

Get savvy on Internet scams!

[Libby Carty McNamee](#)

Richmond.com

Monday, October 25, 2004

Get savvy on Internet scams!

Top Ten Tips to Protect Yourself Against Potentially Losing Your Identity, Money, and Sanity to Internet Scams

10. Don't use the same password to access all of your online accounts. Also, don't permanently plug any of your personal passwords into your computer. If a criminal successfully hijacks your computer and gains control of it, that person would have instant access to all your accounts. Years of saving and investing could be gone in a matter of minutes.

9. Beware of rampant "spyware," technology on your computer. This spyware monitors your actions to gain information about you and sell it to advertisers. A recent study found spyware on 80 percent of the computers participating in the study. In fact, the problem posed by spyware has gotten to be so severe that members of Congress are currently debating the Internet Spyware Prevention Act. This Act would provide the Justice Department with \$10 million to fish out phishers and other online scam artists. Download free spyware detections programs such as www.spybot.com that will run a clean sweep of your computer.

8. Don't leave your connection to the Internet active when you are not using it. It provides the perfect opportunity for a hacker to take over your computer unbeknownst to you. It is worth taking the time to log out.

7. Beware of online investment newsletters that recommend certain stocks, especially those that pressure you buy quickly before the price goes down. Although these reports may appear to be unbiased and chock full of helpful information, some are downright fraudulent. Some companies actually pay newsletter writers to recommend their stock and fail to disclose that information. Sometimes the very newsletter writers themselves are trying to drive up the price of the stock based upon their own hollow recommendations, hoping to profit handsomely from the rise in the stock value.

6. Also watch out for online bulletin boards with various "threads" on investment strategies. You don't really know with whom you are really dealing. Even if the person claims to be an outside observer, proceed with caution. For all you know, it could be an insider. Or all the thread could be the exact same person using several aliases. Verify any information that you receive by researching it using another unrelated source.

5. Don't ever respond to an unsolicited e-mail from your bank or any trusted financial institution such as E-bay asking you to provide any vital personal account information in reply. Be skeptical no matter how legitimate they appear. It is surprisingly easy to generate thousands of spoofed e-mails that appear real and directed to you personally. In reality, chances are quite high that such an e-mail is fraudulent. Most likely it did not originate from your bank but from a fake website that looks real. A criminal may be "phishing" for your financial information to steal your identity, your credit and/or your cash. Don't let these criminals dupe you into giving out your social security number or any other personal information. It can never hurt to be too careful as phishing attacks are becoming increasingly sophisticated. Often phishers can reference the legitimate domain name within the body of their e-mail that actually links up to their own illegitimate site.

4. Do not call the number listed on the e-mail from your bank or financial institution that you believe may be fraudulent. I'll bet you the Brooklyn Bridge that the number provided on that e-mail is fraudulent as well, leading you to a phony call center run by – guess who? – the phishers themselves. Instead, log onto to the official website yourself and obtain the real number listed there to call into the bank and inquire about the suspicious e-mail that you received.

3. Check for and download daily Microsoft updates from www.microsoft.com, a free service that provides patches to combat the latest scam unleashed on the Internet.

2. Never ever open up suspected "spam," even to ask that they take your name off the list. Spam is junk e-mail usually sent in bulk that attempts to sell you something or make some sort of financial investment online. That is a surefire way to let the "spammer" know that you have an active account. Unfortunately it will have a boomerang effect, encouraging yet more spam to head your way. And, God forbid, never buy or invest in anything from a spam e-mail or the barrage of junk e-mail will only get worse. Can you say "sucker?" Chances are good you will never get what you actually paid for in the first place. Make sure the company is legitimate by double-checking their references, address, phone number, and Secretary of State to make sure it is properly incorporated. Check with the Attorney General's Office to see if anyone has filed complaints. Beware of those pesky illegal "pyramid" schemes that ask you to send money to ten people. Don't let yourself be one of the taken.

And, drum-roll please . . .

1. The Number One Rule for protecting yourself on the Internet --

Use your common sense. If a deal proposed on the Internet looks too good to be true, it probably is a fake! Ignore those "exciting, low-risk investment opportunities" to invest in anything from seahorses to pork bellies. No investment is risk-free or it wouldn't be an investment. There is no such thing as a "guaranteed" return on an investment. Stay away from overseas investments no matter how attractive. If the deal falls through and you are out of a lot of cash, it is extremely difficult for American officials to investigate and

prosecute foreign criminals. If you must participate in any of these ventures, pay by credit card, although give out your number sparingly. Your maximum exposure is usually \$50. At least then you can call your credit card company and have the company charged back for your purchase.

Libby Carty McNamee is a lawyer and freelance writer living in the Richmond area. She can be contacted at libbymcnamee@yahoo.com and 804-378-8218. This article does not constitute legal advice. If you need legal assistance, please contact a lawyer.