Notes to ensure information security for personal devices

Anyone who uses the Internet on personal devices faces risks of information insecurity. However, if you have the knowledge and skills, you can limit 80% of these risks.

According to cybersecurity experts, to ensure the safety of personal device information for themselves and their loved ones, users need to take the following measures:

Software updates: Many people think that updating software is time-consuming and annoying. In some cases it is, but it is still the most important form of protection against hackers. The software works on all types of devices: Windows or MacOS operating systems installed on computers or laptops, Android or iOS operating systems installed on mobile devices.

Even routers and other smart devices in your home have software working on them. Make sure you check regularly - once a week - in case there are updates available for the devices you are using, install them as soon as possible.

In addition, you also need to update applications and software that you regularly use on your computer, which is also important, such as internet browsers, PDF readers and Microsoft Office. You will regularly receive notifications if a new version of the software is available.

Set up a strong password: Websites and applications often require you to use a password that combines letters and numbers. But in reality, it is quite easy to crack by hackers and that is why you should consider using passphrases instead of passwords. Long but easy to remember phrases are two prerequisites for a strong password.

Best way to save passwords:

- Use a password manager to generate and store random passwords that are at least 20 characters long.

- Use a passphrase.

- Write down your password and keep it in a safe place to ensure you never lose access to your password manager.

Monitor passwords regularly: No matter how strong your password is, it can still be stolen. That's why it's important to check if your password has been stolen by hackers.

Don't leave personal devices out of your control: Avoid leaving personal devices out of your control. That can create conditions for hackers and scammers to take advantage of your device to steal information or commit crimes on that personal device.

Be wary of public Wi-Fi: Using public Wi-Fi puts you at risk of others tracking your online activities, and some malware can even be transmitted over Wi-Fi. -Fi.

Two-factor authentication: To limit the consequences of losing your password, you can use two-factor authentication (2fa), which is a relatively new security method. You can enable two-factor authentication through the services you use, if they support this method.

Do a backup: Whether you use hardware (like an external hard drive) or software (like a cloud service), make sure your data is backed up to a safe location.

Note the lock icon (but don't trust it): The lock icon in your web browser's address bar indicates you're using an encrypted connection. This means that the information you are entering into the website, such as your password or credit card information, will be sent securely and cannot be intercepted by hackers. So, remember that you only enter sensitive information on websites that display this lock icon in the address bar. If a website address starts with https://, it means it is secure.

However, also note that the lock icon does not mean you can actually trust the website you are visiting. Many scam websites also use such a lock icon to gain your trust, thereby trying to steal your login information.

Pay more attention to the website address and double check whether it is correct or not. Be careful with attachments and check files you don't trust.

You finished reading the article "**Notes to ensure information security for personal devices**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
