

# COMPUTER VIRUS



Lecture five

Presented by : ms.c ghufan abdulameer

# INTRODUCTION

- A computer virus is a malicious application or authored code used to perform destructive activity on a device or local network. The code's malicious activity could damage the local file system, steal data, interrupt services, download additional malware, or any other actions coded into the program by the malware author. Many viruses pretend to be legitimate programs to trick users into executing them on their device, delivering the computer virus payload.

# What Causes Computer Viruses?

- Computer viruses are standard programs; only instead of offering useful resources, these programs can damage your device. For a threat actor to execute a virus on your machine, you must initiate execution. In some cases, an attacker can execute malicious code through your browser or remotely from another network computer. Modern browsers have defenses against local machine code execution, but third-party software installed on the browser could have vulnerabilities that allow viruses to run locally.
- The delivery of a computer virus can happen in several ways. One common method is via a phishing email. Another technique is hosting malware on a server that promises to provide a legitimate program. It can be delivered using macros or by injecting malicious code into legitimate software files.

# Computer Virus Do?

- The way a computer virus acts depends on how it's coded. It could be something as simple as a prank that doesn't cause any damage, or it could be sophisticated, leading to criminal activity and fraud. Many viruses only affect a local device, but others spread across a network environment to find other vulnerable hosts.
- A virus that infects a host device will continue delivering a payload until it's removed. Most antivirus vendors have small removal programs that eliminate the virus. Polymorphic viruses make it difficult for removal because they change their footprint consistently. The payload could be stealing data, destroying data, or interrupting services on the network or the local device.

# Examples of Computer Virus

The web contains millions of computer viruses, but only a few have gained popularity and infect record numbers of machines. Some examples of widespread computer viruses include:


- Worms - A worm is a type of virus that, unlike traditional viruses, usually does not require the action of a user to spread from device to device.
- Trojans - a Trojan is a virus that hides within a legitimate-seeming program to spread itself across networks or devices.
- Ransomware - Ransomware is a type of malware that encrypts a user's files and demands a ransom for its return. Ransomware can be, but isn't necessarily, spread through computer viruses.

# Symptoms of Computer Virus

- Popup windows, including ads (adware) or links to malicious websites.
- Your web browser home page changes, and you did not change it.
- Outbound emails to your contact list or people on your contact list alert you to strange messages sent by your account.
- The computer crashes often, runs out of memory with few active programs, or a blue screen of death in Windows.
- Slow computer performance even when running few programs or the computer was recently booted.
- Unknown programs start when the computer boots or when you open specific programs.
- Passwords change without your knowledge or your interaction on the account.

# How to Prevent Computer Viruses

- **Install antivirus software:** Antivirus should run on any device connected to the network. It's your first defense against viruses. Antivirus software stops malware executable from running on your local device.
- **Don't open executable email attachments:** Many malware attacks including ransomware start with a malicious email attachment. Executable attachments should never be opened, and users should avoid running macros programmed into files such as Microsoft Word or Excel.
- **Keep your operating system updated:** Developers for all major operating systems release patches to remediate common bugs and security vulnerabilities. Always keep your operating system updated and stop using end-of-life versions (e.g., Windows 7 or Windows XP).

- 
- **Avoid questionable websites:** Older browsers are vulnerable to exploits used when just browsing a website. You should always keep your browser updated with the latest patches, but avoiding these sites will stop drive-by downloads or redirecting you to sites that host malware.
  - **Don't use pirated software:** Free pirated software might be tempting, but it's often packaged with malware. Download vendor software only from the official source and avoid using software that's pirated and shared.

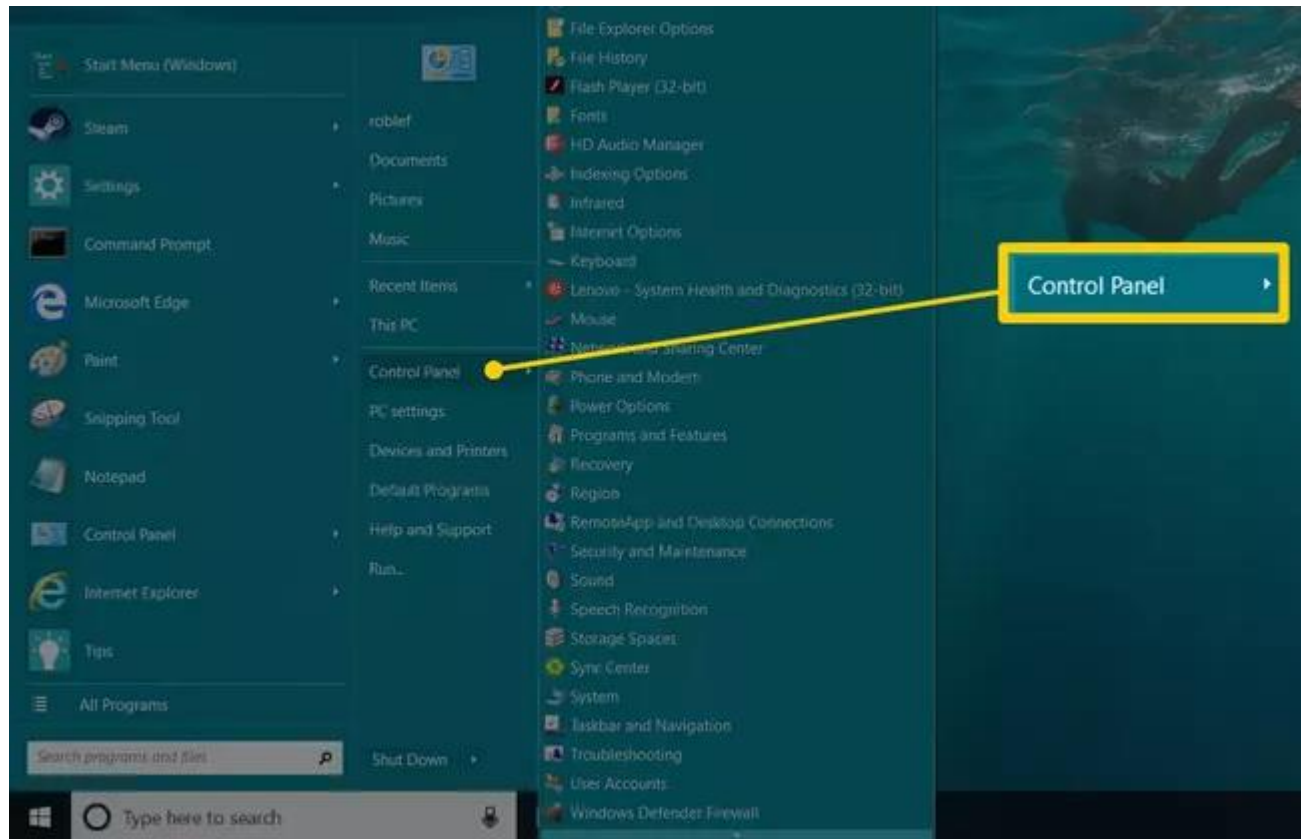


# FIRWALL

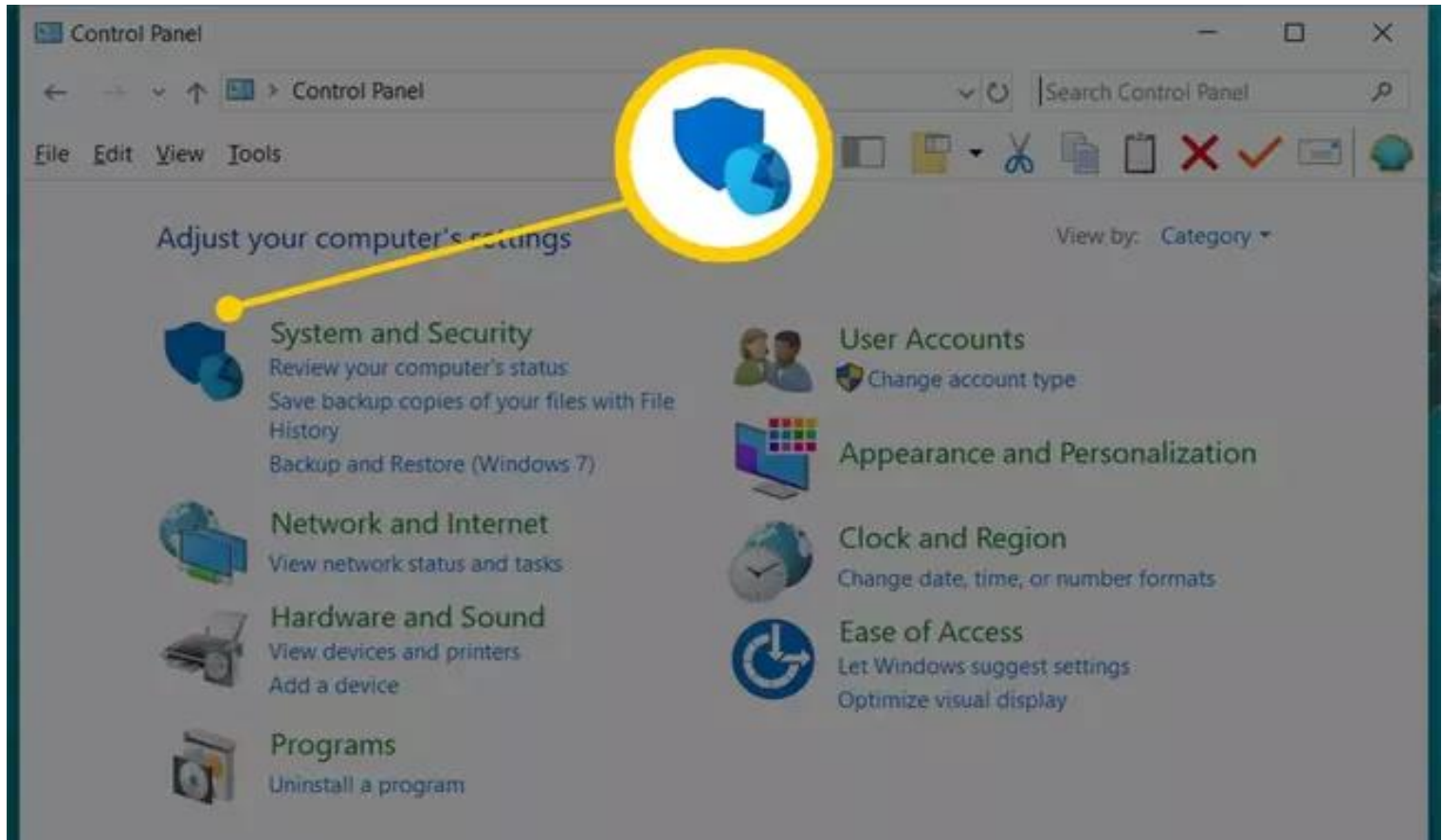
- The Windows Firewall is designed to keep unauthorized users from accessing files and resources on your computer. Still, the Windows Firewall can sometimes cause more harm than good, especially if there's another paid or free firewall program installed. Disabling the Windows Firewall is easy and usually takes less than 10 minutes.

## I-Open Control Panel.

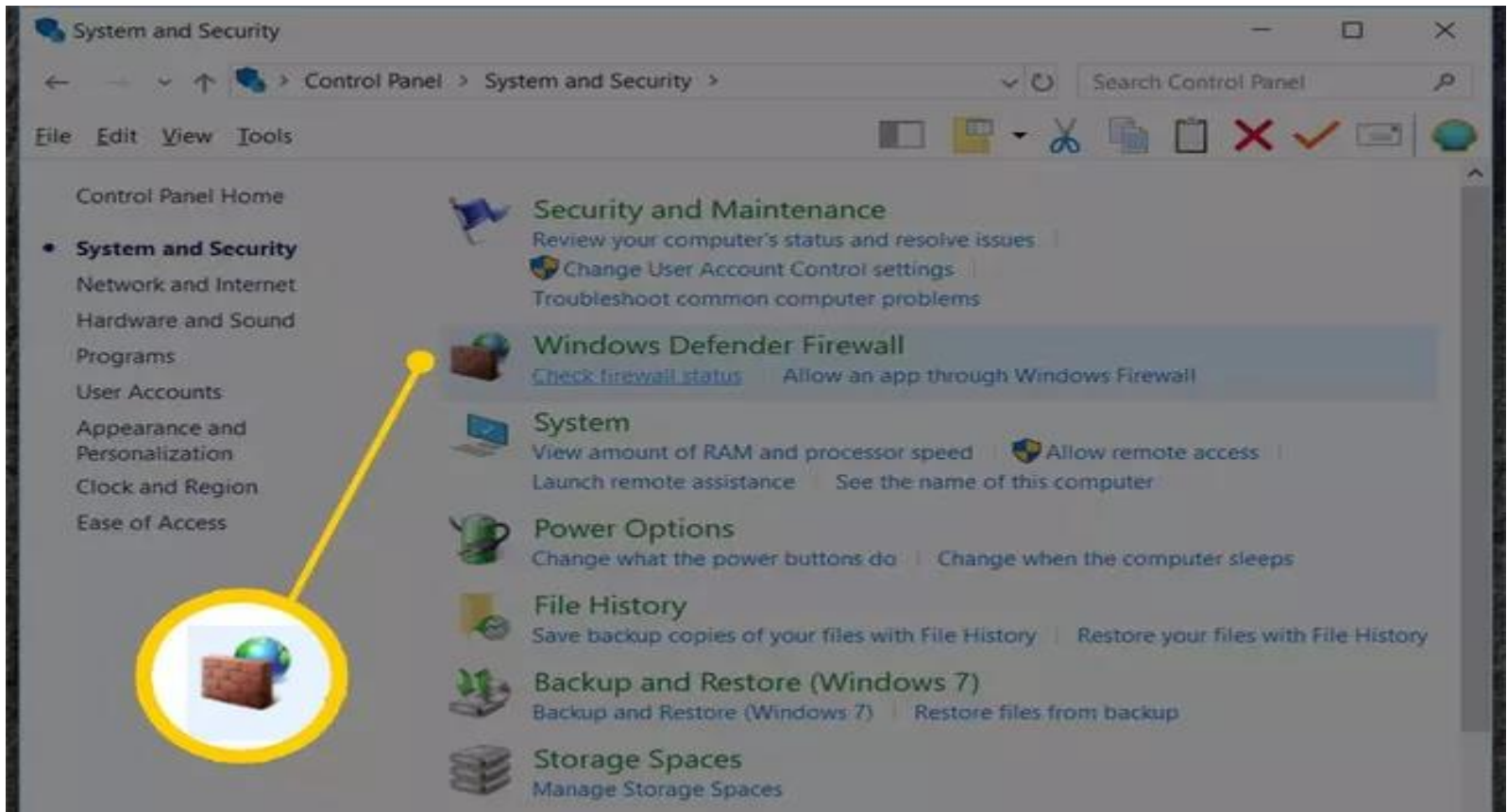
- You can do this a number of ways, but the easiest method is to search for it or select it from the Start menu in Windows 7.



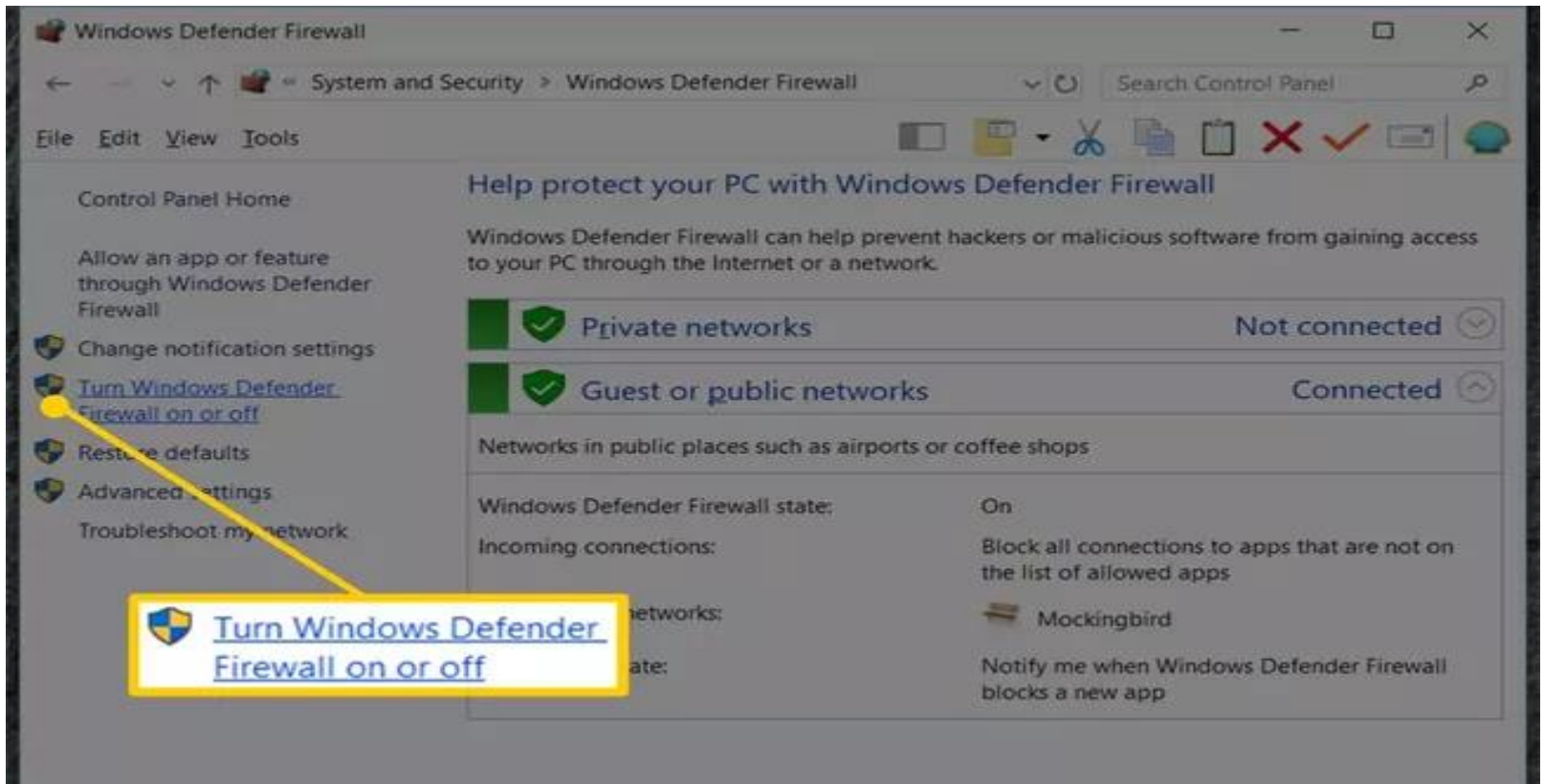
## 2-Select System and Security.



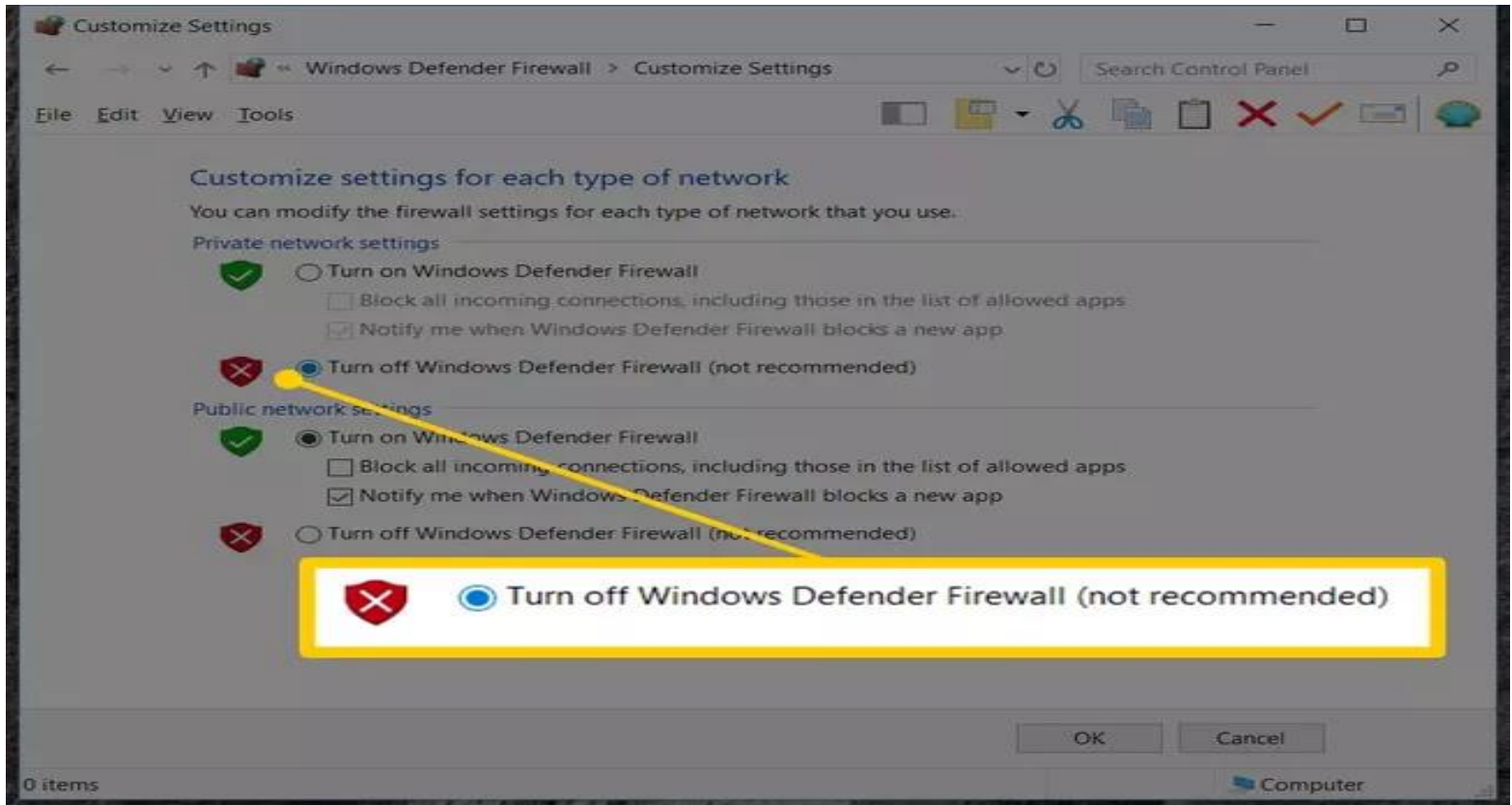
# 3-Choose Windows Firewall



# 4-Select Turn Windows Firewall on or off on the left side of the screen.



5-Select the bubble next to Turn off Windows Firewall (not recommended).



6-Select OK to save the changes.