



How to Avoid Getting Ripped-Off Online

by: Jim Edwards

(c) Jim Edwards - All Rights reserved

Online security is one of the top catch phrases these days, but hardly anybody knows what it means and worse, most home computer users think security only applies to corporations and online businesses.

Most people think online security means simply protecting your credit card data from fraud and theft, but it actually goes way beyond that.

The potential for mayhem and just plain disruption of your life doesn't just mean credit card fraud - it can mean having your identity stolen, your life disrupted and spending hours cleaning up after an online 'vandalism' attack.

You must protect yourself from everyone from the teenage computer hacker to the organized crime syndicate using computer worms and keystroke logging viruses.

The great news is that a number of simple techniques should protect you against the vast majority of threats, since the evil doers will simply move on to easier pastures.

Update your anti-virus files

The widespread 'Bad Trans' worm logged keystrokes and transmitted potentially sensitive data such as credit card and social security numbers to the 'bad guys'.

Though this virus contained a high level of criminal intent, it was easily blocked by anyone with up-to-date anti-virus files.

If you don't have anti-virus software with current virus definitions installed, you leave the door wide open for security problems.

Install a 'Firewall'

A firewall helps prevent unauthorized access to your computer by 'hackers'.

It closes off the entry points (called open 'ports') carried by virtually every computer connected to the Internet.

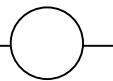
A common misconception is that firewalls are only for people with cable or other high-speed connections.

Even if you use a dial up connection to get online, a firewall can help you detect and prevent people from logging on to your computer, stealing files or even using your computer to break into others!

You can take a free test of your computer's security by logging on to <http://www.symantec.com/securitycheck/> and clicking 'Find out today if you are safe'. The results may surprise you.

Use secure sites

Only give sensitive data such as credit cards, social security numbers and important passwords over



a secure connection.

This means the little yellow lock appears in the lower part of your browser and nobody but the website you are connected to should be able to read the data you send.

Change passwords often

An easy way for you to protect your sensitive data and email is to change your passwords on a monthly basis, or even more often depending on how frequently you use computers away from home.

If you log on to your email at the library, in 'cyber cafes' or any other remote computer then the possibility exists that computer could have a key-stroking virus present.

This means everything you type into the computer (passwords, birthdays, social security numbers, credit cards) could be logged and used by someone else.

** Change your passwords at lease once a month.

Though not fool-proof, these security tips should help reduce your vulnerability and keep you safer online.

About the author:

Jim Edwards is a syndicated newspaper columnist and the co-author of an amazing new ebook that will teach you how to use fr^e articles to quickly drive thousands of targeted visitors to your website or affiliate links...

Simple "Traffic Machine" brings Thousands of NEW visitors to your website for weeks, even months... without spending a dime on advertising! ==> <http://www.turnwordsintotraffic.com>

This book may be given to a third person as a gift but cannot be modified in any manner.

Thise rule have been established to protect the rights and ownership of the authors and to ensure that their work is upheld as their own