SAFE AND SECURE USE OF THE INFORMATION SYSTEMS

When using the information systems in the University of Tsukuba (networks, computers etc.), there are some guidelines you must follow. Before using these systems, you need to read the checklist below. If there are items that do not apply, please read the brochure carefully and follow the guidelines for using the information systems. For more details regarding this brochure, please go to: **https://oii.tsukuba.ac.jp/en/oii-security-2/details/** .

☑Check!

- □ **I never duplicate any copyrighted materials or make them available to a third party on the network.** (A revised copyright law took effect in October 2012 and a penalty was introduced for downloading digital audio or visual recordings which infringe copyright.)
- □ **I do not have any file exchange software program installed.**
  - Examples of file exchange programs: Xunlei, BitTorrent, µTorrent, LimeWire, Cabos, WinMX, Share, Winny, PerfectDark, etc.
- □ **I never download software programs of unknown origin.**
- □ **I regularly update Windows and use all software programs in their most recent version.**
- □ **I have installed an antivirus software program. In addition, I frequently update the virus definition files to protect the computer from viruses.**
- □ **I never give my password to anyone.**
- □ **I never use other people's passwords and user names.**
- □ **I have set up a password which is hard to break.**
- □ **I always manage personal information carefully and I always take measures to prevent information leakage.**
- □ **As a member of the University of Tsukuba, I act responsibly and ethically when posting information on social networking sites and the Internet in general.**
- □ **When I use the Internet, I pay close attention to fraud (phishing or one-click fraud).**
- □ **I am careful not to open suspicious e-mails.**

I never duplicate any copyrighted materials or make them available to a third party on the network. (A revised copyright law took effect in October 2012 and a penalty was introduced for downloading digital audio or visual recordings which infringe copyright.)

The purpose of the copyright law is "to provide for, and to secure protection of, the rights of authors, etc. and the rights neighboring thereto with respect" to "[copyrightable] works as well as performances, phonograms, broadcasts and wire-broadcasts, while giving due regard to the fair exploitation of these cultural products, and by doing so, to contribute to the development of culture." If you duplicate copyrighted works illegally and make them available to a third party without the author's permission, you are subject to punishment. You may also be punished for downloading digital audio or visual recordings when you are aware that they have been uploaded infringing copyright.

I do not have any file exchange software program installed.

Using file exchange software is very dangerous because some people distribute files with bad intentions. Moreover, the file you have downloaded is automatically uploaded for a third party. The University of Tsukuba forbids the use of any file exchange software program inside the campus network, including on the users' personally owned computers. There is a system in place that **blocks the use of file exchange software 24 hours a day** and if you violate these rules, you may be punished by the authorities of the university. However, if you have a legitimate reason to use a file exchange software program on campus, please contact us. (Our contact address is shown on the last page of this brochure.)

I never download software programs of unknown origin.

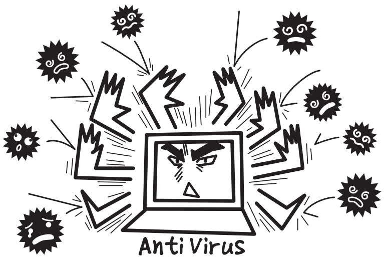
If you find a web page of unknown origin distributing expensive software programs free of charge or at low cost, do not download these programs. In many cases, these are distributed without permission. Besides infringing copyright, you risk infecting your computer with a virus, since the software may have been modified. There is a system in place that monitors downloading of software programs of unknown origin. If you download such programs, you may be punished by the authorities of the university.

I regularly update Windows and use all software programs in their most recent version.

Computer viruses can spread maliciously through the operating system (Microsoft Windows, macOS , etc) and can take advantage of defects in popular software programs (Microsoft Office, Adobe Flash Player, Adobe Reader, Java, etc). For Microsoft Windows, you need to perform Windows Update or Microsoft Update; for macOS, you need to regularly do software updates to maintain the software in its latest version. If the support for the operating system has ended, you need to update to its latest version. It is also important to update all other software programs regularly.

I have installed an antivirus software program. In addition, I frequently update the virus definition files to protect the computer from viruses.

When a computer is infected with a virus, not only data on the computer are destroyed but also the computer itself is taken over by the virus, and it might be used to send spam e-mails and attack other computers. Infection routes have diversified and using e-mails is not the only way a computer virus can spread. Actions such as browsing the Web or simply inserting a USB memory into the computer may cause infection. To avoid being infected with a virus, it is important to install an antivirus software program and update the virus definition files on a regular basis. The University of Tsukuba has purchased a site license of an antivirus software program. The antivirus can be installed on up to three personal devices (Windows machines, Macintosh machines or mobile devices). The total number of installations must be less than 4. If you have no other antivirus program installed or if you are not sure whether you are paying a license fee for an already installed antivirus program, please install this one.
For more details, please go to **https://oii.tsukuba.ac.jp/en/oii-security-2/details/**.



I never give my password to anyone.

Usernames and passwords used for the information systems in the University of Tsukuba are important information to identify the users. If you give your username and password to a third party and he/she causes trouble while using the information systems of the university, you are also responsible for the problem because you gave away your password. Furthermore, you must not use a username and password given to you by somebody else.

I never use other people's passwords and user names.

It is against Act on the Prohibition of Unauthorized Computer Access to acquire somebody else's username and password and log in as that person, or to take advantage of a security hole (flaw in a software program) for avoiding the username and password confirmation, and log into a computer.

I have set up a password which is hard to break.

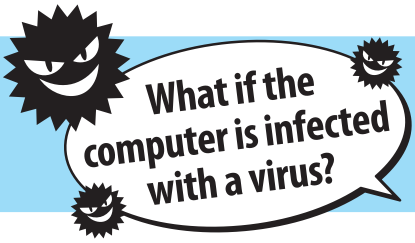
If a password is easy to break (your name, user name, birthday, phone number, repeating the same characters, using an English word more than once, using the alphabet in sequence on a keyboard, like "qwerty", or using the above in reverse), a third party may gain illicit access to your account.
It is important to set a password which is difficult to break (more than 8 characters, combination of capital letters, small letters, symbols and numbers) and change it regularly. Even if a password is difficult to break, it is not advisable to write it down and make it available to a third party.
Furthermore, it is not advisable to use the same password on different Internet services. Incidents have occurred where passwords were leaked from an Internet service; the same passwords were used to gain illegal access to a university computer and send spam emails. If you need passwords for many different online services, you can use a password management software.

I always manage personal information carefully and I always take measures to prevent information leakage.

Faculty members as well as students may handle personal and medical information collected through surveys and so on during lectures and practice classes, but that information must not be released on the network. It is also forbidden to take the information outside the university. If you need to take part of the information out of the campus, you need to obtain permission from an administrator of the respective information, or a person designated by the administrator (an instructor of a class, or a supervisor of a laboratory, in case of a lecture or practice class) and take measures to secure the information (e.g. encrypt it), before carrying it away from the campus. You are not allowed to keep personal information on a computer that is managed personally. If this is unavoidable, you must encrypt the information first.

As a member of the University of Tsukuba, I act responsibly and ethically when posting information on social networking sites and the Internet in general.

Everything you post on the internet can be seen by anyone. If posting carelessly, you may get into trouble and your actions may affect the reputation of our university. You should be very careful not to post confidential, inappropriate or offensive information on the Internet.



To avoid further infection, remove the infected computer from the network (remove the network cable or the external wireless LAN card; if you use an internal wireless LAN card, turn its switch off) and contact us at the address on the last page of this brochure.

When I use the Internet, I pay close attention to fraud (such as phishing or one-click fraud).

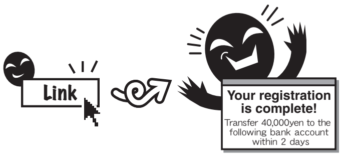
While it is convenient to use the Internet, it is also possible to face unexpected troubles. The following will show you some tips to carefully observe fraud when using the Internet. This information is obtained from “Safe Living: How to Live a Pleasant Student Life”, published by the Student Office.
If you are in trouble and cannot handle the situation, do not attempt an easy solution. Please contact your friends or faculty members or contact a consumer center first.

Phishing

In a phishing fraud, an attacker masquerades as an administrator etc. of a reputable company such as a bank, Rakuten, Amazon, Apple, Microsoft etc., and directs users to a website which is very similar to their real website, in order to steal the users’ personal identification and password. The bank and other companies will never ask you to input and confirm personal information via e-mail. If you receive a suspicious mail, do not provide your information immediately. In such a case, do not contact the address you find in your e-mail, but contact the company directly.

One-click fraud

One-click fraud means that if you click once on a link in an e-mail or on a website, you appear to have entered into an agreement and you are requested to pay a certain amount of money. If you encounter such a situation, ignore the request; do not make any payment for any purchase you are not aware of and do not give out your name or address. However, in some cases the fraudsters exploit the judicial process. If you receive notice that seems to come from court, do not ignore it, but check the address of the courthouse on its web page (http://www.courts.go.jp/) and contact that address. Do not contact the address in the letter sent to you.


Link
Your registration is complete!
Transfer 40,000yen to the following bank account within 2 days

I am careful not to open suspicious e-mails.

The University of Tsukuba has observed an increase in suspicious e-mails. These often include phishing scams, involving fraudulent e-mails that masquerade as e-mails coming from a mail system manager that try to lead you to a fake web page in order to steal your account information. Cyber-attack e-mails claiming to represent delivery notifications from delivery companies designed to let you open an attachment file in order to infect your computer with a virus have also been increasingly observed. If you receive an e-mail that seems suspicious (e.g. you have doubts about the subject, sender, contents), we recommend deleting it, not opening its attachment file, and not accessing the link included in the message.
(Reference) Examples of Phishing Emails : https://www.u.tsukuba.ac.jp/en-phishing-collection/

Contact us if you find any problems

Please contact us immediately if you find security vulnerabilities and defects in the information systems of the University of Tsukuba, infringement of copyright, leaking of classified or personal information, release of classified information or personal information about faculty members of the University of Tsukuba through the information systems outside the university, and unauthorized use of contents owned by the University of Tsukuba.

Contact information

Organization for Information Infrastructure
(Division of Information Infrastructure Management, Department of Academic Information)
e-mail: oii-security@oii.tsukuba.ac.jp

For more details regarding this brochure: **https://oii.tsukuba.ac.jp/en/oii-security-2/details/**

This brochure has been created by the Office for Information Infrastructure Planning, Organization for Information Infrastructure at the University of Tsukuba.

Issued in March, 2020