# Basic information security measures (for students)

Keio University Computer Security Incident Response Team (CSIRT) March 2025

Refer to the supplement for a detailed explanation of sections with ★ symbol.


## What's MFA?

Multi-factor authentication ★[1] helps to prevent unauthorized logins in the event that authentication or phishing prevention fails and password information is leaked.

| Information security measures: | Potential consequences of failure to act: |
|---|---|
| **Authentication-related:** | |
| 1. Set a sufficiently secure★[2]password<br>2. Avoid using the same password on multiple sites<br>3. Don't share your password with others<br>4. Don't log in to others' accounts | 1. Password can be easily guessed or brute-forced<br>2. Password leak at one site affects other accounts★[3]<br>3. May be used for criminal activity ★[4] or other unauthorized use<br>4. Without justifiable reason, may be considered illegal |
| **Software-based prevention:** | |
| 1. Update OS and other software regularly<br>2. Don't use discontinued OS or applications<br>3. Install anti-malware software★[6] on all PCs<br>4. Avoid pirated, cracked, or other illegitimate software<br>5. Be especially careful of infostealer★[7]malware | 1. Malware★[5]infection that exploits an existing vulnerability<br>2. OS and application vulnerabilities remain unfixed<br>3. Much higher possibility of malware infection<br>4. These types of software are often used to share malware<br>5. All passwords and other data stored in your web browser are stolen |
| **Phishing prevention:** | |
| 1. Be careful of emails linked to fake login pages<br>2. Beware of unfamiliar login pages<br>3. Take note of sender email address★[8]<br>4. Be careful of URLs ★[9]included in emails<br>5. Beware of text attempting to unnaturally elicit a response | 1. Provide ID and password to a malicious actor<br>2. Login screens you have never seen before are often fake<br>3. Mistakenly trust an email with a forged sender's name<br>4. Access a fake login screen with a fake URL<br>5. Hastily entered login info into a fake login page without realizing |

## User contact

If CSIRT or KIC becomes aware one of these situations occurred, we may contact individually. Support to help resolve the problem is available.

○ **Consider turning on multifactor authentication for keio.jp and other online services.**

○ **If you receive communication from KIC or CSIRT regarding information security, please respond promptly!**

○ **If you mistakenly entered your password in a phishing page, change your password ASAP and contact KIC!**

★[10]

# Basic information security measures (for students) Supplementary information (1)

Keio University Computer Security Incident Response Team (CSIRT) March 2025

## ★1 What is “multi-factor authentication” (MFA)?


Authentication that uses either “something you have” (e.g. cell phone) or “something you are” (biometrics) at the same time, when used in conjunction with a password. Even if the password is stolen, an unauthorized third party cannot immediately log in. It is available on keio.jp and many off-campus web services, and we recommend that you actively use it where possible.
Refer to the following page for information about keio.jp MFA.
https://www.itc.keio.ac.jp/en/keiojp_mfa2.html

## ★2 What is a sufficiently complex password?

Historically, it was considered good practice to set long passwords with uppercase, lowercase, and special characters and change regularly, but modern password guidance focuses less on regular password changes and more on the complexity of your chosen password.
Please refer to section B of the following page for the current keio.jp password policy:
https://www.itc.keio.ac.jp/en/keiojp_manual_activation.html

## ★3 What are the dangers of reusing passwords?


In the event that your ID/password information from sites outside of Keio is leaked, and you use the same password across multiple sites, an attacker may be able to access any other account using the same password (such as keio.jp or others). Using a password manager to set a unique password for each site is one way to avoid such problems.

## ★4 What are the dangers of giving your password to someone else?

Sharing your password with someone allows them to freely use that account as they wish, including for crime. In particular, if you give someone else your password for financial or payment services (incl. e-money) and they use it to commit a crime, not only could it lead to damage to your credit information, which may be difficult to recover, but you could be considered as an accomplice in crime. Aside from the affected service, you may also be restricted or banned from using other services,.

## ★5 What happens when a malware infection occurs?

Malware is a generic term for malicious software, such as “viruses”, “worms” and “Trojan horses”. The exact behavior when infected can vary depending on the type of malware, but can include increased load on your computer, infection of other systems, remote control, information leakage, system sabotage or destruction, encryption for blackmail or ransom, among others.
If the KIC or CSIRT detects malware-specific behavior, etc., in your network activity, we may contact the user directly, in which case, please take immediate action.

# Basic information security measures (university students) Supplementary information (2)

Keio University Computer Security Incident Response Team (CSIRT) March 2025

## ★[6] What is anti-virus software used on a PC?

Keio University provides a site license for ESET Internet Security to use on personal computers. Enabling Windows Defender, which comes with Windows 10 or later, is also an acceptable choice. Refer to the following page for information about obtaining a license for ESET Internet Security through Keio University.
https://secure.itc.keio.ac.jp/c/a/itc/en/software_license_esets.html
However, there have been examples of malware that can remain undetected by antivirus software in recent years.

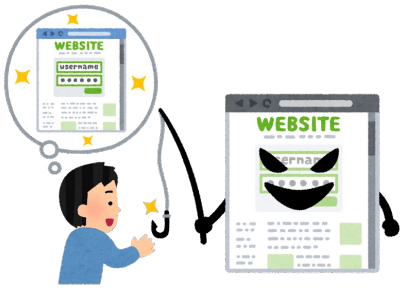
## ★[7] What is infostealer malware?

*Infostealer* is a generic term for a type of malware that steals passwords and other information saved on your computer and is considered especially dangerous. If your antivirus software detects malware containing words such as “Stealer”, “RedLine”, “Raccoon”, or “Lumma”, you may have been infected with an infostealer malware. Please consult with KIC as soon as possible.
Infostealer infections commonly occur from game cheat tools, pirated apps, or other apps installed from unofficial sources, and phishing emails. Avoid such risks as much as possible.


## ★[8] Who is the sender of phishing emails?

In email, the sender is generally indicated in the format “Taro Keio <keio-taro@keio.ac.jp>”. However, many common phishing emails forge only the name and not the email address.

## ★[9] What is a phishing email URL?




In many cases, URLs in phishing emails are created by making partial copies of websites, and often have server names that have nothing to do with the original service. In such cases, it is possible to avoid falling victim by checking the server name in the URL.

## ★[10] Contact and respond quickly!

If you mistakenly entered your ID and password into a phishing site, first change your password for all sites that use that ID/password (starting from the most important sites) then contact KIC.
Similarly, if you opened a suspicious file that you suspect might contain malware, please contact KIC as soon as possible.
Unfortunately, there have been a number of cases in which KIC or CSIRT contacted a user about a security concern, but the user’s response was quite slow.
When you avoid contacting us or have a delay in responding, irreversible damage may occur.
Prompt contact and response are necessary to minimize the damage from a potential cybersecurity incident.

Have questions? Need advice?
csirt@info.keio.ac.jp