

How to protect yourself from e-mail scams

By Robert Vamosi, Senior Associate Editor, Reviews, www.zd-net.com
Monday, Jan. 19, 2004

Shortly after the first of the year, EarthLink customers received an e-mail requesting that they update their personal account information. The e-mail contained a link to what looked like an EarthLink Web page. However, the message requested information, such as social security number and mother's maiden name, that an ISP shouldn't need to know. The other thing that made me suspicious of this mailing was that the e-mail I saw was sent from an MSN.com account. Turns out I was right: It was a scam.

A good firewall--like ZoneAlarm Pro--won't stop “phishing” scams from reaching your inbox, but it will protect your privacy by flagging you anytime your personal information is about to be sent out via e-mail or the Internet.

Since that e-mail circulated the Net, I have heard from many readers involving similar hoaxes--what are often called "phishing" expeditions. These scams invite you to volunteer personal account information under the pretense of a legitimate business transaction. I've written about this phenomenon before, and urge you to read that previous column (if you haven't already) for advice on how to spot these scams and make sure you don't become their next victim.

BUT GIVEN THAT there have been so many phishing scams lately, involving everyone from Citibank and BankOne to Amazon and eBay, I'd like to update you on how these scams work and how to report them to the proper authorities.

Let's start with how they work. It all begins when you receive an HTML e-mail that displays legitimate-looking logos and graphics from the company being spoofed. But if you look closely, there may be typos, or e-mail addresses or URLs that have nothing to do with the company.

The e-mail often contains a link that leads you to a site that looks like the victim company's, but is actually fraudulent. The latest technique for doing this is to place a percentage sign and some numbers--such as "%00" and "%01"--or an ampersand sign between a legitimate Web address and the fraudulent one, so that the legit address displays first should you mouse-over the link. For example, the URL "<http://www.earthlink.net/security@www.fraudlink.com>" would take you to www.fraudlink.com, even though at first glance you might think that link was for an EarthLink page.

For those who want to know exactly how this is done, a Microsoft Knowledge Base article explains the process, and also offers some helpful tips for avoiding fraudulent sites. Interestingly, Microsoft has known about this URL flaw within its Internet Explorer browser for some time, yet hasn't offered a patch or a work-around for its users.

So what should you do if you receive a suspicious-looking e-mail? First, don't respond to it! This may seem obvious, but the Washington Post reports that 5 percent of the people contacted in this way do respond. For an identity thief, that's a healthy response rate.

Second, report these e-mails to the companies being spoofed and to the FTC. Here are a few guidelines to follow when you do.

Include the header. Always forward the original e-mail with its original header information intact. The header information will indicate where the e-mail might have come from (although this too can be spoofed).

To send the header information along with the spoofed e-mail itself in MS Outlook, follow these steps. (If you use some other e-mail client, the header info may reside at the top of any message you receive or forward. If you're not sure, consult the documentation to find out how to view it.)

- * Double-click on the e-mail message in your inbox.
- * Select the View menu and then Options.
- * Copy the text in the Internet header field.
- * Go back to the message, hit the Forward button, and paste the header text near the top of the e-mail.
- * Address it to the appropriate recipient (see below) and hit Send.

Get the right address. You'd think that the companies victimized by these scams would be forthcoming about it. After all, their images are being sullied. But for the most part, they aren't. Some sites do make it easy to report scams that use their name, offering links from their home pages to e-mail addresses where you can forward the spoofed e-mail.

Other sites, however, are significantly less forthcoming--you may have to navigate through various "Contact Us" pages to get the info you need. For your reference, you can click on the links below to find out about reporting spoofed e-mails involving the following companies:

- * Amazon
- * BankOne
- * Citibank
- * EarthLink
- * eBay
- * PayPal

Contact the FTC. Be sure to send a copy of the e-mail (with the header) to the Federal Trade Commission. There's info on the FTC site about how to do so. It might not seem worth it, but the FTC does keep statistics about this sort of thing. The more prevalent they think it is, the more likely they'll be to do something to stop it.

You should not expect a reply from either the company being spoofed or the FTC. This isn't such a big deal, but I wish they'd at least send an auto-reply message so I know they got my submission.

Phishing scams aren't going to go away overnight. And, like it or not, it's up to us to stop them. Just as we've all learned by now not to open e-mail attachments from people we don't know (so as to prevent the spread of viruses), we also need to recognize attempts made by identity thieves to rip us off via e-mail and the Web. Scrutinize every message you get, and don't be quick to give out your personal information. Only when we stop falling for these scams will they finally go away.