

7 steps to use a secure credit card online

Accessing websites starting with https, certified by security companies or not using computers and public wifi for transactions will help users be safer when making online payments.

Accessing websites starting with https, certified by security companies or not using computers and public wifi for transactions will help users be safer when making online payments.

Like the real world, there are many pitfalls on the Internet that scammers spread out to get rich quick. Here, they have many tools to operate anonymously and are hard to detect. However, just follow the steps below, you will be better protected when paying by credit card on the Internet.

1. Always use credit cards when paying online



Credit cards will be safer than debit cards when making online payments.

The first rule to be safe when paying online is to use only a credit card, not a debit card. They are better able to protect users and in the US, cardholders only lose up to 50 USD in case the card is stolen. Many types of cards also allow users to spend no money.

2. Check the 's' on the website address

When entering personal information, make sure the website address you are visiting starts with **https://** rather than **http://**. The word 's' means this website uses an encryption system to protect user information. Of course, this does not guarantee 100% you are safe, but at the very least, it is the fastest and easiest way to check if you are being protected.

3. Do not use public computers

If the website sets the login mode, other users can access your account. Even if you have logged out, hackers can still retrieve information if you install keyboard monitoring software.

Even if you use a laptop or personal phone, you are still unsafe if you access the public wifi network. It is best to use your own home wifi or install a virtual private network (VPN) if you have to go to a public network.

4. Always update antivirus software

All computers need antivirus software. If not, this is like opening your door to theft. Please install a good software and update regularly. Fixes for the browser and operating system are also essential. For those who are not tech-savvy, this can be a bit complicated. But today, all these steps are almost done automatically, as long as you have the software installed.

5. Check the website's certification

Most legitimate websites are certified by security companies such as **McAfee**, **Better Business Bureau**, **VeriSign** or **TRUSTe**. It will help users feel more secure when using the services of these sites. Certificates can also be counterfeited, but if not, you will also have to consider when filling out personal information.

6. Set a secure password

Pay attention to setting a password. It is best to have both numbers, letters, capital letters, lowercase letters and at least one special character such as @ or %. Do not use explicit information such as name, identification number or even the word 'password'. Different accounts should also have their own passwords.

7. Analyze the situation before acting

If a website has a problem, such as a poor interface or an old-fashioned look, you should no longer visit it. Big names like *Amazon* or *Best Buy* will be much more reliable.

Besides, if you receive an email with a link to the website, never click directly on it to shop, even if it's a famous company. Instead, you can manually type the address or search on Google to avoid fake links.

You finished reading the article "**7 steps to use a secure credit card online**" 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.

