10 extremely important things that you should remember when using free Wifi

Please join us to refer to 10 extremely important things that you should remember when using free Wifi in the article below!

1. 9 absolute things you should not do when flying
2. 3 steps to choose jeans that fit without trying
3. 13 tips are extremely useful in modern life today

Free Wifi is obviously an amazing thing in today's modern technology life. However, this public network comes with many risks for you, especially if you can **lose all the accumulated money in your bank account** .

We have collected **10 extremely important things that you should remember when connecting to a free Wifi network** to ensure you never become a victim when using free Wifi.

1. Do not use Internet Banking or enter your bank card information

© depositphotos

The only way to protect yourself from data theft is to use mobile traffic to purchase online or Internet Banking. The cost of megabytes used will be a reasonable price for your account security.

2. Turn off Wifi if not using Internet

Turning off Wifi when not using the Internet helps you solve 3 problems at the same time: drain battery, automatically connect to phishing network and annoying advertising emails. To improve against these problems, you can install DoNotTrackMe extension on your browser, this extension will not let devices track your activities.

3. Connect to the Internet using a VPN

VPN (*Virtual Private Network*), or **virtual private network,** will allow you to be online in anonymized state. This means that the websites you visit only see the virtual network IP address, not your own IP address.

Network types like VPN often cost and slow down your connection. However, its price is not too high and most VPN providers still have free services.

4. Don't let that "free" network memo device

Most devices will automatically remember and connect to the hotspots they have used at least once before . Phishers can create access points of the same name so that when you don't pay attention and access, they can get your personal data or even your bank account.

5. Notice the "free" network name you plan to connect to

© depositphotos
Hackers often use networks with names similar to those already in the neighborhood. The only difference is that an authentic hotspot requires payment or authorization / password, while a fake access point is usually used for free. Therefore, before connecting a free network, **ask the owner of the site about the name of the free Wifi network** .

6. Install a quality antivirus software

Always use the latest antivirus versions . There are more and more new ways to hack your account, so you should update your antivirus software regularly.

Besides, the anti-virus software also warns you about fake hotspot connections that may be unintentional when accessing free Wifi.

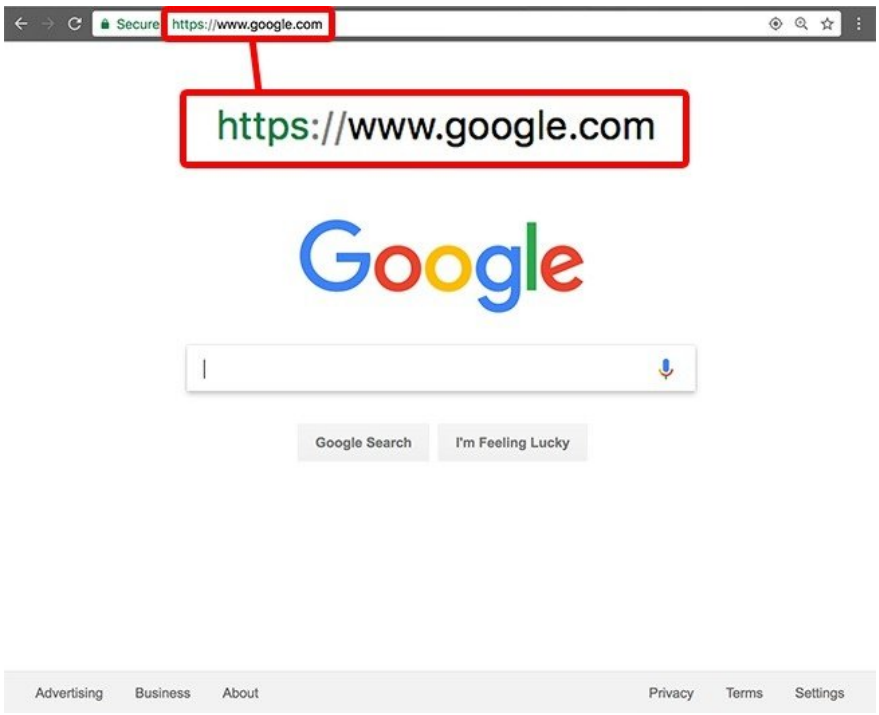
7. Select networks with 2 authentication steps

A network connection does not require any additional authentication steps when connecting, most likely a phishing network. To ensure safety, **select the hotspot that requires entering a code sent to your phone as a message** . This will protect you from online thieves when accessing the network for free.

8. Keep passwords in encrypted form

Although it is clear that passwords should not be saved on your devices, many of us often do so. This carelessness accidentally helps online criminals easily access your data. If you still want to store passwords on the device, you should at least use **password manager** - the **password manager** , to encrypt your password information.

9. Check the URL of the website you want to visit



Phishing networks may redirect to well-known sites but are actually web sites intended to collect your personal data. If you see any strange characters in your familiar website, this could be an unauthenticated website.

Google.com and ?oogle.com are not the same site! Be sure to use a reliable and secure browser, because a quality browser will find differences and warn you.

10. Use a secure connection

© depositphotos
A secure connection is easy to identify, that is: the URL will start with **https: //** instead of just **http:///** as usual. Some websites like Google often use secure connections to transfer data.

If you want all websites to be secure, install the HTTPS Everywhere extension, this extension is compatible with all popular browsers.

See also: 10 extremely useful money-saving tips that many people often overlook

Having fun!

You finished reading the article "**10 extremely important things that you should remember when using free 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.