POLITIET

The little booklet of digital security

1.0/December 2021

No. 1: Use strong passwords

Passwords are the keys to your digital life. Make sure only you can access it!

Simple passwords are easily guessed. Avoid using passwords linked to your private life, such as the name of your pet, football team or child. Your email account should always have a password not used anywhere else. And most importantly: Do not share your passwords!

A strong password can be made up of a combination of three random words, numbers, symbols and upper-case letters. Example: 15fishAtedinnerG1!
NOTE: Do not use this password, make up your own.

No. 2: Use two-step verification

Two-step verification prevents others from posing as you online.

Criminals can steal passwords. Accounts set up to use two-step verification require another piece of information to log in. This will be something only you can access, such as a code provided via text message or an app on your device. This means that even if a criminal knows your password, your account remains safe.

Always activate two-step verification when available.
Go to https://nettvett.no/2-trinns-bekreftelse/ for guidance on how to set up two-step verification for popular online services.

No. 3: Think twice before you click attachments or share links

Clicking unknown attachments or links can give criminals access to your devices.

Received emails or texts can contain links or attachments that you are asked to click. If you do, you bypass all of your security measures. If the message was sent by criminals, they can access or infect your device.

Do a double check before you click an attachment or a link, unless you can verify its origin. You can even call the sender to verify it.
If in doubt, do not click!

No. 4: Be wary when someone asks for your personal information

Criminals can come up with any sort of story to try to trick you into giving up money or personal information.

Be it face to face, on the telephone or online, a lot of crime is based on criminals posing as someone else. They may pose as police officers, tax officials, bank employees or others you trust in an attempt to steal your data or money.

Never give up information to someone who contacts you out of the blue.
Take time to check reliable sources to verify that they really are who they say they are.
Be wary of urgent money transfers.

No. 5: Use antivirus software

Antivirus software is digital vaccine. Remember to install antivirus software on all your devices and keep it up to date.

Virus and other malware can attack any type of device, including computers, mobile phones and tablets. If a virus gains access to your device, it can lock you out and steal your information. It can even be used to put you under surveillance. Antivirus software will protect you against this.

Most computer systems have built-in antivirus protection. Make sure that you use it. You should also consider installing extra antivirus software on all your devices. The software will monitor everything coming into your devices and warn you in the event of an attack.

No. 6: Always keep software up to date

Vulnerabilities are like holes in the computer's security system. Updates close the holes.

Software is never perfect. There are often vulnerabilities or holes that criminals can use to access your systems. Once a vulnerability has been found, the software provider will prepare and publish an update to fix the problem.

Always update your software immediately when such updates are made available to keep your systems safe and secure.

No. 7: Back up your data

Make copies of your most important data. Keep the copies safe.

Your files, contacts and images may be the most important content on your computer equipment. Should your equipment break down or become infected, copies keep you from losing your most important data.

Back up your most important files at regular intervals. Store them externally, for instance on a portable hard drive, a USB disk or a cloud.
Make sure that copies are stored separate from the original files.

No. 8: Be careful when using public Wi-Fi

Public or free Wi-Fi is not secure. Someone may be monitoring your online activity!

If a Wi-Fi network is public, such as those in stores, restaurants, hotels or airports, make sure that the websites you visit are encrypted. If you can see "https" or a padlock on the address bar, that means the site is encrypted and safe to use.

Consider carefully before using a public Wi-Fi network to access something you would not like a stranger to see. Turn off Wi-Fi on your devices when not using it.

No. 9: Be critical when sharing information on social media

If you are not cautious, you may be sharing personal information with the wrong people.

Social media is a good way of keeping in contact with family and friends. However, if you have not checked the privacy settings, you may be sharing more personal information than you think. Know that when something goes on the internet, it is there forever.

Keep control of who can see what you share online, check your privacy settings and set them to a strong protection level. Do not share private information such as your address or school on social media. Make sure that everyone in your family follows this advice.

No. 10: Report cybercrime

The police cannot stop crime they do not know about. You should therefore report cybercrime and fraud attempts to the police.

Even if no money or data are lost, you should report attempted frauds and cyberattacks. This information will help the police in their investigations, stop criminals and reduce the harm they can do. Reporting crime also helps inform trend analyses and awareness campaigns to protect citizens and enterprises.

Report cybercrime and fraud online at the police website politiet.no **or call us on 02800.** On our website you can find more information from the police and cooperating agencies, as well as information on how to report cybercrime.
The response centre of the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) is open between the hours of 08:00 and 16:00. **Telephone: +47 23 29 11 00**

Prepared by Oslo Police District and the National Cybercrime Centre (NC3)

Information in English on the website.