Protect yourself from Internet troubles

Accessing the Internet is a part of your daily life, however, at the same time you can easily be involved in troubles and accidentally be an individual at fault of a rash behavior.

How to handle passwords and personal information

- **Do not use words or numbers that can be easily looked up, such as dictionary words, your birthday, and your name as your password.**
  It would be desirable for the password to contain a mixture of uppercase and lowercase alphanumeric characters and usable symbols.
- **Never disclose your passwords to anyone.**
  Store your passwords in a place that cannot be accessed by other persons. Of course, do not share your password with others.
- **Do not use the same password for multiple sites.**
  Setting up a different password from service to service prevents widespread damage if one of your passwords becomes known. If you need passwords for many different online services, you can use a password management software.

Usage of SNS

- **Be aware that information published on SNS may be spread to an unspecified number of people even if access is restricted.**
  Inappropriate videos and images that you posted all in good fun may be uploaded to other sites. Beware of posts to SNS spread to every place.
- **Be aware that content posted on SNS may remain permanently as "Digital Tattoo".**
  "Digital Tattoo" may continue to affect your future life (employment, marriage, evaluation, etc.).
- **Be aware that you are responsible for your words and actions.**
  It is strictly forbidden to insult individuals or groups, or to make any discriminatory statements or adopt an exclusionary attitude regarding race, gender, nationality, thought, religion, appearance, or occupation.

Protect yourself from scams

- **Beware of phishing scams e-mails.**
  An e-mail that looks like it originated from a company's actual site (e.g., banks, Rakuten Amazon, Apple, Microsoft) may be sent to lure you to a fake webpage; this is called "phishing." Remember that banks do not send e-mails requesting your sensitive information, such as your bank account number, password, or credit card number.
- **If you receive something suspicious, do not reply to the contact information written in the received e-mail, and look up that company's contact information before you make any inquiries.**
  If you face something you don't understand or cannot resolve, ask your friends or a faculty member for advice, or look up the websites like the ones shown below.
  - Tsukuba Consumer Information Center: • National Consumer Affairs Center of Japan
  - Safety and Security Counseling on the Internet, National Police Agency
    https://www.npa.go.jp/cybersafety/ (Only available in Japanese)

Protecting yourself against computer viruses

- **Frequently update the operating system (e.g., Windows) and web browsers (e.g., Microsoft Edge, firefox, chrome) on your device.**
- **Install anti-virus software and always keep the virus definition files up to date.**

Before you use any computers or networks on campus, be aware of the guidelines for use!

When you use the University of Tsukuba Information System (networks, computers, etc.), there are guidelines that you must follow. Please check, confirm and follow these guidelines. They can be viewed from the oncampus network at this site:
https://oii.tsukuba.ac.jp/en/oii-security-2/
Organization for Information Infrastructure (Division of Information Infrastructure Management)
E-mail: oii-security@oii.tsukuba.ac.jp