
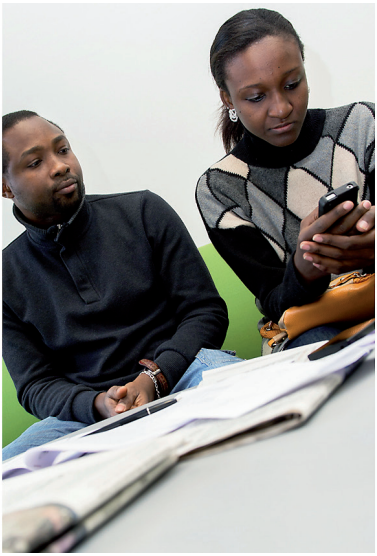
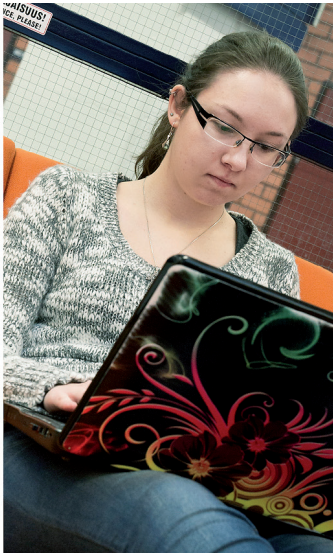

STUDENT'S INFORMATION SECURITY GUIDE

April 2013

TABLE OF CONTENTS

This Information Security Guide is primarily intended to serve as a general guide for university students, regardless of their place of study. It is produced by a group of information security experts from different universities.

Workgroup:
Olavi Manninen (University of Eastern Finland), Mari Karjalainen (University of Oulu), Matti Levänen (University of Jyväskylä), Ulf Pensar (Hanken School of Economics), Jan Wennström (Åbo Akademi University).
Photos:
Raija Törrönen (University of Eastern Finland)
Layout:
Rolf Niskanen (Åbo Akademi University)
Translation:
Miia Santalahti (T:mi Käännös-Ässä)

The guide is an updated version of the 2009 release produced by Kenneth Kahri (University of Helsinki), Olavi Manninen (University of Kuopio), Kaisu Rahko (University of Oulu).

INFORMATION SECURITY IS IMPORTANT - ALSO FOR YOU

- Our daily use of information technology entails various information security threats.

- One serious threat is malware distributed through networks and e-mail. Malware programs can, for example, steal or destroy your files, reveal your user IDs and passwords, or slow down networks. Anti-virus software can never provide full protection against malware, because new versions emerge all the time. Other serious threats include identity theft and the phishing of user information for financial gain.

- You should apply common sense and observe the given guidelines to protect your data, workstations and IT networks. Apart from your personal data, also remember to ensure the security of other people's information that is in your possession, such as personal and contact information, bank account details, health records and e-mail messages.

- Everyone is obligated to maintain information security by observing the relevant laws and the university's information security guidelines. Neglecting these regulations may lead to serious consequences.

USE STRONG PASSWORDS AND KEEP THEM SAFE

- Use your personal username and password to log into the university's systems. Keep your user ID and password as safe as you keep your bank card and its PIN code.

- When you get a new password issued by IT support, immediately change it to one that is only known by you. Change your password regularly according to the university's guidelines, and always if you have any doubt that it has been revealed to someone else.

- You are responsible for all activities carried out under your user ID. Never tell your password to anyone else; not even to the system administrators. If anyone asks for your password, it is definitely for a malicious purpose.

- Choose your password carefully. A good password is easy for you to remember but impossible for others to figure out. Don't use words that are commonly used or somehow connected to you. You shouldn't write down your password as such. Check your university's instructions about choosing a good password.

- Choose different passwords for the university systems and any external services; this way, cracking the external service password will not compromise the university system's security.

E-MAIL USE

- The university e-mail address should be used as your primary contact address for the internal communications and services at the university, such as the study registry and learning platforms. Using the university e-mail services can enhance the security of communications.

- If you receive an e-mail message intended for another recipient, inform the sender about the wrong address. Remember that you are obligated to maintain the message contents as confidential.

- E-mail messages may contain malware or direct you to sites that contain malware. Don't open messages if you are not sure about their origin. You can also turn to IT support for further instructions.

- E-mail messages are usually conveyed in an unencrypted format, so sensitive messages must be separately encrypted before sending.

- Be cautious about sharing your e-mail address. Avoid using the university e-mail address on online forums and social media (e.g. Facebook); get a separate e-mail account for such personal use.

- If you use an external e-mail service instead of the university's services, make sure that the service uses encrypted connections (browser-based service address starts with https://).

BEWARE OF PHISING AND OTHER SCAMS

- Don’t blindly trust all e-mail messages. The e-mail’s sender field may not indicate the actual source of the message. Malware applications can send e-mail without the user’s involvement.

- Beware of phishing, i.e. messages asking you to share your user ID and password or enter them on a website. System administrators never ask for your password.

- Always check the actual target address before clicking a link. Be extra careful with regard to links received in messages.

- Learn to tell which Internet addresses are genuine and which indicate fraud. Familiarise yourself with your university’s guidelines.

- Advertisements and chain letters sent without the recipient’s consent are considered spam. Never respond to such messages; just delete them. If an offer seems too good to be true, it probably is; don’t take it.

- Universities apply various methods of spam and malware filtering, and this may affect the delivery of e-mail messages. Familiarise yourself with your university’s practices.

- Apart from e-mail, you may also encounter other forms of attempted deception, e.g. by telephone or on social media sites. Be cautious about unexpected invoices or messages from senders posing as system administrators.

USE ONLINE SERVICES AND SOCIAL MEDIA WISELY

- Think carefully about sharing information about yourself or others in various online services (Facebook, photo sharing services, etc.). After uploading, a piece of information such as a photo or home address may be impossible to delete permanently from the web.

- Be cautious about pop-up windows and advertisements. Malware spreads efficiently through social media and online services - click carefully!

- Don’t use online services that don’t feel reliable.

- Many online services are implemented in the form of cloud services, which means that the information given by users is only stored on the service provider’s servers, often outside Finland. Cloud services entail many information security risks, which you should be aware of. Before registering as a service user, always check the terms and conditions concerning data ownership and the disclosure of data to third parties.

- Check your user profile’s privacy settings (who can access your information) and adjust them when necessary.

- Be cautious about personal data: think carefully about which information you share and with whom you share it. You are in charge of sharing your own personal information, but others’ personal information can only be shared with their consent.

- In online communities, it is easy to pretend to be someone you are not. Don’t be too gullible with regard to things you read on the Internet.

- Remember the so-called netiquette in e-mail and online communications. For example, harsh comments posted on a discussion board may harm your reputation later when you apply for a job.

- Don’t add location data to photos you post online. Disable your camera’s GPS functionality or remove the location stamp from photos before publishing.

KEEP YOUR OWN COMPUTER HEALTHY AND FUNCTIONAL

You are the systems administrator of your own computer. Monitor its functionality and ensure proper information security according to the following instructions.

- If the computer is connected to a network, it must be protected with a firewall and anti-virus software.
- Don’t install any software application you don’t really need. Install all security updates.
- Create separate user accounts (without administrator rights) for all other users of your computer. Administrator rights should only be used for administrator-level tasks (software installation, creating other accounts).
- Take back-up copies of your files on a regular basis. Keep the back-up copies separated from the computer, preferably in a locked place if possible.
- Don’t dispose of discarded computers, smart phones or flash drives with general waste. Data must be destroyed by means of overwriting or crushing the media; printouts by shredding.

ALSO KEEP YOUR MOBILE DEVICES SECURE

- Phones, tablets and other mobile devices must be protected as carefully as computers.
- Don’t open messages that come from unknown senders or seem suspicious for some other reason. They may contain malware that send messages in your name or cause other kinds of harm and extra costs.
- Protect your mobile devices against theft. Set a security code (in addition to the PIN code) to prevent outsiders from accessing your data. Find out whether it is possible to remotely clear your device contents if necessary.
- Disable wireless connections (Bluetooth and WLAN) when you don’t need them.
- Remember to also take back-up copies of the important data stored on your mobile devices. Dispose of your data when you discard the device.
- Don’t install any software application you don’t really need. Only download and install software from authorised distributors.
- When travelling, remember that foreign data transfer costs are high, so use your mobile devices with consideration.
- Carefully consider whether you should share your location data in online services.

USE THE UNIVERSITY'S COMPUTERS RESPONSIBLY

- Always log in using your personal user details. When finished with your session, delete any temporary files you have created before logging out.

- Always lock the workstation when you leave it, even for a minute (on Windows workstations: Win+L). This prevents unauthorised usage with your account. However, please note that it may be forbidden to lock a workstation and thus keep it reserved for a long time.

Lock a workstation (Win+L).

- Save all important data on a network drive or in your home directory. These are covered by the university's back-up procedures.

- If you print something using a shared printer, pick up your printout immediately.

- When you produce or edit text or other materials, remember to save your changes regularly (in many Windows applications, the shortcut is Ctrl+S). This way, you won't lose all of the work done in case of technical failure.

- Installing software on the university's computers is usually forbidden and also technically prevented. If you need a certain application, contact the IT support.

BE CAUTIOUS WITH OPEN LANS AND PUBLIC WORKSTATIONS

- You should never rely on the information security of Internet cafés, libraries or other public workstations; they may have a program that collects user data. Consider whether it is necessary to access, for example, your e-mail from such a workstation.

- You always leave a trace of your computer and software usage. Learn to clear the browser's cache memory and delete the most typical traces of your session.

- If you use wireless LANs, only contact e-mail and other services that use an encrypted connection (the address starts with https://).

TAKE GOOD CARE OF YOUR USB FLASH DRIVES

- Don't use a USB flash drive as the primary or only file storage, even though it is a practical tool for transferring data and making back-up copies. A flash drive can easily get lost.

- If you intend to save sensitive data on a flash drive, get one that encrypts the data.

- Be wary of other users' flash drives. They may contain a malware application that activates itself automatically and contaminates your computer.

- If you find someone's flash drive in the university's premises, take it to the IT service point without checking its contents.

OBSERVE COPYRIGHTS AND SOFTWARE LICENCES

- Make sure that you have the required licences for the applications you install on your computer. Don't install unauthorised copies.
- Universities provide their students with usage rights to certain special applications; see your university's guidelines for further information.
- Read the library's guidelines to learn the terms and conditions of using electronic library materials.
- Movies and music materials are covered by copyrights. Don't download or share any such material online without due permission from the copyright owner.

WHAT TO DO WHEN YOUR STUDY RIGHT EXPIRES

- The right to use the university's IT services is tied to the study right.
- When you graduate, or your study right expires, the university will close your user account and, after a certain period of time, delete your e-mail folder and other files permanently. Before your user account is closed, take care of the following:
  - Notify your contacts about the change of e-mail address.
  - Copy all files you want to keep from the university's servers for yourself, and delete the remaining ones.
  - Copy your e-mail messages for yourself or forward them to another e-mail account.
  - Uninstall all software you have installed on your own computer under rights granted through the university.

SUSPECT A MALWARE INFECTION OR SECURITY BREACH?

– If you have reason to believe that the workstation you are using is, or has been, infected by malware, proceed as follows:

1. Go to another workstation and immediately change all passwords you have used on the infected workstation. If you use the same password in several services, change it in all of them. Notify the customer support of the main services you have used about the possible malware infection and user ID theft in order to facilitate investigating the case.

2. If the infected computer is your own, don't use it until you find someone to remove the malware. If the infected computer belongs to someone else, notify the owner or person in charge about the situation. Your university's IT support may be able to provide you with some assistance in clearing the malware from your own computer. Help can also be found through the anti-virus software vendor's website.

3. If you suspect a security breach or system abuse, contact the person in charge of the service. If the suspected breach concerns a university service or a service you have used with the university user ID, contact the university's IT support. With regard to other services, send a notification to the organisation's abuse address (e.g. abuse@[domain]) or call the organisation's switchboard and ask to speak to the person in charge of information security. Clearly describe what you have observed and when it has happened. Leave your name and contact details so that you can be contacted for further information if necessary.

MORE INFORMATION AND LINKS

- Your university's information security site
  - » Learn your university's information security guidelines and practices.
- Instructions for safe Internet usage
  - » www.tietoturvaopas.fi/en/index.html
- Information about information security threats and instructions on protection against them
  - » www.tietosuoja.fi --> english
- Netiquette: common courtesy in online communications
  - » en.wikipedia.org/wiki/Etiquette_(technology)#Netiquette
- Instructions about securing communications, information security threat notifications
  - » www.cert.fi/en/index.html
- Finnish Competition and Consumer Authority's instructions about recognising scams
  - » www.kuluttajavirasto.fi/en-GB/scams/
- Information security instructions for mobile device users
  - » www.fucio.org/infosec/students-mobile-security.pdf
- Universities' cloud assessment site (in Finnish)
  - » pilviohje.eduuni.fi