Computer Security Fundamental

Know thy enemy and thyself,
then you will be able to defend.

Why should we keep security?

- There are many important and useful things in computer. So bad person tries to attack computer actively.
- If your computer gets “virus” because of no security, your computer also starts to attack other computers.

⇩

No security make you a person of fault!

Typical security attack: Virus

- Virus is a bad program which goes into computer without user’s permission.
  (Trojan and worm are also kinds of virus.)
- If virus come into a computer,
  it destroys programs, documents, and so on.
  Then at last, the computer is going to destroy.
- Virus can copy itself and spread to other computers via floppy disk, flash memory, pirate software, e-mail, website, network...
- You can get detailed information below.
  http://www.microsoft.com/protect/computer/basics/virus.mspx

Typical security attack: Spyware

- Spyware is a bad program which goes into computer without user’s permission also like virus.
- If spyware come into a computer,
  it brings secret information outside.
  For example, username, password, mail address...
  Bad person can cheat with these information.
- Spyware comes form same routes as virus.
  However, it is difficult to find
  because spyware does not produce strong symptoms.
- You can get detailed information below.
  http://www.microsoft.com/protect/computer/basics/spyware.mspx

Typical security attack: Cracking

- Cracking is a computer attack
  which is done by bad ICT technician (cracker).
- If there are some problems in network or security, computer may catch cracking via internet.
- When a computer is defeated by cracking,
  the computer allows all operations for cracker.
- You can get detailed information below.
  http://kb.iu.edu/data/agwt.html

Symptoms from security attacks

- When a computer is damaged by security attacks, some of following symptoms appear in the computer.
- If your computer shows the symptoms, you must take action against the attacks.

Slowing computer operation speed	Losing mouse and keyboard control
Repeating login and restart	Collapsing displayed object
Coming music and sound suddenly	Appearing strange message and graphic
Destroying program and document	Disappearing program and document
Going internet and printing impossible	Sending virus attached mail in secret
Increasing file-size automatically	Shrinking available memory

Actions against security attacks

- You can take following actions against security attacks.
  According to your computer environment,
  it is impossible to take all the actions.
  However, you should do as much as possible.
  - Applying security tools
    - Anti-virus, anti-spyware, firewall, root-kit scanner...
  - Keeping low-risk operations
    - Showing file extension, displaying hidden files,
      ignoring unnecessary files, killing auto-play function,
      avoiding underground website, selecting low-risk file types...
  - Replacing fragile software with secure software
    - OpenOffice.Org, Linux...

Basic security tool: Anti-virus

- Anti-virus is a program which stays in computer
  for preventing, detecting and removing virus.
- You must apply an anti-virus
  because there are very huge viruses in this country.
- However, if there are multi anti-viruses in a computer,
  the computer gets troubles by conflict of anti-viruses.
- When anti-virus is running,
  computer operation speed is slowing.
- You can get a free anti-virus below.
  http://free.grisoft.com/doc/download-free-anti-virus/us/frt/0/

Basic security tool: Anti-spyware

- Anti-spyware is a program which stays in computer for preventing, detecting and removing spyware.
- You should apply an anti-spyware because there are huge spyware in this country.
- However, if there are multi anti-spyware in a computer, the computer gets troubles by conflict of anti-spyware
- When anti-spyware is running, computer operation speed is slowing.
- You can get a free anti-spyware below.
  http://www.safer-networking.org/en/spybotsd/

Basic security tool: Firewall

- Firewall is a program which stays in computer for preventing cracking.
- You should apply a firewall.
  If not, your computer may become a target of cracking.
- Windows has a firewall, but its function is very cheep.
  So it is better to get and apply other firewall.
- You can get a free firewall below.
  http://www.zonealarm.com/store/content/catalog/products/sku_list_za.jsp

Security tool: Root-kit scanner

- Root-kit scanner is a program which is used
  for detecting security attacks including cracking.
- When you use root-kit scanner,
  it shows system information in detail.
  Then you can find and kill security attacks manually.
- Root-kit scanner is a very strong security tool.
  However, it is difficult to use effectively
  because you have to identify what is security attack.
- You can get a free root-kit scanner below.
  http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis/

Low-risk Operation: Showing file extension

- Normally, Windows hide “file extension” which is ending part of file name.
- Virus and spyware have a fixed file extension. So if you change Windows setting to show file extension, you can identify what file is a virus or a spyware.
- File extensions for virus and spyware are following.
  - .EXE, .COM, .BAT, .CMD, .PIF, .SCR, .VBS, .HTML, .VBE, .JS, .JSE, .WSF, .WSH, .ZIP, .LZH, .RAR, .CAB
- Files which have these extensions are virus or spyware perhaps.
- You can change that setting from “folder option” like below. http://www.fileinfo.net/help/windows-show-extensions.html

Low-risk Operation:
Displaying hidden files

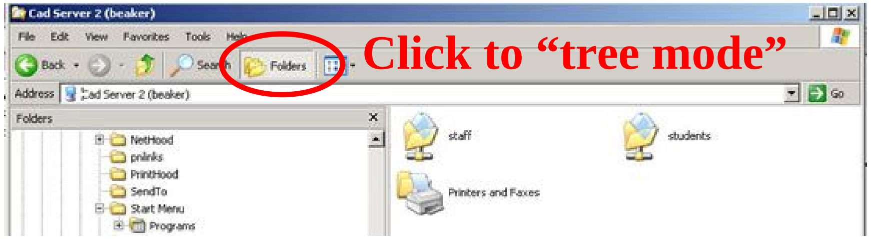
- Normally, Windows system files are invisible because of preventing miss operation by user.
- However, virus and spyware also use this function to hide themselves.
- So it is better to change Windows setting to display system files, and you can easily find virus and spyware.
- You can change that setting from “folder option” like below.
  http://www.winxptutor.com/showallfiles.htm

Low-risk Operation:
Ignoring unnecessary files

- When you get a file from internet, e-mail, pirated CD, you should not open the file before checking with anti-virus and anti-spyware.
- Especially, it is very dangerous if the file has following file extension.
  - .EXE, .COM, .BAT, .CMD, .PIF, .SCR, .VBS, .HTML, .VBE, .JS, .JSE, .WSF, .WSH, .ZIP, .LZH, .RAR, .CAB
- In case the file is not very important for you, it's better to ignore it.
  The wise man keeps away from danger.

Low-risk Operation:
Killing auto-run function

- When you insert flash memory, CD, floppy disk into a computer, Windows runs program automatically.
- Some of virus and spyware use that auto-run function to spread themselves.
- So it is better to kill auto-run function for preventing virus and spyware.
- You can kill auto-run function with pressing “Shift-key” when you insert a storage media into a computer then please use explorer as “tree mode”.



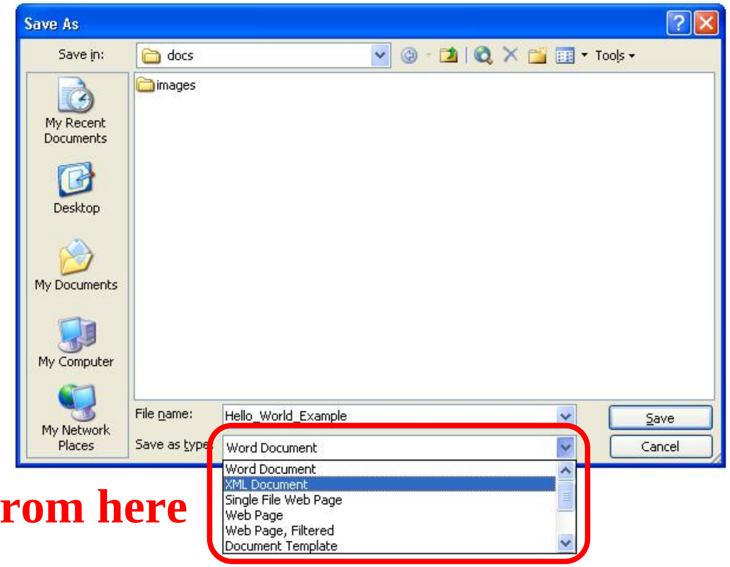
Click to “tree mode”

Low-risk Operation:
Avoiding underground website

- There are many security traps in underground website like porn site, game site, file sharing site...
- So you should not visit underground website.
  Visiting underground website means
  almost welcoming security attacks.
  The wise man keeps away from danger.

Low-risk Operation:
Selecting low-risk file types

- Microsoft Office makes easily virus infected file like .doc, .xls, .ppt, .mdb at default setting.
- So it is better to select a file type except above for keeping your documents from virus when you save them.



Save in: docs

File name: Hello_World_Example

Save as type: Word Document

Select a file type from here

Secure software: OpenOffice.Org

- OpenOffice.Org is a software like Microsoft Office.
  You can read and edit your documents
  made by Microsoft Office from OpenOffice.Org.
- Using OpenOffice.Org is secure
  because it does not make easily virus infected file
  at default setting.
- It is better to replace Microsoft Office
  with OpenOffice.Org.
- You can get the OpenOffice.Org below.
  http://www.openoffice.org/

Secure software: Linux

- Linux is a operating system like Windows. However, Linux has very less problems in security than Windows.
- Almost all virus and spyware are made for Windows. That virus and spyware can not attack against Linux.
- Linux is very secure by the reasons above.
- It is better to replace Windows with Linux.
- You can get a Linux for beginner below.
  http://puppylinux.com/

On-going security update

- Security attacks become strong day by day. So effect of security tools is going weak especially for anti-virus and anti-spyware.
- You should update security tools to enhance again and again, or you may lose computer security.
- Almost all security tools have a function of auto-update via internet, and you should enable it.

Healing chronic symptoms

- You can not heal all symptoms from security attacks though you remove the attacks completely.
- Some of symptoms are only healed by manual,
  so it is difficult and has a possibility of failure.
- This document will shows manual ways following
  to heal symptoms, but you should take effort more
  to keep your computer security than to heal symptoms.
  - Deleting garbage
  - Recovering setting and registry
  - Reinstall program and OS

Healing way: Deleting garbage

- Sometimes, virus and spyware leave garbage files.
- Those garbage files do not throw damage for computer but it is possible to shorten available hard disk capacity.
- So it is better to find and delete those files.

Healing way: Recovering setting

- Sometimes, virus and spyware change settings of programs and hardware without user’s permission.
- If you find places of changed,
  you should take back to original settings.
- However, every way of taking back is deferent
  by each programs and hardware.
  So it is trouble some to take back.

Healing way: Recovering registry

- Sometimes, virus and spyware change settings of Windows without user's permission.
- Windows settings is written on special files which is called "registry".
- If you want to edit registry for taking back settings, you should use "regedit" registry editor.
- However, that editor is very difficult to use and it is possible to destroy Windows.
- You can get detailed information below.
  http://en.wikipedia.org/wiki/Windows_Registry

Healing way: Reinstalling program

- Sometimes, virus and spyware break programs without user’s permission.
- In this case, it is an only alternative to install the programs again.

Healing way: Reinstalling OS

- Sometimes, virus and spyware break Windows without user's permission.
- In this case, it is an only alternative
  to install the Windows again.
- Before installing windows again,
  you should copy important files to another place.
  (It is called "backup")