New Phishing Scams Will Get By Antivirus Software

February 8, 2012 - A lot of internet phishing scams are obvious. They include misspelled words, grammatical errors and promises of millions of dollars in payments in you will only agree to wire two or three thousand dollars to an account in Nigeria. Most of these scams are conducted by e-mail, and a lot of the email messages advertising them contain viruses and Trojan horses that are easily picked up by antivirus software. But there is a new breed of scam artists that are now operating and they are getting very sophisticated. In fact, they are so sophisticated that even the software you may use to protect yourself from scams like this can't protect you.

The new mantra among sophisticated phishing scam artists appears to be subtlety. Instead of sending out messages that have all of the problems mentioned above, they are now sending messages that have been proof read and which contain no viruses. These messages may appear to come from your bank or brokerage house. They may be sent from actual mail addresses used by your bank, and the links in them will take you to your bank's actual website.

Because of this, there is no reason for the person receiving the message that it is anything other than it appears to be.

These phishing messages will contain a "call to action" that is compelling to some people. That call to action may be something like a problem with your account. And they will contain an attachment, asking victims to fill out some information on their account. Once again, that attachment will look like it came from your bank and it won't contain any viruses either. Anyone who fills out the information request and returns it using the instructions in the attached file will eventually find their accounts drained or that their information has been used for identity theft.

Unlike many phishing scams which have traditionally been used to steal information on your computer and to use it immediately, the new breed of phishers are more patient. The name of the game for them is to gather information and use it at a later date. Depending upon the information requested, victims may not be victimized for weeks, or even months.

While computer users still need to make sure that they are using antivirus software, they also need to realize that they can no longer rely on that software to prevent all internet based scams. But one simple rule can keep you from becoming a victim.

If you receive a message from your bank, brokerage house or, for that matter, from any company that is requesting

personally identifiable information from you, pick up the phone and call the company making the request. A simple phone call, to a number that you have looked up yourself or have gotten from directory assistance, is probably the best protection available. Today, too many people rely on online communication for everything. By making a call instead, you should be able to find out relatively quickly if the email inquiry you received is legitimate.

And if you make the phone call, and you can't find anyone who knows about the message you received, then you should print off a copy of the message and take it with you to your bank or brokerage house the next time you visit them. Have someone in the bank take a close look at your account and then tell you if there are any problems with it. If not, you'll know that you have been targeted by scam artists.

As a rule of thumb, you should never give anyone personally identifiable information unless you are the person who initiated the conversation leading to that information exchange. Neither your bank nor the government is ever going to call you or send you an email message asking you for your Social Security Number. That's information that they already have.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS