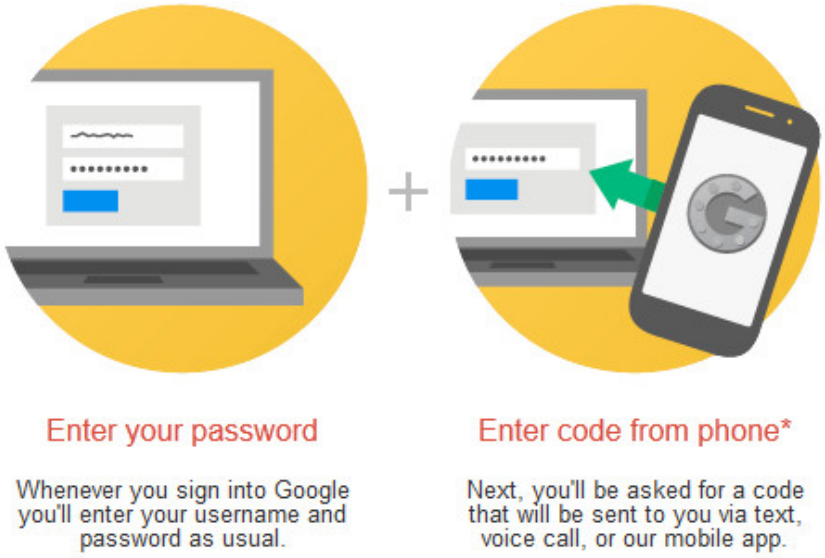
This is a way to prevent hackers from stealing your data when using public Wifi

One advice is to be cautious when browsing the Web. Never let your curiosity be the cause of unworthy errors. On your browser, block and remove all tracking cookies. Especially 'stay away' from unsafe and unknown sources (beware of free software), and stay away from 'suspicious' links sent to your email or links that appear on new feeds social networking sites.

One advice is to be cautious when browsing the Web. Never let your curiosity be the cause of unworthy errors. On your browser, block and remove all tracking cookies. Especially 'stay away' from unsafe and unknown sources (beware of free software), and stay away from 'suspicious' links sent to your email or links that appear on new feeds social networking sites.

Readers can refer to some of the methods that hackers use to attack and steal users' data when using public Wi-Fi here.

1. 2-step verification for password



According to TechRepublic, combining 2-step verification and VPN support for more secure 'sensitive' information security. This security layer is also useful in securing personal information. The VPN will "make it difficult" for hackers to read your password.

So **enable 2-step verification for all of your web services** , such as email, social networking accounts, etc. It is understandable that when you log in to any web site, the website will send you a message containing a confirmation code to enter in the appropriate box to add your password.

Once you've enabled 2-step verification, if the hackers already have your password, there's nothing to do.

2. Caution when browsing the Web

One advice is to be cautious when browsing the Web. Never let your curiosity be the cause of unworthy errors. On your browser, **block and remove all tracking cookies** . Especially 'stay away' from unsafe and unknown sources (beware of free software), and stay away from 'suspicious' links sent to your email or links that appear on new feeds social networking sites.

3. Use mobile data on your device

If registering mobile data packages (3G, etc.) on your device, it is better to use these packages instead of using public Wifi. Because when using mobile data, connections will be more secure and private, hackers will be 'difficult' to attack.

And of course, when using mobile data, you will have to pay a fee and battery capacity will also consume more.

4. Encrypt your data

When using public Wi-Fi, your computer or mobile phone sends data to the router as radio waves. You can protect your data by **encoding radio waves** . When the data is encrypted, others cannot see the data with the eyes.

Websites that use HTTPS encryption technology for your connection. Some websites like Facebook, Paypal, Google ensure your connection with HTTPS (not HTTP). And Man-in-the-middle-attack attacks also happen very rarely with these sites.

Many websites still use HTTP, one of the protocols prone to Man-in-the-middle-attack attacks. Assume that https://www.facebook.com is not connected via HTTPS. A hacker can redirect 'victims' to hacker sites disguised as Facebook. Then the hacker will collect the victim's information in this Man-in-the-middle-attack attack.

On computers and laptops, and on Chrome browsers for Android devices and Safari browsers for iOS devices, you can easily verify a site that is secured by HTTPS with a green icon located next to the URL. And it is difficult to identify which applications are encrypted, although Apple is pushing the use of HTTPS by default.

The reason is because this connection occurs within applications, so it is difficult to tell whether the application is safe or not. Even if an application uses HTTPS, it cannot be guaranteed if it is not done correctly. For example, applications can be set to accept any certificate, and therefore the application can easily be attacked by MITM.

5. Encrypt connection using VPN

Virtual private network service (VPN) acts as an intermediary between your computer and the rest of the Internet. During the connection process, the virtual private network will encrypt your data. If you use a public Wi-Fi connection and you're the victim of an MITM attack, hackers will have to spend a lot of time and energy decoding your data because of VPN encryption.

VPN has the ability to resist packet sniffing quite well. VPN will encrypt your data packets so that hackers cannot read these data. With VPN, your computer will send packets to the VPN server before redirecting to the destination. The VPN encrypts each packet, so the hacker cannot read the data between you and the VPN server and the websites you are visiting.

If your computer has been hacked, VPN will not be able to protect your data. For example, if spyware has attacked on your computer, hackers can read data before a VPN has the opportunity to encrypt that data. Therefore, you can protect yourself from spyware attacks with antivirus software and firewalls.

Refer to some of the following articles:

1. How to know if your computer is being "attacked" by a hacker?

1. How to set super strong iPhone password to hackers also "give up"

1. 50 Registry tricks to help you become a true Windows 7 / Vista "hacker" (Part 1)

Good luck!

You finished reading the article "**This is a way to prevent hackers from stealing your data when using public Wifi**" 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.