# 4 simple ways to secure Email

Outside of Facebook, there will definitely be no more personal online space than your email inbox. Currently, email has a huge number of users and is expected to reach 1.6 billion email users in 2011.

**Outside of Facebook, there will definitely be no more personal online space than your email inbox. Currently, email has a very large number of users and is expected to reach 1.6 billion email users in 2011.** Therefore, the safety of email mailboxes is essential, especially when reusable protocols are relatively old compared to increasingly sophisticated online security threats.

Hacking someone's email address is a very interesting thing for personal information crimes. The most obvious thing these hackers want is to increase access to private conversations, steal sensitive data and personal information. Besides, hackers can also delete messages with the intention of destroying valuable information.

For ordinary online users, the most serious threat when email is hacked is that criminals can use their account to search for keys to open other online accounts, such as financial services. Primary Banking and PayPal. Many websites have secure login portals, allowing users to get back their forgotten username or password. When these sites send that information to your registered email account, it is assumed that only you can access that account. A hacker who has hacked an email account will be able to increase direct access to many things from Facebook accounts to investment accounts, banking and other utilities.

There are four lessons in email security that can help businesses and email users avoid attacks:

**1. Divide the 'eggs' into multiple baskets**

Be aware that email addresses are often provided for free, so reduce your risk by spreading your inbox exposure. For example, using a work email address, a personal email will keep sensitive information when hackers can break into your personal account.

Better yet, you can use separate email addresses for registered accounts on safe and unsafe websites. Some are used for registration on dozens of websites, some related to sensitive information like banking, and others are used for communities. Using other email accounts for secure sites will prevent hackers from forging you to increase access to these sites if they have hacked the account you use for idle sites.

Email readers, including Outlook, Windows Live Mail, Thunderbird and Apple Mail can be configured to simultaneously check multiple accounts (including Gmail) to minimize the inconvenience of having to open multiple tabs on the different accounts.


**2. Against sniffing software (sniffer)**

According to hackers, sniffers are the type of software that can interpret data moving around the network. Depending on the level of security of the network, it can sniff wireless connections and run wires. More typing can be useful for finding password information and logging in when it is transmitted in the network.

The best way to avoid this data sniffing is encryption - by the way, all the hacker sees will be useless. When using email, there are a few classes to consider:

Webmail: When reading an email using a web interface, such as Gmail, Yahoo Mail, or your service provider's webmail reader, you need to use an HTTPS connection instead of HTTP. Google recently upgraded Gmail security by using HTTPS as the default connection type.

When accessing the webmail, look at the URL in the address bar and check if it starts with https: //. Many browsers also display a lock icon when connecting to a secure site, such as online shopping or banking sites. If webmail does not use https, then you need to manually enter these characters; If after entering, still cannot access the website you need to visit, it means that your provider does not support secure connection, then it should be noted before proceeding: the use of webmail via connection Simple HTTP will easily expose login information and mail content before sniffing software in the network.

Email client: If you use an email reader, such as Outlook or Apple Mail, you can then configure it to securely connect to these clients. When installing accounts, you need to choose a POP or IMAP connection - both are done in safe mode, this is an option in the account configuration.

Note that POP and IMAP connections only encrypt the login data - username and password - to the email server. These protocols do not encrypt the entire email content.

Your email client can also provide the option to enable TLS (Transport Layer Security). TLS is basically the same as HTTPS, which means that it will encrypt all data transferred in the network (between server and client). One important thing to note here is that TLS does not encrypt inbox - your inbox messages are not encrypted and anyone accessing your email account can read the messages. TLS only encrypts messages during transmission.

**3. Note when using webmail**

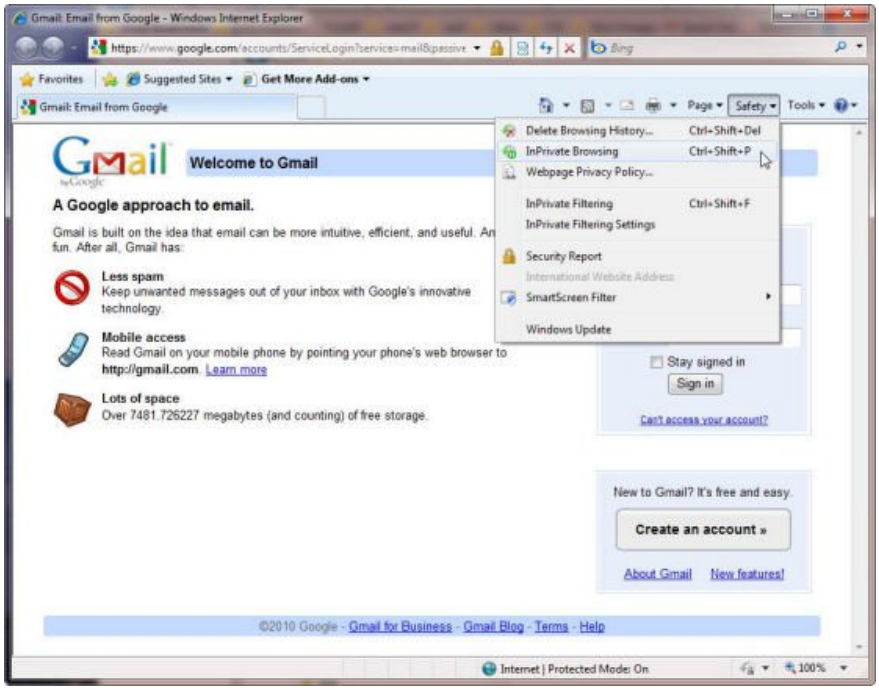
The emergence of webmail services, such as Gmail, Yahoo Mail and even Outlook Web Access, allows users to conveniently use email anywhere through a web browser. However in the process of using the user should have some note.

When using webmail on public computers, such as computers at the library or in the dormitory (or simply browsing on someone's computer), you need to avoid leaving the information behind. these computers.

The most obvious way to prevent it is to log out of the webmail before leaving the computer. The most cautious of us can also forget this simple step, especially when drunk with things like iPods and iPhones.

However, this simple logout will not be enough to combat an experienced hacker. A sophisticated hacker can use the computer you just used, copy browser history and cookies to a USB drive to perform data analysis later. Any useful card or suggestions for webmail accounts can be used. While these logs may not have enough of your passwords, they also provide enough information to cater to the starting point of an attack.

Closing the browser after the session is a good idea. This method can erase some log information. Better yet, you can switch from public browsing mode to private mode before connecting to webmail. It should be noted that not all web browsers support this private browsing mode and switching to this mode in browsers is completely different, so you should see their instructions. You need to remember to exit private mode when you do not use webmail, then the browser will destroy all history or cookies associated with your working session.




**4. Keep the operating system uninfected**

In the above section we have not mentioned the email account password. Obviously the length or combination of some special characters into the password may be a bit safer, but there will be no difference if the computer is infected with malware.

This is a big problem today - malware from infected software and downloads can install keyloggers or some other type of sniffer software on your computer, from which the software will get the password. you enter (or save before).

Therefore, the best way to prevent your email passwords is not the password itself, but rather to keep your operating system healthy and free from malware. That means you need to deploy malware scanners, such as Windows Defender, Windows Security Essentials, or third-party tools like AVG, Avast, Spybot Search and Destroy, or Malwarebytes, these software. will help you reduce the chance of causing infection from malware stealing passwords.

You finished reading the article "**4 simple ways to secure Email**" 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.