Kumamoto University Information Security Pocket Manual (For Students)

Issued by the Information Security Division,
Center for Management of Information Technologies

Use of Computers, Smartphones, etc.

熊本大学
Kumamoto University

■ Various problems with computer and smartphone use have been occurring more frequently. This pocket manual explains what you should be careful of when using these devices.

1 Keep personal IDs and passwords safe!

User IDs and passwords are important identification information. Make sure no one can steal or use your information.
Avoid choosing a password that can be easily guessed (e.g. birthday) or using the same password for multiple websites.
* Kumamoto University recommends that you choose a password with at least eight characters that contains at least three of the following character types: lowercase letters, uppercase letters, numerals, and symbols.

2 Take anti-virus measures!

Anti-virus measures must be taken to protect your computer and smartphone. Make sure you install anti-virus software on your personal computer. The antivirus software F-Secure is available for free for students currently attending the university. You should also keep the operating system and applications updated.

3 Watch out for peeking!

When using a computer or smartphone on the bus/train, in restaurants, or other public place, stay aware of your surroundings. Your screen may be reflected on a glass window or mirror. When you leave your seat, keep your devices with you at all times.

4 View emails in plain text format!

Emails you receive on your personal computer and other devices are usually shown in HTML format by default. However, some viruses are reported to infect computers just by opening an HTML email. Set your display format as well to plain text.

5 Password protect email attachments!

Email texts are just like those on postcards; someone else could easily read the contents. Even attached files can be easily accessible if they are not password protected.
Avoid sending documents that contain personal or research information by email as much as possible. If you must send such information by email, make sure you set a password for the file.

6 Ignore (delete) suspicious emails!

If you receive an email scam from some financial or other institutions that asks you to change your password, or a suspicious email from someone pretending to be your friend or a faculty member, etc., ignore (delete) the mail. Viruses can be transmitted simply by opening the mail or attachment.

7 Use caution with cloud storage services such as Dropbox!

Your data stored in cloud storage (e.g. Dropbox) may belong to the cloud service provider. Make sure you read the terms of use and limit the scope of disclosure when using the service.

8 Maintain awareness of the importance of your personal information!

There have been increasing cases of people involved in some troubles due to having their personal information misused. Do not download applications from unofficial websites; some of them are intended to exploit your personal information. You should also avoid registering your personal information (name, address, part-time job, location information, etc.) without careful consideration.

9 Refrain from posting unnecessary comments on social media such as Facebook and Twitter!

Comments on social media can instantly spread across the world. Many cases have been reported where postings of unlawful behavior (e.g. underage drinking/smoking) and nuisances (e.g. workplace misbehavior) led to problems. Causing such a trouble could affect your future (career).

10 Keep copyrights in mind when using information on the Internet for your reports!

When citing information from books and online sources for your reports and research papers, you must pay attention to their copyrights. If you use such information improperly, you may be sued for copyright infringement.

Use of USB Flash Drives, Printouts, etc.

熊本大学
Kumamoto University

11 Delete data from your USB flash drive and SD card promptly after use!

Compared to mobile phones and smartphones, USB flash drives and SD cards tend to be used casually. When you carry them, you should not only keep them with you at all times, but also delete data after use just in case.

12 Safeguard paper printouts, too!

Loss or theft of paper printouts as well as digital data will be a problem in terms of personal information leakage.
After printing something out, make sure you collect the papers immediately and not leave them on your desk.

13 Report as soon as possible when an incident occurs!

Incidents include virus infection and other matters that could lead to personal information leakage, such as loss of a computer, USB flash drive, or paper printout.
If you find such an event occurring at the university, report it immediately to your instructor (or academic affairs section) and the Help Desk of the Center for Management of Information Technologies.

When an Information Security Incident Occurs

熊本大学 Kumamoto University

If you suspect an incident . . .

Notification from the antivirus software

Computer malfunction

History of emails sent you don't remember sending

Emergency measures (in the computer room)

(1) Shut down the computer.
(2) Report immediately to the academic affairs section and the Help Desk, and follow their instructions.

Emergency measures (in a laboratory)

(1) Unplug the LAN cable from the computer.
(2) Report immediately to your instructor and the Help Desk, and follow their instructions.

[Report to]

- **Center for Management of Information Technologies (Help Desk)**
  096-342-3949 (security@kumamoto-u.ac.jp)