I S LITERACY, LEARNING AND LESSON

January 2020

Different Types of Malware Attack and How to Avoid them

Malware, is a malicious software which is basically designated to damage, impair, or exploit computers or computer systems.

1. **Trojan Horses** - In this, the attackers pretend this malware as something beneficial, such as a specific offer or present, to infiltrate a computer system so that people would enter it without any hesitation. It steals sensitive data, crashes your device, and takes your personal information like payment card information.

Prevention - A Trojan Horse can only enter a system if the user gives permission. Therefore it applies false information in downloads during the agreement section. Thus you should use discretion to withdraw accidental downloading, for example, which could really harm your computer or PC.

2. **Worms** - It is like a virus in the way which can reproduce itself to affect other computer systems. But, not similar to a virus, a worm doesn't require to be connected to a current program or be provoked to perform as we know that a virus needs human interference to enter a file, attachment, or website link while a worm can attach to file by itself and self-grow.

Prevention - Its prevention is quite complex, but the fact is that you can simply make your PC secure by activating the firewall.

3. **Adware** - It is one of the types of malware attack that automatically passes notifications to a user to create wealth for its producer. Adware is mainly used in conjunction with spyware. Thus it can be done with the help of pop-up internet ads or ads inserted in the interface of a program.

Prevention - By observing the locations from where they are downloading the details because the unknown websites are general territories for adware.

4. **Cryptojacking** - it is basically a type of malware that utilizes a victim's computing capability to pit for cryptocurrency.

Prevention - By installing an ad-blocking or anti-crypto mining extensions on your web browsers.

5. **Spyware** - It is accurately what you would imagine this malware intended to spy on and all collect information about the user. It can be practiced to follow and monitor internet activity, find and obtain delicate information, and log keystrokes.

Prevention - There is a pop-up window that can incorporate spyware just by agreeing on the link or window, or by unintentionally installing spyware to the computer. Thus by withdrawing these links can stop an accidental download.

6. **Ransomware** - **I**t can stop users from entering into system or data, and also delete or distribute data if a payment is not paid.

Prevention - An affected system cannot negotiate data that has remained backed up offline. Therefore, users who encounter a ransomware attack will have a whole unharmed backup of their files, and will not be required to pay the ransom to gain access to their data.

7. **Malvertising** - It is a grip of the malicious advertising, and it is the use of advertising to develop malware.

Prevention - You can prevent this malware by installing antivirus tools so that you can keep all software updated from time to time, consisting of the operating system, browsers, Java, and Adobe Flash.

8. **Bots and Botnets** - It is basically a computer that is contaminated with malware that enables it to be remotely managed by an attacker.

Prevention - There are several things to consider such as Anti-Botnet tools, Software patches, Network monitoring, and user awareness.