

Identity Theft - Beware of Phishing Attacks!

Article by: Charles Essmeier

"Dear Bank of the West customer", the message begins. I've just received an e-mail message, purportedly from the security department at the Bank of the West. The message explains that certain features of my account have been suspended due to "suspicious activity" on my account. The message then provides a link that I can follow in order to fill out an online form confirming my identity. It's certainly nice that Bank of the West is worried about the status of my account. There's just one problem – I don't have an account at Bank of the West. In fact, I've never even heard of Bank of the West.

This message is an example of "phishing", a relatively new problem found on the Internet. Unscrupulous individuals are sending spam e-mail messages by the millions, purporting to be from credit card companies, PayPal, eBay, or banks. Each message warns the recipient of questionable activity on his or her account, as asks that the recipient click on a link to verify personal information. The requested information is usually a username or password. Sometimes it's a credit card number and expiration date. These messages are almost always fraudulent, and consumers are falling for them by the thousands. The messages certainly look legitimate, and often mimic the style of the legitimate company's messages exactly. How can you tell the difference between a real message from your bank and a fake one designed to steal your identity?

There are several tips to help identify phishing expeditions. The first is the greeting. "Dear valued customer" is an odd greeting from a company that has a database that contains your name, address, Social Security number and credit card. Any company with whom you do business that legitimately wants to contact you will probably do so by name. Look for misspelled words. Phishing expeditions often come from foreign senders who often mangle the English text of the message rather badly, combining both bad grammar and bad spelling. Check the links in the messages. The link may say www.eBay.com, but if you move your mouse over the link, you may see something like "http://200.118.105..." on the bottom line of your e-mail program, indicating that the link is a fake. Should you click on the link, you'll be taken to a page that looks just like the real Website, but why take the chance?

If you need to contact your bank, credit card company, or online auction house, either go to their Website directly or call them. Never click on a link in a message that threatens you with account suspension; if a company with whom you do business has issues with your account, they will probably contact you by phone or mail. These individuals who use these phishing tips are getting more clever all the time. It pays to be suspicious. If you aren't, you may end up a victim of identity theft.

©Copyright 2005 by Retro Marketing. Charles Essmeier is the owner of Retro Marketing, a firm devoted to informational Websites, including End-Your-Debt.com, a site devoted to debt consolidation and credit counseling, and HomeEquityHelp.com, a site devoted to information regarding home equity lending.