



Personal Technology

How to Avoid Cons That Can Lead to Identity Theft

Published on May 1, 2008
by Walter S. Mossberg

When most people think about Internet security problems, they focus on viruses and spyware — technological attacks that can usually be mitigated by technological defenses. But the most insidious Internet security problems today rely on human gullibility, not tricky software. While technological defenses can help you fend off these newer types of attacks, your best weapons against them are common sense, alertness, and careful email and Web-surfing practices.

These types of attacks are called “social engineering,” and they are used by criminals to steal your money and identity, and to plant on your computer malicious software that can be used to keep ripping you off. Social engineering is the online equivalent of an old-fashioned con game, in which a crook frightens people with false warnings, or tempts them with false promises, and then robs them.

While viruses and spyware overwhelmingly afflict Microsoft's (MSFT) Windows users and spare users of Apple's (AAPL) Macintosh computers, social-engineering schemes can ensnare Mac users as well. There's nothing inherent in Macs that makes their owners more resistant to falling for social-engineering scams.

The most common form of social engineering is called phishing, a one-two punch using both email and Web browsing to trick people into typing confidential information into Web sites that look like the sites of real companies, especially financial institutions. But these phishing sites are actually skillfully designed fakes that transmit your sensitive data to criminals, often in distant countries. Once these creeps have your passwords and account numbers, they can loot your funds and steal your identity.

Here are some tips to help you avoid being the victim of social engineering, updated from a similar column I wrote in 2006. It includes information on some antiphishing software that wasn't available back then. But remember: Security software alone can't save you from scams.

1. Never, ever click on a link embedded in an email that appears to come from a financial institution, even if it's your own bank or brokerage and even if it looks official right down to the logo. The same goes for payment or auction services, like PayPal or eBay (EBAY). Don't do this even if the email asserts that your account has a problem, or that the bank has to verify your information. And certainly don't enter any passwords, Social Security numbers or account numbers directly in an email.

These types of emails are almost always fakes, and the links they contain almost always lead to phony Web sites run by criminals. The only exception might be a confirmation email from a brokerage firm concerning a trade you know you made minutes before. Even legitimate-looking addresses in emails or in the address bar of Web browsers can be fakes that hide the crooks' true Web addresses. The lock icon on a Web site can also be falsified.

If you are truly worried about your account, call the bank or company, or go to its Web site by manually typing in its address or by using a well-established bookmark in your browser that you created yourself.

2. Don't click on links to offers for free software or goods that you receive in an email, especially from a sender or company you've never heard of.

3. Never download software from unfamiliar Web sites unless you are absolutely sure you need it and it's legitimate. Even if it claims to be a useful program, it may very well be a malicious application like a "key logger," which can report back to crooks everything you type into your computer. If you really want the program, do a Web search on it first, to see if others have reported it as a malicious fake.

4. If a Web site tells you that you need to download special viewing software to see its videos, don't do it. Even if it claims to be giving you legitimate viewing software, like Microsoft's Silverlight, Adobe's (ADBE) Flash or Apple's QuickTime, don't download it there. Go to the official Microsoft, Adobe or Apple Web sites to get these viewers.

5. Use a Web browser, like Internet Explorer 7 on Windows, or Firefox 2.0 on Windows or Mac, that includes built-in features to warn you about, or block access to, known phishing sites. The next versions of these two browsers will have even stronger features that will detect sites that are not only fake, but which are known to distribute malicious software.

Unfortunately, the third major browser, Apple's otherwise excellent Safari for Mac and Windows, lacks any such antiphishing detection, though I expect Apple to add the feature in a future version. So, for now, Mac users worried about phishing should rely on Firefox.

6. Consider security software that tries to detect and block phishing sites. McAfee's (MFE) free Site Advisor and paid Site Advisor Plus products do a good job. Symantec (SYMC) has similar features built into its large security suites, Norton 360 2.0 and Norton Internet Security 2008.

7. Educate yourself by reading about social engineering and phishing and how to avoid being a victim. Microsoft has a very good guide at: microsoft.com/protect/yourself/phishing/identify.msp and Symantec has one at: symantec.com/norton/clubsymantec/library/article.jsp?aid=cs_phishing.

Follow these tips and you'll be a happier — and safer — surfer.

Find all of Walt Mossberg's columns and videos online, free, at the new All Things Digital Web site, <http://walt.allthingsd.com/>.

- Email him at mossberg@wsj.com.

Return to: [How to Avoid Cons That Can Lead to Identity Theft](#)

Brought to you by The Wall Street Journal | © 2005-2008 Dow Jones & Company, Inc. All Rights Reserved.