Privacy and data protection on the Internet

An ever increasing number of data is stored on the Internet nowadays – whether you are aware of it or not. But how secure are your personal data?

Protect yourself and your data on the Internet:

- Use your browser securely.
- Be circumspect with your passwords.
- Be careful with social media.
- Be vigilant when using cloud storage.
- Configure your operating system securely.

Use your browser securely

Your browser is your gateway to the Internet. You should change some relevant settings to ensure your data are protected.

Delete cookies, or prevent them from being stored

Cookies are text files containing information about your surfing behaviour. Once you finish your Internet session, you should delete (https://www.ebas.ch/en/deleting-browser-history/) them. Alternatively, you can also surf in incognito or private mode, so that your browser doesn't store any data in the first place.

Don't store any passwords in your browser
It is a very risky practice to store your passwords in your browser. You should use a password manager (https://www.ebas.ch/en/4-protecting-online-access/) instead.

Use secure search engines
Google is the search engine used most often, but it collects a large quantity of data about you and your surfing behaviour. Use alternatives such as "DuckDuckGo (https://duckduckgo.com/) " which don't analyse or store personal data.

Use anti-tracking software
Extensions for common browsers (on PC / Mac) such as "Ghostery (https://www.ghostery.com/) " block hidden services which transmit personal data in the background while surfing. Further information (https://www.ebas.ch/en/ad-blocker-and-anti-tracking-tools/)

Be circumspect with your passwords
Web shops, e-mail accounts, e-banking, etc.: Secure passwords are critical to identify users.

Use secure passwords
The important thing to note is that you shouldn't just choose a complex password (http://www.ebas.ch/securepassword) ,

but also use different passwords for different services.

Use a password manager
Hardly anyone can remember all their passwords. A password manager (http://www.ebas.ch/securepassword) serves to save all your passwords in encrypted form.

Be careful with social media
We can no longer do without social media such as Facebook, Twitter or Instagram in our everyday lives, yet they require responsible behaviour.

Be restrained in your communications
Only publish information you would also be happy to tell any stranger in the street as well. Further information (http://www.ebas.ch/socialmedia)

Securely configure the social media you use
Limit access to the information you publish. Our instructions are meant to assist you in establishing secure Facebook (https://www.ebas.ch/en/facebook-settings/) , Twitter (https://www.ebas.ch/en/twitter-settings/) , Instagram (https://www.ebas.ch/en/instagram-settings/) and LinkedIn (https://www.ebas.ch/en/linkedin-settings/) configuration.

Be vigilant when using cloud storage
Moving data to external storage on the Internet, for instance using Dropbox, OneDrive, Google Cloud or iCloud, is quite comfortable. Yet you still have to take into account security aspects here, too.

Choose a suitable cloud provider
Those large international providers usually store your data abroad, something which can lead to local data protection laws being infringed. You should therefore choose a Swiss provider (https://www.ebas.ch/en/cloud-storage/) , if possible.

Use cloud storage securely
If possible, use two factor authentication (https://www.ebas.ch/en/4-protecting-online-access/) , similar to the method used with e-banking. You should regularly create local back-ups (https://www.ebas.ch/en/1-backing-up-data/) of all your data stored in the cloud, too.

Configure your operating system securely
Many operating systems regularly transmit reports about users to the system operator. You can usually at least partially switch off this function.

Limit data transmission in Windows
Amongst other things, Windows analyses personal data and sometimes also transmits them to Microsoft. However, you can strictly limit (https://www.ebas.ch/en/data-protection-under-windows-10/) such data transmissions.

Data protection and duty to provide information
In accordance with Swiss law, a variety of obligations are placed on website operators to warrant data are protected. For instance, a Legal Notice and data protection statement are mandatory.

Every website must inform visitors of the kind of personal data it collects and stores, and for what purpose. Such

personal data also include online Ids, for instance your ID address and click behaviour. Hence something almost every website stores.

In addition, there is the duty of disclosure: If you would like to find out what kind of data is stored about you, you are entitled to receive this information free of charge. If any of your stored data are incorrect, they will have to be corrected or deleted if you request this.

How secure are your data on the Internet? It is not a simple question to answer. On the one hand, Internet service providers have to fulfil certain requirements. On the other though, you can take some measures yourself to protect your data on the Internet.