

Spyware and Adware

Spyware and Adware

Spyware is a type of malicious code. When spyware is installed on a computer, it will forward the user's computer files, information of online activities or even keystrokes to a third party without the user's knowledge and consent.

Adware or Advertising-supported software is a software program attaching with advertisements. It downloads and displays advertisements on screen automatically while a program is running. Some types of adware are also spyware that possesses spyware features.

Causes of Infection

Under what circumstances may spyware or adware be installed on your computer?

- Download or install software from suspicious sources such as websites, peer-to-peer (P2P) network etc. Spyware or adware may have been embedded into the software secretly.
- Some adware programs even install on computers automatically and secretly without notifying users.

Symptoms of Infection

If adware has been installed on your computer, the following changes may occur:

- The default start page of the web browser is replaced by another website. You cannot change this default start page using the standard way of setting up the browser.
- New items are added to the "My Favorite" folder.
- New software components, such as browser toolbars, are installed on browsers.
- Pop-up windows with advertisements are displayed on the screen even if

your browser is not running or the system is not connected to the Internet.

Potential Threats

If spyware or adware is installed on your computer, what information security threats are you facing?

- After installing adware, advertisements, which are displayed automatically on the screen, can make you feel annoyed.
- Spyware can steal and collect computer data and personal information, such as email address, name and credit card number etc, and secretly forward the collected information to the third parties. The collected information may then be sold or used for marketing purpose and other illegal means.
- Based on the information collected, intruders may find loopholes in your computer. It allows intruders to install malicious code like Trojan horse to attack or take control of your computer to perform illegal activities.

Preventive Measures

To protect a computer against the threats of spyware and adware, you should take appropriate preventive measures, including:

- Do not download or install software from suspicious sources such as websites, P2P network etc.
- Read the terms and conditions of use before downloading and installing a legitimate piece of software, because they may require you to accept the installation of other data collection programs.
- Read the terms of use carefully when you visit websites that require you to install a plug-in or use active content.
- Delete the web browsing history in the browser.

Furthermore, your computer must adopt basic security measures, including:

- Install anti-malicious code software, such as anti-spyware software, with the latest malicious code definition files. Activate the real-time detection function of the software and schedule a full scan on the computer at least once a week.
- Install and activate a personal firewall.
- Install the latest security patches.
- Enable the Auto Update features of downloading and install the latest malicious code definition files and security patches.

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