How to Avoid Phishing E-mails

SecurIT360
The physics of securing IT

E-mail phishing is a form of cyber fraud. The e-mail sender tries to "lure" the receiver into taking an action which will

- Disclose valuable information such as user id's and passwords
- Steal your money (Complete a fraudulent financial transaction)
- Install a virus that will damage the operation of the user's computer
- Install malicious software that will give the sender access or control of the user's computer

Phishing e-mails may use many different forms, but they appear to come from a legitimate source for a legitimate reason. They try to convince the reader to take an action, which provides the opportunity for the cyber-criminal to take advantage.

Cyber-criminals are working hard every day to create legitimate looking fraud. In order to protect yourself, you must learn more about e-mail phishing fraud and form a "cyber-defense" mindset.

Slow Down!

Everyone is in a hurry. Often, we don't look carefully at our e-mails. That is one of the main things foster cyber-crime. Verify links and attachments before you click on them. We don't have time to stop and analyze every single e-mail, but we need to learn how to spot suspicious ones. Don't click so fast.

Beware of Poor Spelling and Grammar

Phishing e-mails are sent from all over the world. If you spot spelling and/or grammatical errors, there is a good chance it was sent by someone unfamiliar with the language. There is also a good chance it is fraudulent. Delete the e-mail.

Perform a "Mouse-Over" on Links

One common fraud technique is to give a hyperlink a legitimate looking label, while the actual link takes you to a fake website. For example, the hyperlink might say www.firstnationalbank.com, but the actual link may take you a fake site that looks like the bank website. In many cases, the site will look legitimate enough to convince you to enter your bank account id and password. And then they have it.

However, by positioning your mouse over the link, you will see a pop-up link which will show the true destination of the hyper-link. If the two don't match, do not click on the link, delete the e-mail.

Do not log directly into any of your accounts from an e-mail

Phishing e-mails may conveniently provide a link to login to one of your accounts. In some cases, it will encourage you to login due to fraud on your account. In reality, that link may function as the gateway to a malicious website. (see Mouse-Over above.)

If you think this may be a legitimate request, then open your browser and go to the known website address and login as you normally would. If the premise is legitimate, deal with it there. If not, you just avoided being "phished."

Verify the mailing address and company logos

Cyber criminals try to make their phishing e-mails look as real as possible. But in many cases, they make errors when trying to mimic company logos and other information. If a logo or address looks "a little off," that may be a good indication that it is fraudulent. Again, you can always go directly to the company website if you are suspicious of the information in the e-mail.

How to Avoid Phishing E-mails

Be Skeptical

As the old saying goes, “If it sounds too good to be true, it probably is.” If you receive an offer of any kind via e-mail with an unusually high or unreasonable benefit, you should be skeptical of it. Some examples –

- Popular products for ridiculously low prices (iPads, smartphones, TV’s, etc.)
- An offer to give you a large handling fee for assisting with a money transfer (especially international exchanges)

You also have to be very careful evaluating any request for donations. Online fund-raising has become a very popular and effective way to raise money and support people and causes. It is also a fertile ground for fraud. Do your homework before making an online donation.

Be careful when buying or selling anything through an online listing

Online listing services such as eBay are wildly popular. Local community sales groups are growing quickly as well. They also provide more opportunities for fraud. Most of the online auction services are pretty secure and reputable. However, if you receive an e-mail offering you a higher price than you are asking for an online listing, or has unusual payment terms, it may be an attempt to take advantage of you. Be very careful of local online listings which may connect you with people you don’t know. Consider good safety practices before you agree to meet someone you don’t know. Always meet in a populated area and don’t go alone.

Read security blogs and stay in the know

Just what you wanted to do with your spare time, huh? You really do need to keep up with what is going on terms of cyber-fraud, and it doesn’t have to be painful. Find a couple of sources that you like and follow them on Twitter or Flipboard. You can also set up RSA feeds for newsletters and other good resources.

If you receive a phishing e-mail that looks legitimate, contact the company

Obviously, you should delete any phishing e-mail that you receive. But it is also important to let a company know when fraud is being committed in their name. It is good to follow the Golden Rule here. Otherwise, you may be the one to be fooled the next time.

Phishing e-mails often come with malware attached

Again, be very careful of attachments in e-mails. Not only can they damage your computer and provide access to personal information, they can also contain Ransomware. Ransomware locks your computer and requires you to pay a fee, or “ransom” to the cyber criminals to unlock your computer. In some cases, they just take the payment and don’t do anything. If you are not sure about the attachment, do not open it!

Remember, cyber-criminals are always “phishing’ for your information. Develop a “cyber-defense” mindset and protect yourself!

If you would like to learn more about Cyber Security and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250