8 safe ways to use IE8 for online purchases

Here are 8 tips, simple but very effective, to help online 'followers' protect themselves against hackers and viruses, along with Internet Explorer 8's web browser.

Security and information security solutions are always worries of customers when participating in online transactions and payments. Here are 8 tips, simple but very effective, to help online ' *followers* ' protect themselves against hackers and viruses, along with Internet Explorer 8's web browser.

According to comShore research firm, the e-commerce market in the US on **Friday alone** has achieved a turnover of US $ 595 million, an increase of 11% compared to this shopping day in 2008. These That number is the most convincing evidence of the ongoing growth of online shopping needs.

In e-commerce environment, all forms of transactions, payments . are conducted through the Internet. Therefore, **the security as well as login information, accounts need to be very carefully protected against hackers or viruses, keyloggers . stalking at any " *corner* " on the network** .

And here are eight shared tips for users to be assured of *'hackers'* or other more sophisticated computer viruses with Microsoft's Internet Explorer 8 browser.

1. Only download, use and update the software provided by the vendor's home page at ***Microsoft Download Center*** . This will prove the obvious origin of the software used including the latest browser is IE 8.

2. Install anti-virus software, prevent spyware, malware, trojans and keylogs . in the most effective and appropriate way. These programs will combine with IE 8's security system to prevent bad factors hiding on the network to attack, hack users' passwords and accounts.

3. Always open the smart website selection feature (*SmartScreen Filter*) of IE 8 with the ability to notify users of websites that contain spamware, malware (spyware, advertising) or keylogs (software to steal passwords and accounts) . often hide themselves to prevent. IE 8 users can easily find this SmartScreen Filter feature on the **Safety** tab in the upper right hand corner of the browser interface.

4. One of the most common errors of web surfing software is that **XSS** attack (Cross-Site Scripting) is also very well blocked by IE 8 with the source selection feature (XSS Filter). Built in this browser and always in active state.

Cross-Site Scripting , also called XSS for short (instead of referred to as CSS, to avoid confusion with HTML CSS-Cascading Style Sheet) is an attack technique by inserting dynamic websites (ASP, PHP, CGI). , JSP .) dangerous HTML tags or script scripts can be harmful to other users. If you are using IE 8 with the **XSS Filter** function **enabled** , the fear of being attacked by *hackers* when accessing the web will not be as big a problem as before.

5. For a long time, fake (***fake***) websites look just like the real thing. It is always a concern for any web visitor because they have nearly identical domain names to the official sites we want to access. confused, from there can steal accounts as well as the password of ' *victims* '. However, when typing the name of any website in the process of using IE 8, the feature clearly marks and blackens the domain name, the domain of the website that is officially approved by this browser maximizes its ability to distinguish it from fake information pages to avoid unfortunate " *accidents* " for users.

6. IE 8 also ensures the privacy, password, and personal information of web surfers with individual selection (*InPrivate Browsing*) in the Tools tab of the browser interface. This feature will help to hide frequently accessed information stored in temporary Internet access data such as web addresses, accounts, passwords . in order to avoid the above information may be monitored by others.

7. If you have not really trusted your security when accessing websites with payment and payment features and directly related to credit cards, one of the characteristics of online transactions and payments, IE 8 will help you **verify and encrypt** these payment sites.

With any information that does not match the correct information about your account or credit card (including errors in the process of typing a website address) **IE 8** will appear a lock icon (**block access**) in the address bar or on the bottom right of the screen. In case all information is matched and correct, IE 8 will have a green address bar to emphasize and confirm access.

8. The last and equally important advice for all users is **that never responding to e-mail messages of unclear origin** requires updating personal account information. Providers will never send mails or messages of unknown origin, lack of determination to require users to provide passwords and account information.