The Little Handbook of IT Security

Three precautions to remember

This handbook was created as a part of the
IT security awareness campaign at the IT University of Copenhagen.

Text: Peter Smidt
Design and graphics: Regitze Breddal Puck

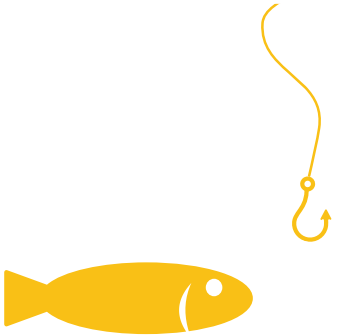
Contact for security issues and/or questions:
Security Officer Lilian Schelde Baunbæk (lils@itu.dk)

October 2016
Second Edition
September 2017

Rued Langgaards Vej 7
2300 Copenhagen S

securIT by IT DEPARTMENT

Table of contents



Be aware of phishing

Protect your password

Stay updated

PHISHING

Be aware of phishing

"Phishing" is the act of sending emails pretending to be from a trustworthy source like ITU, another university, an online store or a financial institution, etc.

The notion of phishing stems from traditional fishing, depending on the user taking the bait. The attacker will typically try to mislead you to login and give personal information through a false webpage. The intention of phishing attacks is to obtain personal information from you, such as passwords, credit card and bank information, or other private information that can be abused.

Traditionally, phishing emails have been easy to spot because of incorrect language or poor localization. However, phishing attacks are becoming more sophisticated and precisely targeted at specific groups, and can therefore be harder to spot.

Avoid getting phished

Never respond to emails that seem suspicious.

You might be asked to confirm login information or disclose personal information. But as a rule of thumb, always assume that real companies or institutions will never send you emails containing links to login pages asking you to confirm your information.

If you receive a phishing email do not respond - just delete it.

Also be aware that other kinds of attacks against you can occur through emails. For instance, you can get infected by ransomware, which can encrypt and leave all your personal files inaccessibly for good! You can get infected by ransomware by opening links or attached files in suspicious emails.

PASSWORD

Protect your passwords

Passwords are personal information,
which is only as secure as you treat it.

Therefore, use strong passwords and never share them with anyone. If you use weak passwords or expose them to others, there is a risk that people with bad intensions might get unauthorized access to IT systems and services in your name.

You should never use the same password in different places. And do not treat your passwords in unsecure ways like writing them down on a piece of paper or storing them in an unprotected file on your computer.

Change your password immediately and contact the IT Department's Helpdesk if you suspect it has been compromised!

Create strong passwords

A strong password needs some complexity to it.

Your password at ITU must be at least eight characters long and consist of both uppercase and lowercase letters, numbers or special characters.

Also, a strong password should not be easy to guess or extract from your personal information such as your name, username, phone number, birthday or similar.

Try to figure out a system that works for you to make a good and strong password that you can remember. For instance, it is a good idea to use associations or acronyms as methods for memorizing.

UPDATING

Stay updated

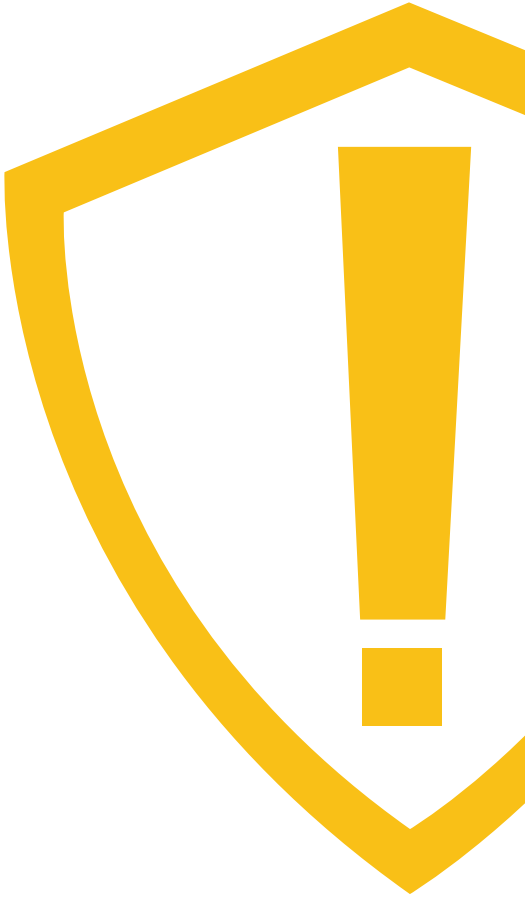
Security holes in software cause a higher risk of being infected by malicious software or even being hacked.

Every day software flaws allowing unauthorized users to gain access to systems and network are discovered. When these get publicly known, people with bad intentions will almost surely exploit it, by benefiting on people forgetting or hesitating to install security updates.

Security updates for your OS (e.g. Windows, Mac OS, Android and IOS) are often distributed to you automatically, but it is important that you apply these updates as soon as possible. In addition, you should also make sure that all other software on your devices (e.g. browsers and browser plugins) are kept up to date.

Avoid getting infected

Keep your software up-to-date and
use the newest version of your antivirus program.



To avoid getting your devices infected by malware or hacked, you should keep all your software up-to-date by accepting and installing all new security updates without delay. Also, you should use the current version of your operating system and avoid using old discontinued versions.

In addition, be sure always to use an updated antivirus program on your computer.