a game or a screen saver, but while it runs it does something malicious in the background without your knowledge.

Backdoor programs is a program that allow hackers to gain access to your computer and take almost complete control of it without your knowledge.

Zombie a computer that a hacker controls it.

Distributed denial-of-service(DDoS)attack which launches DoS attacks from more than one zombie(sometimes thousands of zombies) at the same time.

Botnet is a large group of software programs that runs autonomously on zombie computers.

Exploit kits are software programs that run on servers and search for vulnerabilities of computers that visit the server.

Logical port are virtual-that is,not physical-communication gateways or paths that allow a computer to organize requests for information.

Virus basics

Virus is a computer program that attaches itself to another computer program(known as **the host**) and attempts to spread to other computers when files are exchanged. The viruses main purpose is to replicate itself and copy its code into as many other host files as possible.

How does my computer catch a virus?

- Shared flash drives.

- Downloading infected audio and video files.
- E-mail attachment.

How can I tell if my computer is infected?

1. Existing program icons or files suddenly disappear.
2. You start your browser and it takes you to an unusual home page.
3. Odd messages, pop-ups, or images are displayed on the screen.
4. Data files become corrupt.
5. Programs stop working properly, which could be caused by either a corrupted file or a virus.
6. Your system shuts down unexpectedly.

Types of Viruses

Boot-sector virus is a program that executes whenever a computer boots up, ensuring that the virus will be loaded into memory immediately, even before some virus protection programs can load.

Logic bomb is a virus that is triggered when certain logical conditions are met.

Worm is subtly different. Viruses require human interaction to spread, whereas worms take advantage of file transport methods.

Script is a series of commands a(miniprogram) that is executed without your knowledge.

Macro virus is a virus that attaches itself to a document that uses macros. A macro is a short series of commands that usually automates repetitive tasks.

e-mail virus use the address book in victim's e-mail system to distribute the virus.it sent itself to the first 50 people in the e-mail address book on the infected computer.

Encryption viruses hold files hostage by encrypting them, asking for payment to unlock them.

Polymorphic virus changes its own code to avoid detection.

Multipartite virus is designed to infect multiple files types in an effort to fool the antivirus.

Stealth viruses temporarily erase their code from the files where they reside and then hide in the active memory of the computer. This helps them avoid detection if only the hard drive is being searched for viruses. Fortunately, current antivirus software scans memory as well as the hard drive.

Malware: Adware and Spyware

Malware is software that has a malicious intent. There are three forms of malware: adware, spyware, and viruses.

Adware is software that displays sponsored advertisements in a section of your browser window or as a pop-up box. Fortunately, web browsers such as Firefox, Chrome, and Edge have built-in pop-up blockers.

Spyware is an unwanted piggyback programs that usually downloads with other software you install form the internet and that runs in the background of your system. Without your knowledge, spyware transmits information about you, to the owner of the program so that the information can be used for marketing purposes. One type of spyware programs known as a **Keystroke logger** monitors keystrokes with the intent of stealing password, login IDs, or credit card information.

spam

Companies that send out **Spam** find your e-mail address either from a list they purchase or with software that looks for e-mail address on the internet.

Spam filter is an option you can select in your e-mail account that places known or suspected spam messages into a special folder.

How can I prevent spam?

1. Before registering on a website, read its privacy policy to see how it uses your e-mail.
2. Don't reply to spam to remove yourself from the spam list.
3. Subscribe to an e-mail forwarding service such as versa-forward.

Cookies are small text files that some website automatically store on your hard drive when you visit them. the site marks your visit and keeps track of it in its database. Making your next visit to a website more efficient and better geared to your interests. Cookies pose no security threat.

Social engineering is any technique that uses social skills to generate human interaction that entices individuals to reveal sensitive information.

Pretexting involves creating a scenario that sounds legitimate enough that someone will trust you.

Phishing lures internet users to reveal personal information such as credit card numbers, or other sensitive information that could lead to identity theft.

Pharming when malicious is planted on your computer.

How can I avoid phishing and pharming?

- never reply directly to any e-mail asking for personal information.
- Don't click on a link in an e-mail to go to a website.
- Check with the company asking for the information.
- Never give personal information over the internet unless you know the site is secure.
- Use phishing filters.
- Use internet security software.

Scareware is a type of malware that downloads onto your computer and tries to convince you that your computer is infected with a virus, then you're directed to a website where you can buy fake antivirus. To protect yourself from scareware, make sure you never click on website banners or pop-up boxes.

Firewall is a software program or hardware device designed to protect computers from hackers. A firewall specifically designed for home network is called a **personal firewall.** both windows and OS X include reliable firewall.

How do firewalls protect you from hackers?

1. By blocking access to logical ports.
2. By keeping your computer's network address secure.

Firewalls can be configured so that they filter out packets sent to specific logical ports in a process known as **packet flirting.**

Firewalls are also often configured to ignore requests that originate from the internet asking for access to certain ports. This process is referred to as **logical port blocking.**

Firewalls use a process called **network address translation (NAT)** to assign internal IP addresses on a network. The internal IP addresses are used only on the internet network and therefore can't be detected by hackers.

What is the best way to protect my device from viruses?

There are two main ways to protect you computer from viruses: by installing antivirus and by keeping your software up to date.

1-Antivirus software is specifically designed to detect viruses and protect your computer and files from harm. Symantec, Kaspersky, Trend micro, and McAfee are among the companies that offer highly rated antivirus software packages. You should run an active scan on your entire computer at least once a week.

How dose antivirus software work?

- Detection**:** Antivirus software looks for virus signatures in files. A **virus signature** is a portion of the virus code that's unique to a particular computer virus.
- Stopping virus executing: if the antivirus software detects a virus signature or suspicious activity. It also places the virus in a secure area on your hard drive so that it won't spread to other files; this procedure is known as **quarantining.**
- Prevention of future infection: most antivirus software will also attempt to prevent infection by inoculating key files on your computer. In **inoculating.**

Most antivirus programs have an automatic update feature.

2-Software updates malicious websites can be set up to attack your computer by downloading harmful software onto your computer. This type of attack known as a **drive-by download.**

What constitutes a strong password?

- Don't use easily deduced components related to your life.
- Use a password that is at least 14 characters long.
- Don't use words found in the dictionary.
- Use a mix of upper-and lowercase letters and symbols.
- Never tell anyone your password or write it down in a place where others might see.
- Change your passwords on a regular basis.
- Don't use the same password for every account you have.

A biometric authentication device is a device that reads a unique personal characteristic and converts its pattern to a digital code. Such as fingerprint, the iris pattern in your eye, voice authentication, and face recognition.

Virtual private networks (VPNs) are secure networks that are established using the public internet infrastructure.

Protecting your personal information

Information identity thieves crave never make this information visible on websites.

- ❖ Social security number.
- ❖ Full Date of Birth.
- ❖ Phone Number.
- ❖ Street Address.

Other sensitive information only reveal this information to people you know-don't make it visible to everyone.

- Full Legal Name
- E-mail Address
- Zip Code
- Gender
- School or Workplace

How might I damage the data on my computer?

1. Unauthorized access
2. Tampering
3. Destruction

Backups are copies of files that you can use to replace the originals if they're lost or damaged.

What types of files do I need to back up?

1. **Program files** include files used to install software.
2. **Data files** include files you've created or purchased.

What types of backups can I perform?

1. **Incremental:** only backs up files that have changed.
2. **Image:** snapshot of your entire computer including system software.

Where to store backup files

Backup location	PROS	CONS
❖ Online(in the cloud)	❖ Accessible anywhere. ❖ Remote location.	❖ Don't provide enough space for image backup.
❖ External hard drive	❖ Fast backups with USB port3 ❖ Inexpensive, one time cost.	❖ Could be destroyed. ❖ Slightly more difficult to back up multiple computers. ❖ Can be stolen.
❖ Network-attached storage device.	❖ Makes backups much easier for multiple computing devices.	❖ More expensive than a stand-alone external hard drive. ❖ Could be destroyed. ❖ Can be stolen.

Surge protector is a device that protects your computer against power surges. note that you should replace your surge protector every two to three years.

Whole-house surge protector they protect all electrical devices in the house.

You have four main security concerns with mobile devices:

1. Keeping them from being stolen.
2. Keeping data secure in case they are stolen.
3. Finding a device if it is stolen.
4. Remotely recovering and wiping data off a stolen device.