Measures to prevent malware or ransomware infection

□ **Don’t click on links in spam, unexpected or suspicious emails.**

- Never open attachments in emails from someone you don’t know. Cybercriminals often distribute fake email messages that closely resemble email notifications from an online store, a bank, the police, a court, or a tax collection agency. They lure recipients into clicking on a malicious link that will release the malware into their system.
- Be aware that any account can be compromised, and malicious links can be sent from email and social media accounts of friends or colleagues.

□ **Be wary while browsing the internet and do not click on suspicious links, pop-ups, or dialogue boxes.**

- Clicking on them might download malware to your systems, with the link often not leading to the intended website. If you aren't sure, run the website through a search engine first to see if it really exists.

□ **Browse and download only official versions of software and always from trusted websites.**

- If you are downloading something on your phone or tablet, make sure you use reputable sources and stores, like the App Store (Apple) or Google Play Store (Android). The best way to determine whether a website is fraudulent is to pay close attention to the URL. The domain name in the URL should match the name of the website. An HTTPS connection and displaying the padlock icon are signs of secure connection, but this doesn't mean you can trust it.

□ **Regularly back up data stored on your computer, so a ransomware infection wouldn’t destroy your personal data forever.**

□ **Use robust security products and ensure that your security software and operating system are up to date.**

- For Mac users, please use McAfee Endpoint Security for Mac which you can download from the ISTC download system. For Windows users, please use Windows Defender.
- Don't switch off the 'heuristic functions' to detect malware and ransomware.
- When your operating system (OS) or applications release a new version,

install it. If the software offers the option of automatically installing updates, take it.

□ **Turn on local firewall.**

- Turn on your local firewall to defend against unauthorized access.
  - On Apple devices: System Preferences > Security & Privacy.
  - On Windows devices: Start > Settings > Update & Security > Windows Security > Firewall & network protection.

■ **When it is suspected that an information security incident has occurred on the university network,**

- The ISTC will first contact the GSICS IT Committee. The member of the Committee will then contact the user of the terminal where the virus was detected. In this case, follow the instructions.
- First disconnect your computer from the network. In the case of a wireless LAN, turn off the wireless function. Try not to shut it down in order to preserve evidence.
- Once your computer is infected with a virus, it is highly likely that the information on your computer has been extracted and transmitted, so change the passwords of all IDs registered (or used) with the web browser or applications on that computer. Especially in the case of bank or credit card related information, contact the company immediately and stop using them temporarily.
- Follow the GSICS IT Committee's instructions for recovery. If a virus infection is suspected, you will be instructed to work based on the investigation and results of the antivirus software.
- Do not connect to the network until you have been authorized to do so by the GSICS IT Committee.

Cited from:

- NO MORE RANSOM > Advice for regular users
  https://www.nomoreransom.org/en/prevention-advice-for-users.html
- 神戸大学 LMS BEEF ＞ Venture 情報基礎 2022 ＞３．インターネットの利用
  https://venture.center.kobe-u.ac.jp/pluginfile.php/95820/mod_resource/content/0/johokiso3.pdf

IT Committee, GSICS