Ten Tips to Avoid a Phishing Attack

By Secure Banking Solutions

March 17, 2016

Follow these ten tips and look for the red flags to avoid falling victim to a phishing attack. A good rule to follow is “when in doubt, check it out.” Verify a suspicious email with the sender before clicking on any links or downloading an attachment.

Ten Tips to Avoid a Phishing Attack:

1. **To click or not to click?** Ensure you always think before you click on a link in an email, especially if it is coming from an unknown or non-common source. This is one of the best ways for a hacker to infiltrate a computer system; the link will normally take you to a phony or defunct page that is not real. From there a backdoor is opened into your system, due to malware downloaded, and the hacker gains access. A trick you can use is to hover your mouse over the link to find the exact website address the link is taking you to. When you hover your mouse over the link it will display the exact webpage address in the lower left hand corner of the screen.

2. **Check the sender.** Often times our jobs can be so busy, we open emails without even noticing who sent them. One of the first sure-fire ways to sniff out a phishing email is by looking at who sent it. If you’re unsure who the email came from or why it’s being sent to you, stop and ask yourself these questions: Is the email from someone you don’t normally communicate with? Does the email come from outside my organization or does it have to do with my job? Or does this email sound too good to be true? If you answered yes to any of these questions, chances are it’s a phishing email so delete it ASAP.

3. **Spelling Counts!** Is the email grammatically correct? Phishing emails often contain spelling errors, typos, and fragmented sentences. These kinds of errors can be blatantly obvious or may be difficult to identify. If you are having difficulty identifying grammatical errors, be sure to check the sender of the email (see above). If it is from an unknown and questionable email domain, it most likely is a phishing email.

4. **What does the email say?** If you are having a difficult time figuring out if the email is a scam or not, ask yourself, “what does the email contain?” What point is the sender trying to get across? If the email is asking for personal or sensitive information, then this should be the first red flag. Hackers will sometimes create a sense-of-urgency in a message asking you to open an attachment or click on a link to avoid something negative from happening or to gain something of value. Another trick you can use in situations like this is to check and see if the message content matches the subject line of the email. If it doesn’t, immediately delete the email and report what happened to your IT team.

5. **Look to see if the email is sent at weird business hours.** An easy and fast way to determine if an email is a phishing email is to look at the date and time it was sent. If the email is sent at add odd hours during the day, i.e. between 12pm – 4am, chances are it might be a phishing email. Again, quickly delete the email and report it to the IT team.

6. **Does the email have an attachment?** Attachments can be just as deceiving as links in an email, or worse. Often times there are security parameters set up on email servers that disallow emails with links, however, these controls may not always catch messages with attachments. Because of this known vulnerability, hackers are becoming sneakier and adding attachments loaded with viruses to emails. When opened, the attachment installs malware onto your computer, and the hacker can gain access to the network.

7. **Ask a professional.** It can be very difficult to identify phishing emails, especially if they are specifically targeting you. In times like this it is best to ask the IT or Security Analyst where you work if an email is safe or potentially dangerous. If a professional is unavailable, try contacting the person or organization that sent you the email. If you don't have contact information handy, a simple Internet search will give you results quickly.

8. **Were you CC'd on the email?** A great way to spot a phishing email is by looking at to whom the email was sent. If you were CC'd in the email but don't recognize the other contacts CC'd, and it is coming from an outside source, chances are it may be a phishing email. Another key thing to look for: is the email addressed to you specifically? If it is coming from a legitimate business, your name will more than likely be included. If not, stay on your guard because it could be a scam.

9. **Are you expecting the email?** If you get an unexpected email from a family member, coworker, or friend asking for assistance, i.e. by sending money, or you receive an email in general that you were not expecting, be on guard. If it is a case between yourself and a person you know, give them a call to see if they actually need help. If it is a business claiming you owe something or can gain financial reward by entering personal info, delete and report the email or try giving the business a call.

10. **Risk is just ONE click away.** When all else fails and you've gone through the other nine steps to try and determine if you being phished, and you're still not sure if the email is legitimate, rely on your own confidence. Every email you open has the potential to put the organization at risk. Think and re-think if clicking on that particular email is a good idea. If an email just seems "off" or "shady," get rid of it. Don't follow the links or open attachments that come with the email. Most importantly, report it to your IT team to help create awareness for the problem. In the end you have to ask yourself, "is clicking on this email worth putting my organization at risk?" If the answer is a potential "yes," then don't click that link or download that attachment!