Tips for personal data security

The development of the internet is a new development, but it also entails many consequences in terms of ensuring network security. Therefore, the following personal data security tips will help you a great deal

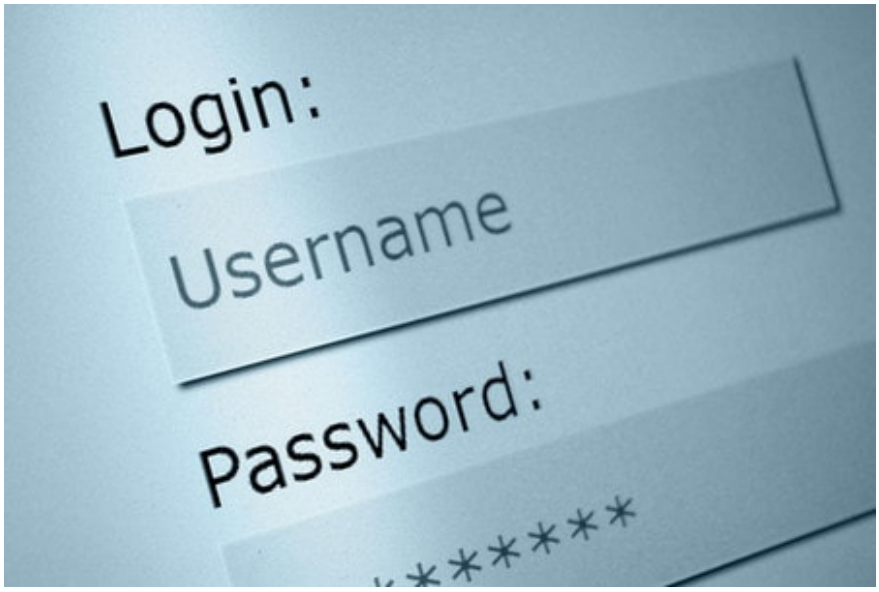
Your logging into online services as well as your daily internet use can also cause your personal information to be stolen. Or like the issue of network security in recent times has also made you more or less worried. Even though you're worried about your data being stolen, many people still have to use the internet to transact for work every day, so you have to live with the flood. So is there any solution to ensure the safety of your personal data?

The following article will give you some useful advice

Tips for personal data security

Your password must be unique and secure.

That means you must create a secure password that contains both letters, numbers and characters. Or you can create passwords like taking the first letter of each word in a sentence and using that acronym as the password.



Don't use a single password for multiple services.

In fact, using the same term for all your passwords can lead to your accounts and data being stolen. This means if a hacker gets one password, he will have all your passwords.

Enable two-step authentication

There are quite a few services that provide two-step authentication for logging into accounts. Instead of just entering a username and password, the site prompts you to enter a code sent to your smartphone to verify your identity.

Update software regularly

because updates will help you increase security. Major companies such as Apple, Google, and Microsoft often

provide security patches in their latest software updates. So don't ignore those annoying reminders and make sure your software is up to date.

Read the terms carefully before installing an app.

There are quite a few apps that ask for a long list of terms, and that doesn't mean they're all malicious. However, it's important to be aware of the types of information your app accesses which can include contacts, location, and even camera.

Check the app publisher before you install.

On Google Play, there are quite a few scam apps trying to get your personal information. In late 2012 an illegal developer posted an app impersonating Temple Run on Google Play. This app comes from a developer named 'apkdeveloper', and not from Imangi Studios - the actual publisher of the game.

Do not plug strange hard drives and portable hard drives into your computer.

Unexpectedly, you have a USB on your desk. Don't hesitate to plug it into your computer right away. Because it's very possible that someone has downloaded malware onto the USB with the intention of the person picking it up to plug it into a personal device.

Make sure the website you are visiting is safe before entering personal information.

Please enter personal information on familiar and safe sites. Avoid declaring personal information and account numbers to unfamiliar websites.

Do not send personal data via email

Because sending important information such as credit card numbers or bank accounts via email can put you in danger when they are intercepted by hackers or affected in attacks. cyberspace.

Note with online games

Hackers often use phishing emails or websites, they install malware on your computer. Their designs resemble a normal email or website to make visitors trust and hand over personal information. In fact, we can easily detect

online scams.

Do not log in to important accounts on public computers.

Sometimes you will have to use computers at coffee shops or libraries to log in to pay accounts or do something. However, a word of advice is to be sure to clear your browser history when you are done using it.

Back up personal files to avoid loss.

You should keep a copy of all important files on a cloud storage service and some type of hard drive. Because if unfortunately the files are hacked or If damaged, you will still have a backup to use. In addition, if you own the Windows 10 operating system, you should also know how to set a password on this operating system. Setting **a password for Windows 10** is similar to Windows 7, making your computer more secure.

Creating a USB security key on Windows 10 helps you protect important data on your computer. With this method, only when you plug in a USB that has been created securely can your computer be opened, quite interesting. no? Refer to how to **create a USB security key on Windows 10** for more details.