Phishing â€“ It Isnâ€™t Just For Email Anymore

October 29, 2015 â€“ It has been a few years since the word â€œphishingâ€• entered the American lexicon. Dictionary.com defi
the word as, â€œto try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.â€• Anyone falling for a phishing email can find their computer infected with viruses and their identity in jeopardy of being stolen. The thieves behind phishing attacks have evolved and many of them are now using social media to carry out their activities; often with much better results than through email.

Weâ€™ve all seen phishing email messages. Some are quite clever; disguising themselves as coming from legitimate companies that we do business with on a daily basis. Others are quite primitive; grammatically incorrect and written in plain text. Regardless of their appearance the barrier to entry for those behind phishing email attacks is so small that even a very low response rate can pay big dividends to the people sending the message. The only things required are a computer, an email list and a mass mail program.

But the crooks are learning that using social media for phishing can result in a significantly larger returns than email.

Email phishing involves sending a potential victim and unsolicited email message. If that message makes it past junk email filters and other anti-SPAM technology, the person receiving the message has to be interested enough in the content to click on a link. Letâ€™s say you receive a message from a well-known bank saying your account has been breached. You may click on it if you actually have an account at that bank, but youâ€™ll likely just delete it if you donâ€™t. For this kind of attack to be profitable, the phisher will have to send out a lot of email messages.

Social media is much more targeted. Thatâ€™s because the phishers are actively looking for victims who have posted information about a company online; for instance, maybe your bank has charged your account for some fees that you think are unfair. As a result, you decide to go on Yelp and complain about the bank. Along comes a phisher who reads your message.

In this case, the phisher knows where you actually bank and may learn your real name. He goes off, creates a new social media account that includes your bankâ€™s name in the user ID, and then he responds to you. In the response, you are provided a link to click on so that you can provide more information about your complaint. Then you are told that the complaint will be resolved in the next few days.

The point here is that you have a completely different mindset on social media. Instead of an unsolicited email, youâ€™re receiving what appears to be a one-on-one response to a real issue. The chance that you click on the link provided is astronomically higher than with email.

Once you click on the link, there are a lot of bad things that can happen to you. Your computer can be infected with malware or a virus. And, youâ€™ll likely be asked to fill out a form. Since in this case, we used a bank as the company you were complaining about, the form will probably include your bankâ€™s logo and ask you to provide certain information. What account are you inquiring about? Please provide the account number. What is your home address? Whatâ€™s the best email address to reach you at? What is your phone number? If it is a credit card account, please provide your card security code to verify you are actually in posession of the card. You get the idea.

If you received an email message asking for this information, you wouldnâ€™t respond. But because you are actually in the process of trying to resolve a legitimate complaint about a specific issue, there is a very good chance that you will respond with all of the requested information. And in a few days, youâ€™ll find out that your credit card is maxed out and your identity is being sold online.

So, what do you do to protect yourself? Well, the first thing to do is take a close look at any provided links. Make sure that they actually take you to the website of the company you are trying to get in touch with rather than to another similarly spelled website.

Secondly, donâ€™t blindly provide account information just because someone is asking for it. If you wind up on a form asking for detailed information about you, stop. Google the phone number for the company you are trying to contact â€“ donâ€™t use any phone number that appear on the form you're filling out â€“ and call the company directly.

This move to social media for phishing is disturbing. There is a very real possibility that even the most vigilant consumes could be vulnerable to this type of attack.
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