Computer Sciences

University of Anbar
College of Pharmacy
2020 - 2021

Jamal Ali Hammad

List of Contents

Chapter Three

Computer Viruses and Crimes

1. Computer Viruses

A computer virus is defined as a piece code or program which is executed in a target computer to hamper the smooth functioning of the PC. It replicates itself and can quickly affect hosts of other computers, thus paralyzing the entire network. So, it is important for you to know how to remove it as soon as possible because a malware infection can severely damage your data. It showed its existence in the year 1986 when the first computer virus was created by the name of Brain for MS-DOS operating systems. Mainly a boot sector Virus, it spreads through floppy disks. Nowadays, there are several types of malicious software, which are developed using advanced coding technology.

- **Types of PC Virus**

Although there are thousands of infectious programs that can affect your PC, these are categorized on the basis of their infection targets.

1. **Boot Sector Virus**

Boot Sector Virus infects the Master Boot Record (MBR) of hard disks. Some virus also infects the boot sector of hard drives. It spreads via external sources, for example, an infected floppy disk or USB drive.

2. **Macro Virus**

A macro virus usually targets Microsoft Word, Microsoft Outlook, and similar applications. The piece of the virus is embedded in documents or emails. And you accidentally open the file, the virus gets activated and can spread to other files and folders.

3. **Email Virus**

Email Virus uses email medium to spread and infect PCs. These types of malware come hidden in email attachments and execute as soon as you download or open the attachment.

- **How do Computer Viruses Spread?**

A computer virus may spread if any external virus infected hard drive is inserted into your PC. These removable devices can be a pen drive, an external hard disk or a floppy drive. Apart from external hard drives, it spreads via email attachments, which can easily carry malware. Your computer can also get infected if you download software, movies, songs, etc. from untrusted websites.

- **Symptoms of Computer Virus Infection**

You can easily identify the symptoms of computer virus infection. One major indication is that your PC getting extremely slow. Another symptom can be your existing firewall protection getting disabled. You will also experience frequent crashes of applications running on your PC. Other alerts can be hard drive malfunction, error messages & pop-ups.

- **How to Prevent Viruses?**

In order to prevent viruses from infecting your computer, you must follow certain best practices such as:

- Do not insert removable devices/USB devices without scanning using a virus scanner
- Abstain from downloading software from untrusted websites
- Don't open email attachments without verifying the sender id, content, and purpose
- Use a premium antivirus software rather than free software as those may not be capable of providing 100% protection.

- **How to Remove a Virus?**

In order to eliminate the possibility of infection on your device, you need to first delete all temporary files to speed up the virus scan process. Once you have deleted the temp files, scan your PC using an antivirus software. You can use REVE Antivirus, which scans computer threats using the turbo scan technology. This results in quick virus detection and removal. After the removal of malicious code or infectious files from your computer, always keep your antivirus software updated, so that any kind of latest threat can be detected.

2. Computer Crimes

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company or a nation's security and financial health.

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

Classifications of Computer crime

- **Computer crime encompasses a broad range of activities.**
    1. Financial fraud crimes
    2. Cyberterrorism
    3. Cyberextortion
    4. Cybersex trafficking
    5. Cyberwarfare
    6. Computer as a target
    7. Computer as a tool
    8. Obscene or offensive content
    9. Online harassment
    10. Drug trafficking

- **Combating computer crime**
    1. Investigation
    2. Prevention
    3. Legislation
    4. Awareness
    5. Intelligence