

Protect Your Identity Online

Written by www.WootHosting.com
Thursday, 15 January 2009 00:17 -

Every time you go online and conduct some type of transaction, whether it is monetary or an exchange of information, you put your identity at risk. Unfortunately, criminals use the Internet too, making use of the technology to perpetrate identity theft. This type of cyber-criminal gathers personal information online and either sells it to others for profit, or uses it to his/her own purpose.

Luckily, there are many things you can do to stay one step ahead of these "bandits" and keep your identity as safe as possible. The Internet landscape is always changing, so you need to keep on top of things if you want to remain as safe as possible.

The first thing you need to do is learn how to avoid phishing scams. Phishers use fake e-mails and websites to pretend they are actual, trustworthy companies and institutions, such as banks and insurance companies. When people receive a fake e-mail or are directed to a counterfeit website, they are tricked into revealing passwords, credit card numbers, and other such information. Be warned: the criminals are good at what they do, so you must be very careful when dealing with e-mails from your bank or other organization. The key thing to remember is that real institutions never ask you to verify personal information online - be cautious and contact the sender directly, over the phone, to authenticate the request and, if necessary, provide any information they might actually require.

Because many phishers use spam e-mail as a way to obtain your personal passwords and information, install a good spam filter to keep out as much spam as possible. If you strain out most of the problem e-mails from the get-go, you won't have to worry about dealing with too many suspicious messages on your own. Also, avoid sending any sensitive information via e-mail or instant messengers. Scam artists are notorious for intercepting e-mails and IMs. Use common sense when dealing with e-mail as well. For instance, avoid opening e-mail or IM attachments that you deem suspicious. Only open files from someone if you know the sender and what they are sending you.

Protect Your Identity Online

Written by www.WootHosting.com
Thursday, 15 January 2009 00:17 -

And **NEVER send your social security number over the Internet**. No one should be requesting it, but if you are asked for it, confirm who is requesting it and send it directly to that person.

Another great way to prevent ID theft is by password protecting all your computers, laptops, and PDAs. For each item, come up with a unique user name and password. The same rule should be followed when selecting passwords for any online activity. Why? If one password is discovered by an individual with ill intentions, and all your bank accounts, credit cards, and other private logins use the same password, he/she could gain access to everything. When selecting passwords, create them with letters, numbers, special characters, and make up nonsense character strings not found in the dictionary. These will be much more difficult to decipher by a potential scammer.

Keep the amount of personal data present on your computer to a minimum. In the event that your computer is hacked or your laptop is stolen, you will be much less prone to ID theft because you won't be giving the thief much to work with. Another good idea is to install a personal firewall program. Although systems such as Windows already contain a basic firewall program, setting up another program will ensure that your computer is hidden from hackers, stop intruders from reaching sensitive information, and let you control Internet traffic.

Purchase antivirus software and keep it updated. A high-quality virus protection package can help prevent and eliminate viruses, Trojan horses, and other dangerous items designed to steal your personal information. It will also scan e-mail and IM attachments for viruses.

In addition to antivirus software, be sure to equip your PC with the latest in anti-spyware protection. Although a great many of the spyware programs out there simply monitor your online actions for the purposes of marketing, some have been created for malicious reasons, including keystroke logging and, of course, identity theft.

One last tip: when you decide to update your computer and throw away or sell your old one, remember to remove all your data from the hard disk. Many people mistakenly believe that simply deleting files makes them disappear - but this is not the case. When you delete files they are still present on your hard drive, and have to be erased prior to handing the machine over to another person. Software known as wipe programs or shredders can be used to overwrite data

Protect Your Identity Online

Written by www.WootHosting.com
Thursday, 15 January 2009 00:17 -

with zeroes or random patterns making it completely unreadable.