10 Tips for Safe Internet Use

1. Customize your web browser and keep it up to date

To surf the internet, you need a browser. Extensions, add-ons, or plugins are small programs that can add extra functionality to your browser. Disable or uninstall the programs you don't necessarily need. This is often possible via the menu items of the same name in the settings of your browser. There you can also make further security and privacy settings that reduce the storage of confidential information and its transmission to third parties.

Information that provides information about you or your behavior on the internet is considered confidential. For example, "Private Mode" or "Clear History" prevent other users of the same device from seeing which websites you have visited. "Do not allow third-party cookies" ensures that only websites that you have actually visited can track your browsing behavior.

Also make sure that your web browser is always up to date. Updates also close security gaps. Use an ad blocking program to protect yourself from malvertising, i.e. the spread of malware via advertisements.

First carefully enter the addresses for particularly security-critical websites, such as online banking, by hand in the address bar of the browser and save the entered address as a bookmark, which you will then use for secure access from then on.

2. Keep your operating system and other software up to date

Use an up-to-date version of the operating system and installed programs. If possible, use the auto-update feature. You can find out whether your computer's operating system is up to date in the settings under "Update". Also, keep an eye out for references to new versions of the operating system or applications. Uninstall programs that you no longer use. The fewer applications are installed, the smaller the attack surface of your entire system.

3. Use antivirus applications and a firewall

The common operating systems have integrated virus protection and a firewall, which make attacks from the internet more difficult even in the standard configuration. Activate it or use an antivirus program from another provider.

Bear in mind that this measure can only be effective if it is accompanied. Their application does not diminish the importance of the rest of the tips mentioned here. Don't be fooled by an activated antivirus or the firewall, they don't guarantee complete security.

4. Create different user accounts

Malware has the same rights on the PC as the user account through which it entered the computer. As an administrator, you have full access to almost all areas of your PC. Therefore, you should only work with administrator privileges when absolutely necessary. Set up different, password-protected user accounts for all users of the PC. Depending on the operating system, this can be done via the (system) settings or the control panel. Only assign the permissions that the respective user needs for these accounts. This also protects private files from access by others. Browse the web with a limited user account and not in the role of administrator.

5. Protect your online and user accounts with strong passwords

Set a separate, secure password for each online and user account and change all passwords as quickly as possible if they could have fallen into the wrong hands. Also, change the passwords preset by the manufacturers or service providers after the first use.

The following criteria apply to a secure password:

- The longer the password, the better.
- The password should be at least eight characters long.
- As a rule, all available characters can be used for a password, i.e. upper and lower case letters, numbers and special characters.
- The full password should not appear in the dictionary. Common number sequences or keyboard patterns are also out of the question as a secure password.
- Adding simple numbers or special characters before or after a normal word is not recommended.

By the way, no matter how strong a password is it is of little help if you cannot remember it. A password manager can make it easier to handle different passwords and save your passwords for you. Where two-factor authentication (2FA) is offered, you can use it to further secure access to your online account.

It is particularly important to never share your passwords with third parties.

6. Be wary of emails and their attachments

If possible, avoid displaying and creating emails in HTML format, use plain text format instead. You can change the use of the HTML format via the settings of your email program. Be careful when opening email attachments or clicking on a link, because malware is often spread via images or file attachments integrated into emails or is hidden behind links. This is particularly important for emails whose sender is not known to you. If an email from a known sender seems strange to you, it is better to ask the sender whether the email is actually from him or her. However, do not use the contact options provided in the email. They could be fake.

You can identify unwanted or dangerous emails by a few characteristics, for example by hovering over or clicking on the sender you can see whether the sender is fake. Pay attention to confused letter sequences, the replacement with visually similar letters or a foreign domain, i.e. the ending of the email address. Also check the subject line and the body of the email for meaningfulness and spelling. Scammers often make mistakes here. Also, be skeptical if you are asked to react quickly.

7. Be wary of downloads, especially of programs

Be careful when downloading anything from the internet, especially if it is programs. Avoid sources where you have doubts about the seriousness. Before downloading programs, make sure that the source is trustworthy. Use search engines to get more information about the manufacturer or to obtain testimonials from other users. If possible, use the website of the respective manufacturer for download and encrypted pages, which you can recognize by the abbreviation https in the address bar of your browser.

8. Be cautious about sharing personal information

Criminals on the internet increase their success rates by addressing their victims individually. Previously spied on data, such as surfing habits or names from the personal environment, are

used to inspire trust. Today, personal data is considered currency on the internet and it is traded as such. Consider which online services you want to entrust with your personal data. The unprotected transfer of personal data in open, unsecured networks should also be avoided.

9. Protect your data with encryption

Only visit and enter your personal information on websites that offer an encrypted “https” connection. If the site uses the secure communication protocol “https”, you can recognize this by the internet address which always starts with “https” and typically displays a lock icon or a similar symbol to designate a secure connection. Confidential emails can also be encrypted, check with your email provider.

If you use Wi-Fi to access the internet, pay particular attention to the encryption of the wireless network. In your router, select the WPA3 encryption standard or, if it is not yet supported, WPA2 until further notice. Choose a complex password that is at least 20 characters long. You can access the router via a fixed internet address that is noted in your router’s manual.

If you have the option of connecting to your home network or its router via a virtual private network (VPN), you can also be just as secure in public Wi-Fi hotspots as you are used to at home. A VPN is a particularly secure connection between two points. This involves building a tunnel, e.g. from a smartphone through the public internet to your home network, from where you can then use your own internet access. Modern routers often offer the option of setting up a VPN.

10. Make regular backup copies

If despite all protective measures one of your devices is infected, important data can be lost. This also applies if the device is lost or becomes defective. In order to minimize damage, it is important to create backup copies of your data on external hard drives or USB sticks on a regular basis. These storage devices should only be connected to the PC when necessary. Cloud services can be used for backup copies of encrypted data. Restore only your data from the backup. When resetting the device after a malware infection, no programs should be removed from a backup copy, as they could already be infected.