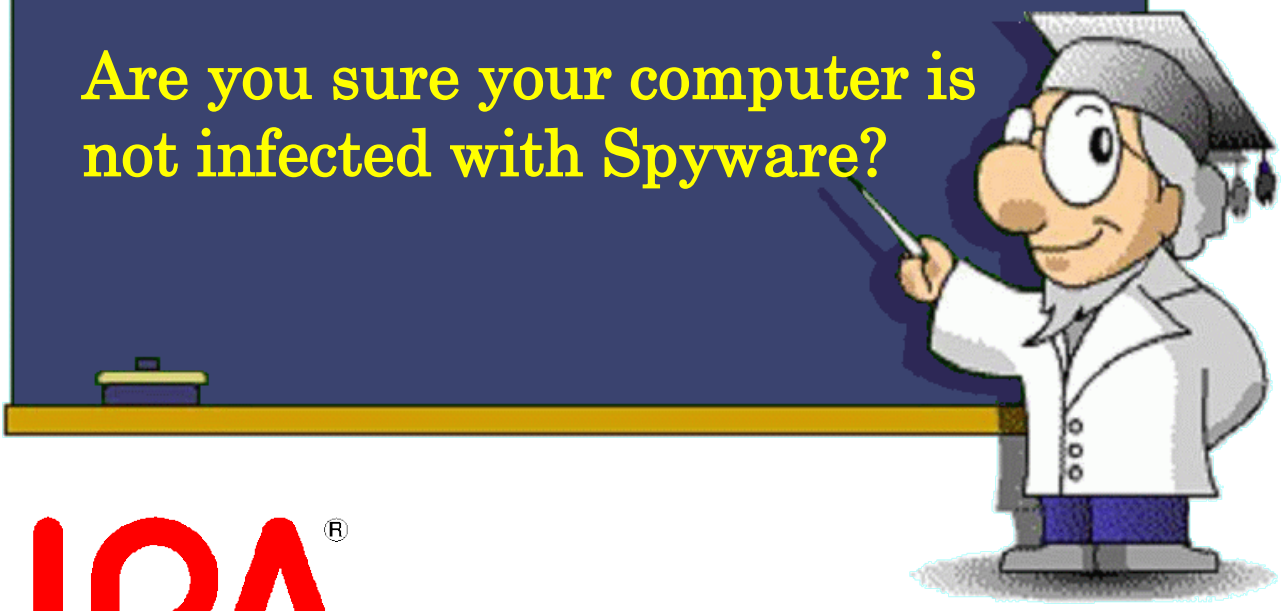
IPA Countemeasure Guide Series (2)

Countermeasures against Spyware

Are you sure your computer is not infected with Spyware?

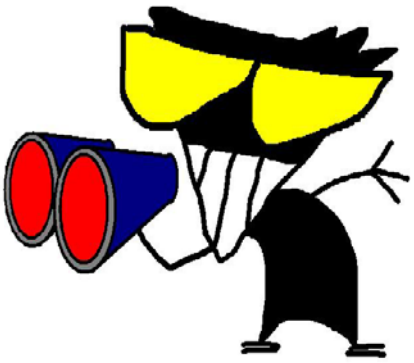


IPA®

Information-technology Promotion Agency
IT Security Center
http://www.ipa.go.jp/security/

1. What is a Spyware?

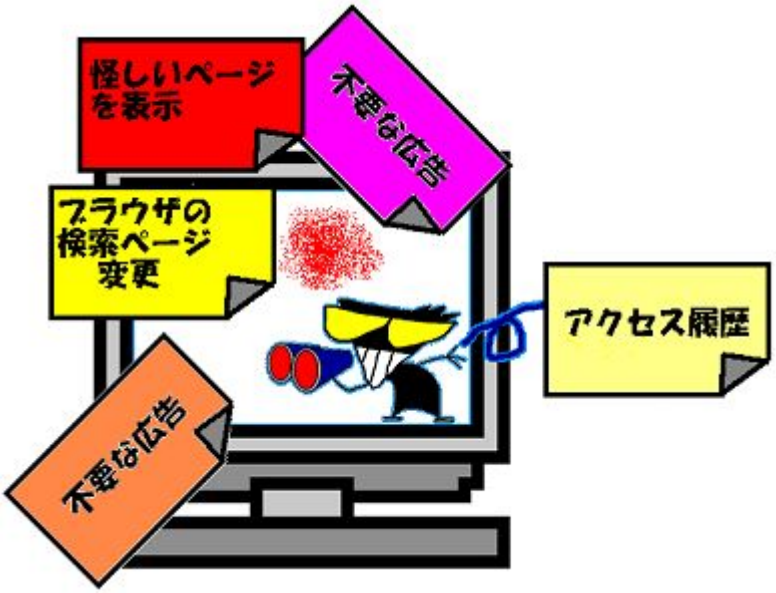
Definitions



Spyware is “a program designed to illicitly collect users’ important information (such as personal data, access logs, etc), which is installed (or embedded) without the consent of users and administrators.”
[The above definition was introduced by the Working Group for the Development of Spyware Prevention Measures that was set up jointly by Information-technology Promotion Agency (IPA) and Japan Network Security Association (JNSA).]

Spyware currently spreading across a wide area has the following functions: collecting information and saving it in a file, automatically transferring such information to external users (other than legitimate users.) W32/Antinny virus is also a Spyware that compromises information using file-swapping software.

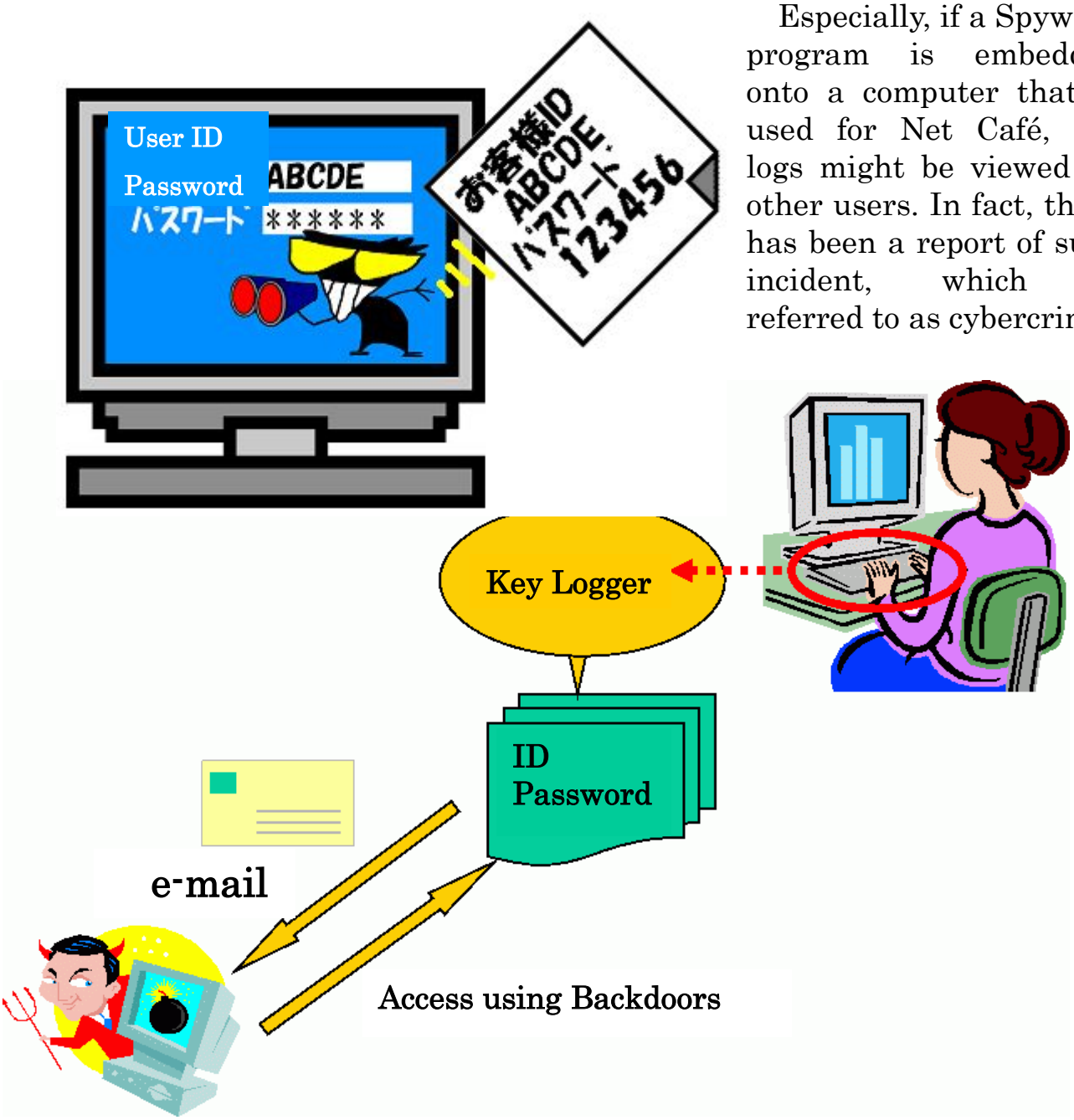
Another program called “Hijacker”, which takes over the control of a web browser and induces users to a malicious site or displays unexpected search results, can also be categorized as Spyware because it collects information and performs such malicious tasks.



However, not all programs capable of gathering information are Spyware.

For example, “Key Logger”, a program that logs key-inputs for a system operation test or automatic execution, can serve as a useful tool, as long as users utilize it in a legitimate manner. However, if other functions such as data transmission, backdoors, and remote access are added to this program, it might become a Spyware.

Especially, if a Spyware program is embedded onto a computer that is used for Net Café, the logs might be viewed by other users. In fact, there has been a report of such incident, which is referred to as cybercrime.



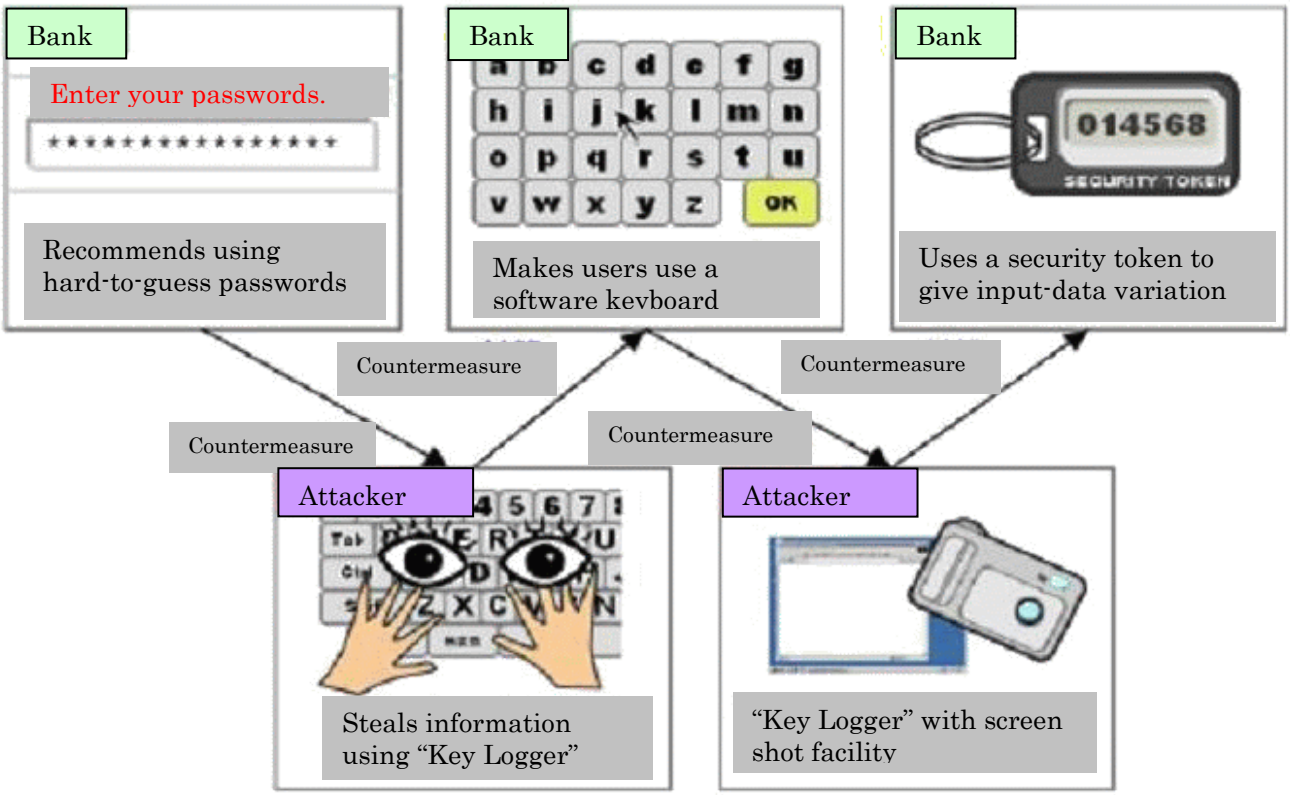
There are cases where system management programs used within enterprises are recognized as Spyware by anti-Spyware software.

Furthermore, due to different points of view between the supplier and clients, a software program designed to improve the convenience of the Internet might be regarded as Spyware by the clients. In most cases, the problem lies in their inability to distinguish Spyware from Adware (*1), a program designed to display advertising information.

Remember that the term “Spyware” is ambiguous. Even if a number of Spywares programs are detected by Antivirus software, you don’t need to be panic. Not all of them are created to compromise information. Just like removing things you don’t want, clean the viruses.

Reference:

Spyware (Key Logger) evolves … Banks versus Attackers.

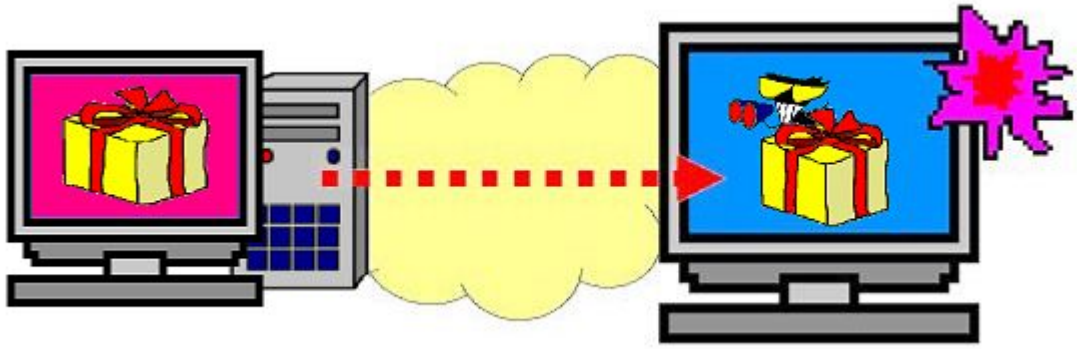


Source: IT Security White Paper 2006
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

2. How do they enter your system?

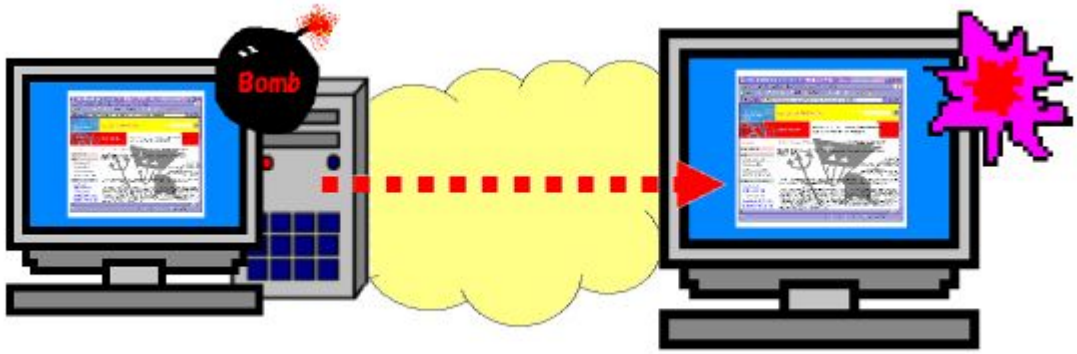
In most cases, Spyware is installed without users' knowledge. Some time, it is contained in a computer virus/Worm and transmitted.

1) **Spyware can be installed onto your PC by carelessly downloading (*2) or installing (*3) programs (such as free software, shareware, free tools that claim to be convenient etc) from a Web site or external media.**



There are cases where files downloaded from Web sites are Spyware. Read carefully the license agreements displayed when downloading or installing software programs, and do not apply them unless you think they are really necessary. If needed, scan the downloaded files for viruses before installing them.

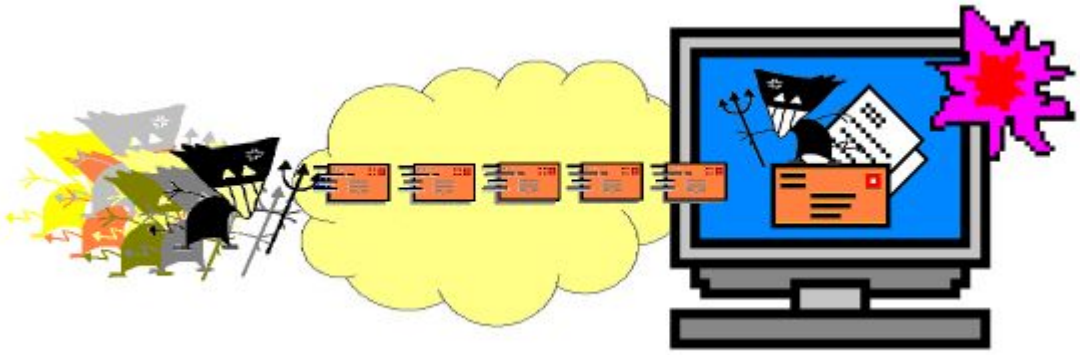
2) **Infected by accessing a Web page (containing a malicious script)**
3) **Infected by clicking a link (URL) presented in a Spam mail message, which takes users to a malicious Web site**



You might be taken to a Spyware-embedded site by clicking a link provided in an email message or on the electronic bulletin board. So you must be careful not to click any unnecessary links, which could allow the malicious program to be installed.

2) and 3) are the cases where vulnerabilities or improper security settings are exploited to compromise the systems. Do not access any Web sites that you think are illegal or suspicious, and be sure to apply security patches by using the Windows Update to mitigate the vulnerabilities and enhance the security level of your Web browser. This is a very important measure.

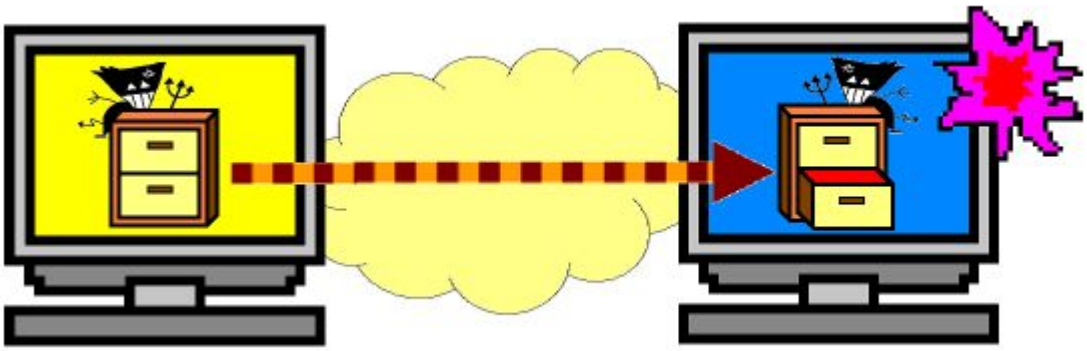
4) Infected by opening a file attached to a virus mail



5) Entering through P2P file-swapping software

There are cases where a computer virus or Spyware is contained in a file downloaded using file-swapping software. To avoid this, be sure to scan for viruses each time you download a file.

Note, however, that a virus like “W32/Antinny”, which is transmitted via the file-swapping software “Winny”, is mainly detected in Japan and other Asian countries, and therefore, it might not be detected by free antivirus software produced in other areas.



3. Five Codes for Spyware Prevention Measures for PC Users

As in the case of computer viruses, countermeasures should be taken against Spyware. It is too easy to think that single measure is enough. We recommend implementing the following five steps (plus supplemental point), because such multiple defenses are required to protect against Spyware and unauthorized access.

(1) Use anti-Spyware software, keep virus definition files updated, and scan your system for Spyware
(2) Keep your computer up-to-date
(3) Be careful about suspicious sites and emails
(4) Enhance the security level of your computer
(5) In case of emergency, back up important files

Supplemental point:
Do not input personal information on any computer that is not under your control.

(1) Use anti-Spyware software, keep virus definition files updated, and scan your system for Spyware

By using anti-Spyware software or antivirus software, you can prevent Spyware from being installed and executed. Note, however, that the software and its definition files should be kept up-to-date.

If any software (or part of the program) installed intentionally by a user is regarded as Spyware, he (or she) needs to remove it by himself, which means that such software should be used at the user's own risk.

Most of the recent antivirus software products are capable of detecting Spyware. However, not all Spyware can be detected and removed by these products. Although vendors of antivirus software and Anti-Spyware are striving to develop new detection methods and improve their programs in an attempt to deal with even unknown viruses (or Spyware), there is nothing perfect in this world; you should not rely too much on these products.

(2) Keep your computer up-to-date

The existence of a Spyware program entering computers by exploiting vulnerabilities (security holes) has been disclosed. To mitigate vulnerabilities, it is important to keep your computer up-to-date.

Vulnerabilities can exist in not only the operating systems that are primary software programs, but other applications.

Windows users are highly recommended to periodically perform the Windows Update or Microsoft Update. For those using other operation systems or software products, it is recommended to refer to the information publicized by the vendors or other sources, and take necessary steps against any vulnerability detected.

- Windows Update (Microsoft)
  http://windowsupdate.microsoft.com

(3) Be careful about suspicious sites and emails

- **Web Site Access**

Your computer might be infected with Spyware only by browsing a Web site containing a malicious script.

Do not access any suspicious sites that are retrieved by search engines, provided in Spam mail messages, or displayed on pop-up windows. If necessary, tighten up the security settings on your Web browser.

- **Downloading Convenient Tools**

If you want to download Shareware or Freeware from a Web site, make sure that the site is secure. Similarly, be careful with software programs obtained through P2P file-swapping software. Before using or installing such programs, do not forget to scan them for viruses, using anti-Spyware software or antivirus software.

- **Suspicious Mail**

As in the case of virus mails, Spyware can be installed by opening a file attached to an email, or visiting a Web site whose URL is presented in an email message.

Bear in mind the following points:

- **Do not open any files attached to a suspicious email.**
- **Do not access any links presented in a suspicious mail message.**

Note: the following file extensions (the last three characters of a file name) are often used for a malicious program: “exe”, “pif”, and “scr”, etc. Attachment files having these extensions should be scanned for viruses.

- **Sudden Appearance of an Incomprehensible Pop-up Window and Confirmation Screen**

Clicking a button on an incomprehensible pop-up window or confirmation screen may result in the execution of embedded malicious code. If you are suspicious about the messages, close the window (or screen) by clicking the X button on the upper right corner, which is equivalent to pressing the ALT and F4 keys.

Be sure to close the following windows (or screens) by clicking the X button on the upper right corner:

- Incomprehensible pop-up window
- Incomprehensible confirmation screen

- 0

Bogus Anti-Spyware

Among the increasing Spyware incidents, there are incidents caused by a bogus Anti-Spyware. This kind of software behaves as if it were a legitimate Anti-Spyware, but in fact, it contains Adware or Troyjans; it displays messages indicating that your computer is infected with a Spyware, and then recommends that you purchase a specific product to remove the malicious software.

It is highly likely that Anti-Spyware scanning your computer without your consent is a bogus one. You should not believe any suspicious warning messages.

Free-online-services to detect and remove Spyware and viruses are available from the Web sites of the venders listed in the Reference section. Use them to scan your computer (or remove such malicious programs) if necessary.

(4) Enhance the security level of your computer

- **Use a Personal Firewall**

Spyware can be installed by an external source hacking into your computer systems. If configured properly, Firewall can prevent it. Depending on the firewall, data transmitted from an already installed Spyware can be blocked (using functions such as Application Firewall.)

Note: the Windows Firewall supplied with routers or Windows XP cannot prevent Spyware from transmitting data to external devices.

- **Change Your Browser's Security Settings**

When surfing the Internet, it is recommended to change the default security settings on your browser. For example, if you are going to access suspicious Web sites mentioned earlier, set the security level to "High". Regardless of users' consent, malicious ActiveX or scripts install Spyware programs onto their computer.

If you are using Windows Internet Explorer, set its security level to medium or higher (by selecting [Tools] > [Internet Options] and clicking the [Security] tab.)

As for Cookies (*4) that are often associated with Spyware, set the privacy level to medium or higher (by selecting [Tools] > [Internet Options] and clicking the [privacy] tab.)

- **Ensure the Security with Internet Explorer (Microsoft)**
  http://www.microsoft.com/windows/ie_intl/ja/using/howto/security/settings.mspx

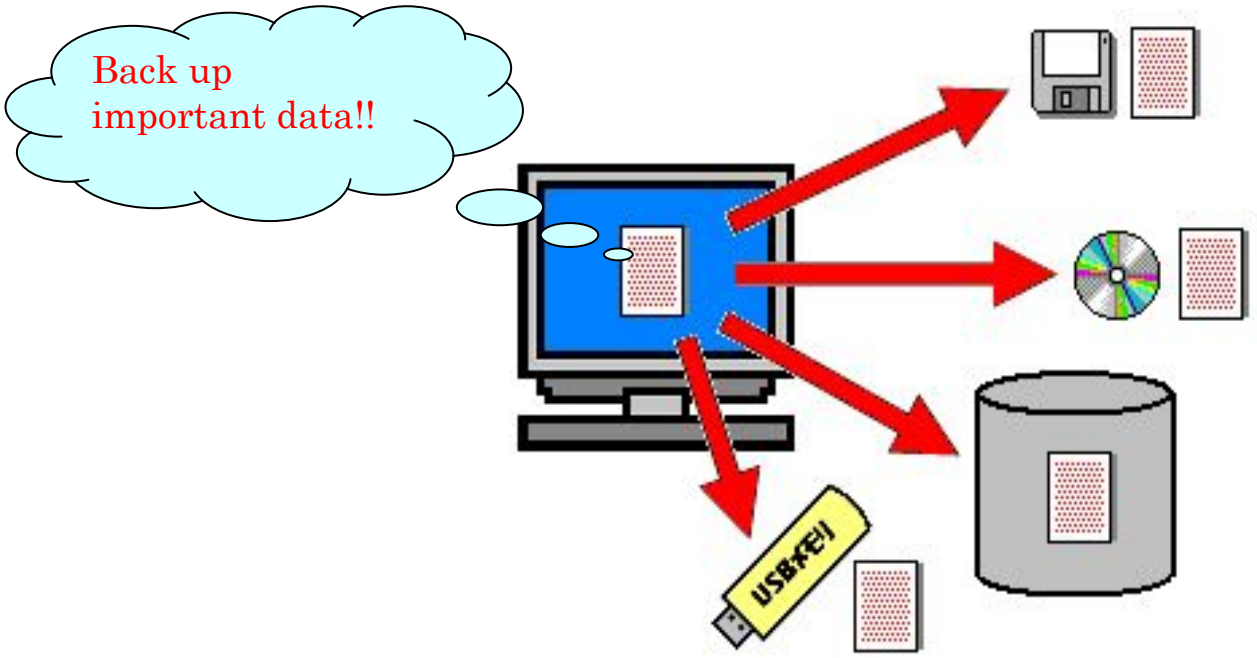
- **If Not Necessary, Do Not Use the Administrator Mode (*5)**

If a malicious program is executed while (you are) in the administrator mode, entire control of the computer might be taken over. Do not use the administrator mode unless it is really necessary.

(5) In case of emergency, back up important files

In any case, to restore the healthy state of your computer, you might have to initialize your system. Considering this, it is important to backup important files on a regular basis.

If a malicious program has already been installed or the system has been modified by an attacker, you may have no choice but to initialize the hard drive. It is recommended to back up data on a regular basis. In addition, keep in a safe place the original CD-ROMs of application software. Should any of the system programs be modified, you can re-install it using the original CD-ROM.



(Supplemental point) Do not input personal information on any computer that is not under your control.

It is recommended not to input personal information (such as bank account numbers, card information, etc) on any computer that is not under your control, including the computers used for Net Café that can be accessed by any number of users. Be careful not to become a victim of a crime.

4. References

- Cautions to Prevent Damage Caused by Spyware (Japanese only)
  http://www.ipa.go.jp/security/topics/170720_spyware.html

- Anti-Spyware (Microsoft)
  http://www.microsoft.com/athome/security/computer/spyware/protectyourcomputer_spyware.mspx

- Internet Security Knowledge, Spyware Features (Trendmicro) (Japanese only)
  http://is702.jp/special/spyware/

- Symantec
  http://www.symantec.com/

- McAfee
  http://www.mcafee.com/us/

- Spyware Research Center (Ahkun) (Japanese only)
  http://www.ahkun.jp/researchcenter/SpywareResearchCenter.html

- Spyware Guide (Next Technology Ltd.)
  http://www.spywareguide.com/

- CA nospy (Japan CA) (Japanese only)
  http://www.nospy.jp/

- Panda Software Japan
  http://www.pandasoftware.com/

- webroot
  http://www.webroot.com/
  http://www.webroot.com/consumer/products/spysweeper/freescan.html

5. Terminology

(*1) Adware

A software that displays advertising messages on users' browsers. Users can use it for free as its purpose is to advertise something for sale. Some Adwares steal users' information (such as computer environment, Web access logs) and transfer it to an external source; this is why Adware is considered to be a classic Spyware.

(*2) Downloading

Transferring data from a Web site to a client's computer.

(*3) Installing

Loading software into a client's computer system. This enables users to use the software.

(*4) Cookie

A piece of information (such as user information, access information, etc) sent to a browser by a Web server.

(*5) Administrator Mode

Computer operating systems provide a facility for setting privileges for each user. Administrator mode is a privileged mode that enables users to do whatever they want on the computer, including modifying important settings. Another mode called "user mode" is available to general users, in which they can perform general operations but cannot change settings that affect how the computer operates. For more details, please refer to your computer manual.

IPA Countermeasure Guides Series

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA Countermeasure Guide (1) Countermeasures against Virus
- **IPA Countermeasure Guide (2) Countermeasures against Spyware**
- IPA Countermeasure Guide (3) Countermeasures against Bots
- IPA Countermeasure Guide (4) Countermeasures against Unauthorized Access
- IPA Countermeasure Guide (5) Countermeasures against Information Leakage

---

We enlisted cooperation from the following organizations in creating and publishing this guide.

- Japan Network Security Association (JNSA)
  Spyware Countermeasure Development Working Group
  http://www.jnsa.org/
  http://www.jnsa.org/spyware/

- Japan Complex Café Association (JCCA)
  http://www.jcca.ne.jp/

IPA®
Information-technology Promotion Agency
IT Security Center
2-28-8, Honkomagome, Bunkyo, Tokyo, 113-6591 Japan
TEL 81-(0)3-5978-7508
FAX 81-(0)3-5978-7518
E-mail virus@ipa.go.jp (Virus) crack@ipa.go.jp (Hacking)
URL http://www.ipa.go.jp/security/

Issued June 1, 2007 Issue No.6