Sophia University
Sophia University Junior College Division
Sophia School of Social Welfare

Information Security Handbook for Students

Information and Communication Technology is progressing rapidly in the fields of education and research as well, and the use of computers and the Internet is increasing. At the same time, threats on the Internet are also increasing. Examples of this include the exploiting of information and communications technology spreading computer viruses and the sending of massive amounts of spam and fraudulent mails. Our university has also faced serious security incidents, including virus infection and account hacking that could lead to information leak incidents, making this an issue that concerns each student.

Please use this handbook to understand the necessity of information security measures and to implement countermeasures.

April 1, 2019
ICT Office, Sophia University

Information Security Policy: 8 Steps

1. Software Vulnerability Measures (OS, Office applications, etc.)
2. Antivirus Measures for Computers
3. Proper Software Management
4. Using Web Apps (File-sharing software, online storage, etc.)
5. Security Measures for Wireless LAN
6. Password Management
7. Avoiding Internet Trouble (SNS)
8. Procedures for Disposing of Unneeded Computers

STEP

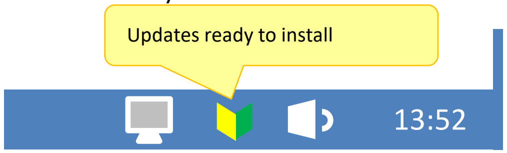
01

Software Vulnerability Measures (OS, Office applications, etc.)

Over time, web browsers, e-mail software, OS, Office applications, and other software may encounter a problem called vulnerability. If you fail to solve the vulnerability problem, even if you install antivirus software, there is a high risk of virus infection or of intrusion from another computer. Please be sure to take the following precautionary measures against software vulnerability:

- **Update** OS and software regularly.

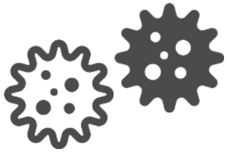
  On Windows, using Windows Update will strengthen protection against vulnerability, the weak point in a program where viruses can easily enter. (Windows 10 normally updates automatically)



- On other OS and software, determine **how to update** and do so regularly.

- Be careful with smartphone updates.
  - Check the OS and app update notifications and update appropriately.
  - Some apps fail to function after an OS update. Updating may cause problems, so obtain necessary information in advance and check safety before updating.

- Avoid using OS or software that is **no longer supported**
  - If there are no alternatives, take measures such as not connecting to the network.



STEP

02

Antivirus Measures for Computers

Recent viruses are becoming diverse and sophisticated and are able to do such things as display e-mails, or infect websites merely by browsing them with web browsers. Also, compared to the past, some attacks work in such a way that the contents and magnitude of the damage are not immediately detected. In addition, virus infection claims its next victim not only by the first target's information leakage but also through secondary and tertiary infections, so there is also the danger of unknowingly becoming a perpetrator.

▶▶ **Install antivirus software.**

During the enrollment period, faculty members and students enrolled at Sophia University (including the junior college division) and Sophia College of Social Welfare can **download anti-virus software (Trend Micro Virus Buster Corporate Edition) for personal computers from the Web page of the ICT Office free of charge**.

▶▶ **Automatically update** anti-virus software **definition file**.

Simply installing antivirus software will not allow it to always respond to the latest virus. It is necessary to always keep the pattern file up-to-date.

▶▶ **Run virus scan on a regular basis**.

▶▶ **Stay aware of virus infections and security related news.**

We often hear news about leakage of personal information from free online storage services and other ICT security issues. Seeing this as someone else's problem and continuing to use your device without thinking may make you a victim. Always pay attention in the use of your smartphone or computer.

▶▶ When inserting storage medium, be sure to execute the virus check before opening the folder or file. There are incidents in which a virus is spread just by inserting storage media such a USB memory into a personal computer and using the automatic execution function.

STEP

03

Proper Software Management

Since software is a copyrighted work, copying or distributing it illegally makes one subject to criminal penalties and damages compensation. Take responsibility for way that you acquire software, as there are cases in which merely saying "I didn't know" won't protect you, some that even result in arrest and prosecution.
Please manage software properly observing the following:

▶▶ Do not **get software illegally** from unofficial websites etc.

- Apps now have a tracking feature. If you use software that is not legal, **you may be identified by the user, reported to the police, or may be required to pay a large amount of compensation**.
- In many cases, viruses have been incorporated and **many cases of damages have been reported**.

▶▶ **Confirm the usage rights and other details** of software licenses.

▶▶ Do not copy and use properly purchased software.

▶▶ **Use software as stipulated** in the contract.

If you use unauthorized software or apps ･･･●

Apps claiming to be "useful" and urging you to install them are frequently sent in SPAM emails and include many fraudulent items. Masquerading as an appealing app that one simply must have, they try to trick the user into installing it. Once these apps are installed on your smartphone or PC, others can control your device remotely from outside. As a result,

□ Personal information such as address books are stolen
□ SPAM messages are posted through SNS and email
□ The app is used for the next attack and more fraud. If you use your smartphone as a wallet, your card and other information can be stolen and used illegally.

STEP

04

Using Web Apps (File-sharing software, online storage, etc.)

There have been cases where file transfer software has been accessed illegally and personal information of members leaked. Free file transfer and online storage (services that allow files to be accessed from various terminals by placing the files on the Web) are very convenient, but personal information can be at risk due to human error within the managing company.

Information leaks may result in claims for compensation and lead to mental distress.

Please take the following measures for using such software and services:

- Some free cloud services exist to steal data, so **use great caution when storing important personal information**.
- Use external **services** (cloud services) **that use contract terms and can be trusted**.

- When using online storage (iCloud, Dropbox, GoogleDrive), backup to protect data in case of a sudden access outage or the server going down.

Using online storage

Online storage is very convenient because you can easily share files simply by sending the URL of the file uploaded on the Web to the other party. However, cases are increasing where clicking on a URL in a phishing email leads to a fake site or file and virus infection. If the virus infects a shared folder, the damage can spread quickly. Always keep safety in mind when using online storage.

As our school uses Sophia Mail, we recommend **OneDrive** provided by Office365. OneDrive has a file restoration function as a measure against ransomware.

□ How to use **OneDrive**:

https://ccweb.cc.sophia.ac.jp/documents/#_217

STEP

05

Security Measures for Wireless LAN

Wireless LAN is being introduced in homes and offices because of its great convenience. Public wireless LAN service has become widespread, and it is now available in stations, airports, cafes and restaurants. However, because wireless LAN communicates using radio waves, there is a **danger of others stealing communication contents**.

When installing in your home, office, or elsewhere a wireless LAN router you have purchased, please pay attention to the security settings.

▶▶Use the wireless LAN specified by the Sophia ICT Office: **sophiawifi2019, eduroam**

▶▶When setting up a wireless LAN environment at home or elsewhere, do not keep using the initial password. Strengthen security by combining WPA2 personal (AES) or MAC address authentication.

▶▶Avoid using public wireless LAN as these cannot guarantee security.

Wireless LAN risks･･･

Public wireless LAN service has become common in stations and restaurants as places offering wireless LAN increase. Take special care to confirm reliability before accessing wireless LANs that do not require passwords or use common passwords.

Wireless LAN has become easy to use. People purchase wireless LAN routers for individual use and rent mobile routers when traveling abroad. These devices are convenient and easy to use, but please use the following functions to enhance safety (examples given for reference).

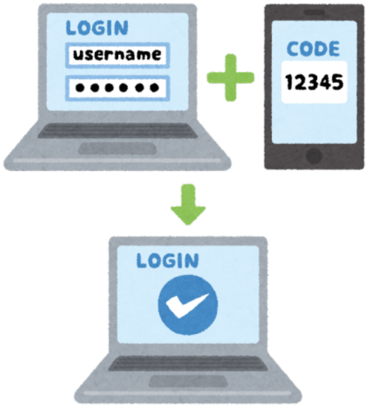
◆A fixed number called a MAC address is assigned to the communication device. When configuring the router, register the MAC address and limit the clients that can use it.

◆ The wireless LAN router has a name (SSID) to identify it, and an encryption key (password). Although it is possible to use the initial password, change the name to strengthen security, but not to an easily guessed name such as that of the user or organization.

STEP

06

Password Management



It is important to create a secure password that is hard to guess and to keep it from being seen so that others cannot use your account illegally.
Please practice password management as follows:

▶▶ Manage your smartphone password/passcode well.

- Make sure you are not being watched when using your device in crowded places.
- Do not use an easily guessable password/passcode.

▶▶ **Do not use personal information** such as name or birthdate.

▶▶ Use **12 or more characters** including alphanumerics.

- Combinations of upper and lowercase letters, numbers, and symbols are desirable.
- When system restrictions exist, stay as close to the above as possible.

▶▶ **Never give your password** to others.

▶▶ **Do not use the same password** with multiple services.

▶▶ If a service has **2-step authentication** (security code with ID and password), we recommend using this procedure.

Making a secure password・・●

1. Make a simple sentence. 2. Use only the first letters of words. 3. Replace letters with symbols.

Ex: 1. ”I am learning Yoga every Wednesday night from 6 o’clock”
2. → “IalyeWnf6o”
3. → “I@1yeWnf6o”

Use a site that performs password strength checks such as Kaspersky https://password.kaspersky.com/jp/.
Similar checkers are available at Microsoft, Intel, etc.

STEP

07

Avoiding Internet Trouble (SNS)

Popularization of services such as SNS have increased opportunities for individuals to disseminate information. This can lead to trouble, for example, as when careless written comments subject the object of the comments to intense criticism by large numbers of users. Organizations and individuals have filed damage claims in response to such incidents.

To avoid trouble on the Internet, please take the following countermeasures:

▶▶ When using services such as SNS, **use common sense and appropriate manner** in your content.

▶▶ **Realize that it is easy to identify the individuals** that write. Do not advocate illegal acts or write antisocial messages.

▶▶ If you post photos to SNS that an unspecified number of people browse, be careful not to embed **geotags** that can identify the location where you took the photo.

▶▶ Do not carelessly write personal information.

▶▶ Know that you **cannot completely delete** items once they are posted. Damage claims may sometimes result.

SNS and part-time worker terrorism ●

Inappropriate videos taken by part-time workers during work and disseminated through SNS in what is called "part-time worker terror" have caused great damage to businesses. While the perpetrator may regard the act as a prank, it is a very serious matter for companies that have their brand image tarnished. People thinking they are posting anonymously may face the following:

□ **Being quickly identified and subjected to continuing harsh judgment and criticism.**

□ **Criminal charges and charges for damages.**

No matter how much you regret what you did, you cannot regain other’s trust in you. Think before you act!

STEP

08

Procedures for Disposing of Unneeded Computers

When disposing of items such as personal computers that are no longer needed or when transferring them to another person, there is the possibility of information leak from the installed hard disc, for example.

When disposing of personal computers or other devices no longer needed, please take the following precautions:

- **Erase data** using software created for this purpose or ask a professional data-erasing company.
- Remove the hard disk mounted on a personal computer or other device and **physically destroy** it.
- When discarding medium on which personal data is recorded (CD-ROM, documents, etc.) physically destroy the medium with a shredder or the like.
- When disposing of a smartphone, **be sure to delete** personal information such as addresses and phone numbers.
  - Carelessly giving your smartphone to a recycling company may result in leakage of personal information.
- It is easy to lose your smartphone, so take precautions such as being able to **remotely set a lock or delete your data**.

Social engineering･･･

Social engineering refers to finding and taking advantage of human psychological gaps and behavior rather than using ICT to obtain sensitive information such as passwords necessary for entering a network.

<Methods and countermeasures>

■ Dumpster Diving (trashing): Posing as a garbage collector to remove trash from targeted company.

■ Visual hacking (shoulder surfing): Approaching someone from behind and peeking while they are entering important information such as a password (be careful on trains as well). Glancing at an ID or password written on paper (such as sticky notes) and memorizing the information.

Resources for Information Security

Security updates
Information-Technology Promotion Agency,
Independent Administrative Institution (https://www.ipa.go.jp/security/personal/)

Security alerts
JPCERT Coordination Center
(https://www.jpcert.or.jp/）

Copyright information
Public Interest Corporation Copyright Information Center
(http://www.cric.or.jp/)

In case of an information security incident

In the case of a possible information security incident such as a personal computer, USB, or other item being lost or a computer being infected with a computer virus, promptly contact the ICT Office (Media Center).

Loss of personal computer or USB memory
Department name: General Affairs Group
Contact: 03-3238-3172 Ext. 3172

Technical inquiries
Department name: ICT Office
Contact: 03-3238-3101 Ext. 3101 or 4473

Campus Information Security Rules and Resources

· Sophia University ICT Security Basic Policy
· Sophia University ICT System Security Regulations
(https://kitei.cl.sophia.ac.jp/doc/suallstaffs/listall.html#)

Systems Usage Guide
Sophia University ICT Office (Media Center)
(https://ccweb.cc.sophia.ac.jp/userguide/)

Sources

□ Ministry of Internal Affairs "Information Security Site for Citizens"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html)
□ Independent Administrative Agency Information Processing Center Security Center (IPA) "Minimal Information Security Measures for Businesses and Organizations + 1
（https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)