Al Mustaqbal University
College of Medicine

Computer Science

Lecture 5
Computer Viruses

Dr Mohammed Fadhil
mohammed.fadhil1@uomus.edu.iq
and
Dr Ahmed Janabi
Ahmed.Janabi@uomus.edu.iq

Digital Security Risks

- Before discussing computer viruses, it is essential to address a **digital security risk**.
- A **digital security risk** is any event or action that could result in the loss or damage of hardware, software, data, information, or processing capability of a computer or mobile device.
- **Any illegal act** involving the use of a computer or related devices is generally termed as a **computer crime**
- A **cybercrime** is an online or Internet-based illegal act

Digital Security Risks

What is a Computer Virus?

- The term, **computer virus**, describes a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge or permission.
- Once the virus is in a computer, it can spread throughout and may damage your files and operating system.
- *Computer viruses do not generate by chance*. The programmer of a virus, known as a virus author, **intentionally** writes a virus program.
- Some **virus authors** find writing viruses a **challenge**. Others write them to cause **destruction**.
- Writing a virus program usually requires significant programming skills.

What is a Computer Virus?

- **A computer virus** is a program which can harm our device and files and infect them for no further use.
- When a virus program is executed, **it replicates itself** by modifying other computer programs and instead enters its own **coding**.
- **This code** infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.
- Across the world, **Computer viruses** are a great issue of concern as they can cause billions of dollars' worth harm to the economy each year.

Computer Virus

- A computer virus is not visible since it affects the programming of the device. However, certain signs can help you identify a virus-infected device:
  - **System Speed:** Applications take longer to open, and the system slows down.
  - **Pop-up Windows:** Frequent and excessive pop-ups appear.
  - **Self-Execution:** Programs or files open by themselves in the background.
  - **Account Logouts:** Increased risk of accounts getting hacked, causing automatic logouts.
  - **Device Crashes:** The device may crash and stop working if the virus spreads widely.

Types of Computer Virus

- A **worm** copies itself repeatedly, for example, in memory or over a network, using up system resources and possibly shutting the system down.
- A **Trojan horse** hides within or looks like a legitimate program such as a screen saver.
  - A certain condition or action usually triggers the Trojan horse.
  - Unlike a virus or worm, a **Trojan horse does not replicate itself to other computers**. Currently, more than one million known threats to your computer exist

Other Types of Computer Virus

- **Direct Action Virus**
  - Attaches to .exe or .com files and activates upon execution.
  - Known as Non-Resident Virus.
  - Hidden if installed in memory, does not stay permanently.
- **Resident Virus**
  - Saves itself in the computer's memory.
  - Infects other files and programs even when the originating program is not running.
  - Difficult to detect and remove because it hides in memory.

Types of Computer Virus

- **Multipartite Virus**
  - Can infect both the boot sector and executable files.
  - Poses a significant cyber threat if it attacks a system.
- **Overwrite Virus**
  - Replaces existing programs with malicious code.
  - Completely removes the original programming code of the host.
  - Highly destructive.
- **Polymorphic Virus**
  - Spread through spam and infected websites.
  - File infectors that modify themselves to avoid detection.
  - Retains original code while creating morphed versions.

Types of Computer Virus

- **File Infector Virus**
  - Infects a single file first, then spreads to other executable files and programs.
  - Often originates from games and word processors.
- **Spacefiller Virus**
  - Fills empty spaces within files without increasing the file size.
  - Known as cavity virus.
  - Difficult to detect.
- **Macro Virus**
  - Written in the same macro language used by software programs.
  - Activates when infected word processor files are opened.
  - Commonly spread via emails.

How To Protect Your Computer from Virus?

- The most suitable way of making your computer virus-free is by ***installing an Anti-virus software***. Such software help in removing the viruses from the device and can be installed in a computer via two means:
  - **Online** download
  - **Buying** an Anti-virus software and installing it

What is an Anti-Virus?

- An **anti-virus** is a software which comprises program or set of programs which can detect and remove all the harmful and malicious software from your device.
- An **anti-virus** program protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files
- This **anti-virus** software is designed in a manner that they **can search through the files** in a computer and determine the files which are heavy or mildly infected by a virus.

Antivirus software

- The popular antivirus programs are:
  - **Norton Antivirus**
  - **F-Secure Antivirus**
  - **Kaspersky Antivirus**
  - **AVAST Antivirus**
  - **Comodo Antivirus**
  - **McAfee Antivirus**
- Most of which also contains spyware removers, Internet filters, and other utilities.

Antivirus software

- **A spyware remover** is a program that detects and deletes spyware, and similar programs.
- **An adware remover** is a program that detects and deletes adware.
- **Internet Filters** are programs that remove or block certain items from being displayed.
  - Four widely used Internet filters are anti-spam programs, Web filters, phishing filters, and pop-up blockers.

THANK YOU ☺