

Computer Virus and Worm

Computer Virus and Worm

Computer virus is one of the most common type of malicious code. It attaches itself to another data file or program, propagates itself when that program is executed and causes damage to computers.

Computer worm is another common type of malicious code. Unlike virus, it is a self-replicating program that does not need to attach to a host program/file. It can spread through connected systems and consume resources of affected computers or cause other damages.

Computer worm may, without a user's knowledge or consent, automatically spread to other computer devices (such as mobile phones or PDA) through different channels. Spreading channels include email, instant messaging, MMS, Bluetooth etc.

Since the symptoms of infection and preventive measures of computer virus and worm are similar, computer virus will be used as an example for illustration in the following.

Causes of Infection

Under what circumstances may your computer be infected by computer virus?

- Installing or opening a file or an attachment of a spam email from an untrusted source;
- Visiting a malicious website, such as a fraudulent website;

Infection Symptoms

If your computer is infected by computer virus, the following symptoms may appear:

- Cannot run an anti-virus software or update the definition file of the anti-virus software;

- Degradation of computer performance;
- Reduction on available system memory or disk space;
- Unknown or newly created files, programs or processes appear on the computer;
- Abnormal restarts or shutdowns of the computer.

Preventive Measures

In the daily use of computer, you should:

- Install anti-virus software or anti-malicious code software with the latest virus definition files. Enable the real time detection feature and schedule a weekly full scan.
- Install and enable a personal firewall.
- Install the latest security patches.
- Enable the automatic updating feature for downloading and installing the latest security patches and malicious code definition files.
- Backup your programs and data regularly.
- Perform virus scan on portable electronic devices before use.

Relying only on technical measures are not enough to protect your computer. Remember:

- Do not visit or download software from suspicious or untrusted websites.
- Do not install software from a dubious source.
- Do not open any unknown emails or instant messages or their attachments, etc.

To learn more about information security, please visit the InfoSec website at:
<http://www.infosec.gov.hk>