01 Activate lock screen

02 Choose secure passwords

03 Keep operating systems and antivirus software up to date

04 Think before clicking

05 Use secure WLAN networks

06 Never use work profiles for personal purposes

07 Check the identity of unknown persons

08 Store sensitive data correctly

09 Use approved software

10 Report concerns

The Ten Golden Rules of IT Security

01 Activate lock screen

Always lock your screen before leaving your workspace and never leave mobile devices unattended.

Windows: ⊞ + L
Mac: ⌘ + Ctrl + Q
Mobile devices: At least one PIN

02 Choose secure passwords

Never share your password. Always use strong passwords and create a different password for each account.
A password manager can help you generate and administer passwords. When possible, use two factor authentication to protect your accounts in the event of password leaks.

03 Keep operating systems and antivirus software up to date

Update your computer's operating system regularly and use the latest version of antivirus software. This is the only way to close security loopholes and stay protected against new viruses.

04 Think before clicking

Before clicking on a link or opening an attachment, ensure the source is trustworthy to avoid unknowingly installing malware on your computer.

05 Use secure WLAN networks

When traveling, avoid using public and unsecured WLAN networks – you never know who else is using them.

06 Never use work profiles for personal purposes

To protect your work account in the event of a data leak, never use your UZH e-mail address or UZH user name for personal purposes such as social media accounts.

07 Check the identity of unknown persons

To prevent important information falling into the wrong hands, check the identity of unknown persons before sharing work-related information or completing transactions.

08 Store sensitive data correctly

If data is sensitive or confidential, encrypt it or save it in protected folders. Store physical documents in lockable cabinets and dispose of them only in specially designated containers, as normal trash containers can be searched for saleable information.

09 Use approved software

Use only software that has been pre-installed by IT or provided for download in the UZH Software Center. Do not install any software that has not been checked by IT and approved as secure. Back doors or a wiretap can be built into even the most reputable-looking software

10 Report concerns

Follow the rules and instructions issued by IT Security and contact the Helpdesk or IT Security if you feel unsure or if an e-mail seems suspicious. Every lead can help.

security@uzh.ch or **044 634 3333**

Universität Zürich[UZH]