

PHISHING

Two to three times per month, I receive an email that appears to be from PayPal or some U.S. bank, telling me that someone has tried to access my account, and would I please click on the link to confirm my account information for security purposes?

The answer, if you're not already sure, is NO! This email is part of a scam that is known as "phishing". If I were to click on the link, I would be taken to a web site that looks like it really is PayPal (or that U.S. bank) where I could fill out a bunch of information, including my credit card number (for verification purposes only, of course). The criminals that are really behind this operation could then use my information to steal my identity and rack up unbelievable credit card bills in my name. From a criminal standpoint, it is a low-risk, high yield activity, sort of like fishing, hence the name. Phishing makes so much money (because there are so many people that who willingly fill out such forms) that they are the number one scam on the net right now.

For those not in the know, PayPal is an online service (owned by Ebay) that facilitates money transfers across the net. As an example, I can use PayPal to pay an Ebay seller for a chess set. He gets paid directly without risk, and I get to pay without giving him my credit card number. Of course, PayPal has my credit card number, and I am trusting that they won't lose it, just like I trust Amazon and a host of other online retailers. Unfortunately, this trust allows the phishers to try and take advantage of my gullibility or lack of knowledge. Simply by being asked, many victims unwittingly hand over their personal information to a website, without even thinking about the risks involved.

Common phishing attempts will use banks, Ebay, Amazon, investment companies, PayPal, really anything that potentially uses a credit card. It is the apparent authenticity of the email that sucks people in. How can you spot a fraudulent email? First, the email will usually use a generic greeting, like "Dear PayPal member:" If it really were from PayPal, the email should include your name. Second, the email will have a false sense of urgency, something about how you have to update your info ASAP or you will lose your account. Finally, and probably the most important thing about the fraudulent email is that the links don't actually go to where they say they go. For example, when you hover your mouse over the www.paypal.com/account-login.asp link in your email, you will notice down in the status bar at the bottom left of the window that the real address might be secure.paypal2.org.biz/login.asp, a completely bogus address. If you do actually go to the phishing website, you will also notice that few of the links actually work because, after all, it is not really PayPal! It is there just to scam you out of your info.

If you have question or comments, I can always be reached via email sean@intrex.ca or join our forums at <http://intrex.ca> for more in-depth conversations.