Enhance Fundamental IT Security

All of computers connected to the Internet are the targets of malicious people. Some people might say "I do not mind it even if my computer has been cracked and data breach has occurred; my data is not so valuable." However, the cracked computer can be abused by the attackers to relay their attacks, and you might face responsibility issues and some other difficulties. Therefore, all of us must enhance the security of our computers as well as smartphones.

Apply security updates immediately after the release

Make sure "Automatic update" feature is enabled in the security update tools of Operating System and Applications. When you see a pop-up of update, do not suspend it, and do it ***as soon as possible***. Microsoft provides comprehensive security updates every 2nd Tuesday @U.S. time zone (2nd Wednesday @ JST). Please never forget such regular updates as well.

Do not use End-of-Support software, devices, etc.

Do not use End-of-Support software (OS, applications, etc.) or End-of-Support devices. If you must use it, do not connect to the network and use it standalone. Even in a stand-alone environment, be sure to regularly scan with the latest antivirus software using specific tools[1]. When exchanging data with a PC in a stand-alone environment, prepare a dedicated medium for data exchange (USB memory, external HDD, etc.). Before opening a file obtained from a PC in a stand-alone environment, be sure to perform a virus check on another PC connected to the Internet.

Keep anti-virus software as latest version

When did you perform version upgrade of "ウイルスバスタークラウド" or its English Edition "Trend Micro Internet Security?" Version upgrade is different from daily automated updates of virus-pattern files; ***version upgrade is not performed automatically by itself.*** Trend Micro offers a new version every year, and the support of old versions terminates in 2 years from its initial release. After the support period, you can no longer expect virus protection by the obsolete version. Check the version of your "ウイルスバスタークラウド" now. If it is not the latest version, perform version upgrade as soon as possible[2]. And be sure to perform version upgrade at least once a year.

(Continued on the back.)

[1] For example, there is a product called "Portable Security" by Trend Micro. Lending is available in the Computer Center.
(URL as of the end of March 2020, Japanese only)
https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint/portable-security-2.html

[2] For the version and the end of support date about the "ウイルスバスタークラウド", refer to the following URL. (Japanese only)
https://helpcenter.trendmicro.com/ja-jp/article/TMKA-01074

Do not open attachment files/URLs of suspicious E-mails.

You might receive hoax E-mails titled, say, “Alert from mail server administrator”, “Notice to appear in court”, etc. They usually have something illogical or strange. For example, sender's E-mail address may tell you something is wrong. Receiving an E-mail from "the Administrator of University Network" and it's from someone@yahoo.com?
It's a fake.

When you receive such suspicious e-mails, never open the attachment files/URLs of the E-mails. They might contain viruses, and even the latest anti-virus software could fail to remove/quarantine it because virus evolution is very quick.

Manage Passwords with Strict Policy

In addition to your IIS user account, most of you may have other accounts for a wide variety of web services and so on (e.g. Google, Amazon). Please manage your passwords of your accounts with keeping strict policy.

- Use sufficiently complicated password (e.g. combine multiple words, partly replaced with numbers or symbols.)
- Do not use the same password for multiple accounts/services.
- Keep passwords secret. If you suspect someone else is aware of your password, change it immediately.

Take periodical backup of important files

“Ransom ware” is a type of malicious software, which encrypts your files suddenly and requests you a ransom for decryption key. Considering resilience in case of these attacks, you should take periodical backup of important files, and separate the backup storage device from the computer or keep it write-protected, so that you can recover the important files from the backup.

Computer Center
Institute of Industrial Science, the University of Tokyo.
April 1st, 2020