Instructions for online security protection

Use these tips to protect you against security attacks associated with your actions on Facebook, MySpace, or Linked-In.

Andrew Brandt

Network Administration - It can be said that social networks are quite interesting and useful for many friends' work, a great way to keep in touch with friends, business contacts and other relationships. . However, in addition to the above advantages, social networks also have certain disadvantages: for example, someone knows you are using these networks fascinated, they can exploit the information about you. up there.

There are also other online security threats that can come from revealing credit cards and Google privacy factors.

Traps of social networks

Reasons for concern : Secret links can use social networking sites to infect, fake and spam you.

Fix : A message from one of your friends appears in your inbox, sent via a social networking site you regularly use, such as Facebook.

This message promises to give you a smile and point to websites you've never heard of before. You think you can trust it, so click on the link - and what has come, your computer will be misdirected to a fake page to steal

login details or Take you to a download page used to infect your system by a password-stealing Trojan horse. Meanwhile the fact that your friend said she never sent you that message ever.

Crime can be a fake LinkedIn profile page for dangerous URLs or it can be a fake Twitter message that comes from your friends, so social networks quickly become new environments most against malware attacks. As operating systems and applications become increasingly difficult to hack directly, online crime types have realized that it will be easier to attack users by clicking on bad links. , open dangerous files and run malicious software. The best place to exploit is trust between friends and colleagues, which is the mechanism of social networks themselves.

At this point, most Internet users are knowledgeable enough to recognize spam emails. But what happens to spam tweets is unpredictable because it comes from one of your friends and takes you to a page that is almost like the page you use to log into Twitter. Data thieves who want to control your account take random actions to send messages with URLs - one of which is used to infect recipients' computers with malware. - to anyone in the social network.

Facebook and MySpace users had to deal with some types of worms and other unpleasant issues spread regardless of any action taken by the account holder.

Remedy : If you think your social network account information has been compromised or stolen, report your suspicion to the site's support team immediately. Change your password on a regular basis and avoid clicking on links that send you back to the social networking site, but instead directly type the address of the page into the browser (or follow the bookmark you saved. from before) to return to your account.

Credit card exposed online

Reasons for concern : Addressing the fraudulent credit card burdens can be quite complicated and time consuming.

Scenario : When checking an email, see a message from a large online retailer announcing that the order you recently returned is ready to ship - but you have not actually ordered anything. Follow a link in the message to return to the site's login page (assuming so), the page includes web forms that list the wrong credit card number and address for your account and requirements make you fill in the correct information so that the company can begin its dispute resolution process.

You enter the credit card number, expiration date of the card, address, CVV number (card verification value) printed on the back, date of birth, and . Completely by chance that way provides a lot of important credit card information into the hands of online scammers.

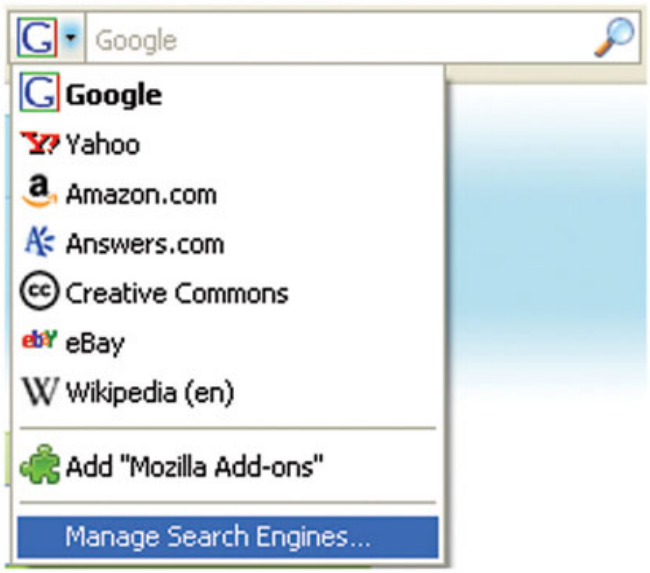
Consumers never have a legal obligation of over $ 50 in fraudulent credit card fees, so you may wonder whether the theft of your credit card information is a way to respond. pay for this action. The answer is correct. You can not pay directly and immediately for fraud, but all credit card users have to take a charge in the form of fees and interest rates to secure costs with credit card issuers.

In addition, it will take considerable time to cancel credit card accounts, replace them with newly issued cards, check your card reports, change the number in your account if you use them. for automatic payment.

Remedies : Some large banks still offer single-use credit card numbers - you log in to the bank's website and recognize the overall number of purchases from the online store concerned. , the bank site will respond by giving

out a credit card number that can only be used with that number and in that online store. ShopSafe of the US bank, Citibank's virtual credit card number and some of Discover's secure online accounts still ensure safety, though American newspapers have also destroyed a similar service. here many years.

Google and your privacy



Reasons to care : Any business that maintains too much information about you puts you at risk for data-related issues.

Scenario : Google appears to be appearing in areas. From running a massive search engine, this company has provided a lot of services for emailing, receiving news feeds, and selling online. In addition, many of your favorite websites often use Google to advertise, share content, or even check their own performance. Your Google account is like a diary for all your online work: It can track your surfing behavior and even show you the trends you may not not knowing.

Huge amounts of information that Google manages from increasing users: email, IM, VoIP, phone calls, photos, maps, finance and portfolio, home and work addresses jobs, references, interesting videos and reviews, online sales, the most frequent searches, search results. Can you trust that a certain business has too much valuable information about you that needs to be considered.

Remedy : You can remove yourself from Google, but don't acknowledge that the letter 'G' is not in your mind. So the good way here is to change Google's default search settings in Firefox if you have to; Stop using your Gmail, iGoogle, and Google Account if you really need it. However, too many sites incorporate the common components, analyzes, and benefits of the company, from which quitting the Google system is almost impossible for anyone using an Internet connection.

You finished reading the article "**Instructions for online security protection**" 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.

© 2019 TipsMake.com