RobbLAW

IT Security &
Compliance Consulting

Phishing Campaigns

How do you protect yourself from a phishing campaign?

By: Robert Adams, Esq.
Date: July 17, 2017

Have you ever received an email from a foreign government official who needs your help to get some money out of their country? All they need you to do is help cover some fees to make the transfer and in exchange for your time, money, and effort, you will be rewarded with a percentage of the money. It sounds like an easy and cheap way to make a lot of money, right?

Almost everyone with an email address has seen this email even if they have no idea what it is called. It is called a "phishing" (pronounced "fishing") email and they come in many forms. They are the number one way of infecting your computer with malware. Phishing emails can also be used to compromise your passwords by tricking you into providing the attackers with your sensitive username and password information. They use fear or get-rich-quick schemes with a rapidly approaching deadline to create a sense of urgency in the reader to take some action and it is that action that causes problems.

It is important to learn how to protect yourself from these dangerous emails. There are several things you can look at to help determine if an email is legitimate or not. Until you determine for yourself that the email is legitimate, do not click on any links or open any attachments in the email. Every email should be suspected of being malicious until proven innocent. If you cannot determine its legitimacy, the best thing to do is call the sender directly and confirm if it came from them. If that is not possible, delete the email.

Here are some steps to take when checking an email. The very first thing to look at is the sender's address. It may say it is from Bank of America, but when you look at the actual address, you see something like "Bank of America <bankofamerica@austinvan.co>." It is important to look at the full address. In this example, the email claims to be from Bank of America; however, the actual email address is contained within the < and > symbols so the actual sender's email address is bankofamerica@austinvan.co. Make sure to notice what follows the @. Here, the sender's domain is austinvan.co. The question you have to ask yourself is "Do you believe that

austinvan.co has any relationship with **Bank of America**?" If you cannot conclusively answer "YES" to that question, then you should be suspicious about the source of this email.

Call the sender, whether it is a company or an individual, If you are suspicious about the email.

Second, look at the content of the email. There are two things to look for within the email itself. First off, when you read the message, ask yourself "Does this message sound like a professional email?" Look for misspellings, poor grammar, or bad word or phrase choices. Listen to your gut when it tells you that something does not sound right and remember if it sounds too good to be true, then it probably is! Second, look at the point of the overall message and ask yourself "Is the message trying to use fear to motivate me to take some action?" For example, an email message that says you just purchased a new album from iTunes and you can "Click Here" if it was not an authorized purchase by you so you can cancel the transaction is a message that uses your internal fear about having your account compromised. The sender is trying to trick you into clicking on that link which, ironically, is what will compromise your account.

In another example, you may receive an email that says your inbox needs to be increased or extended and all you need to do is "Click Here." Once you click that link, you are directed to a webpage to type in your username and password to complete your request. If you do that, you just gave your username and password to the attacker. You need to immediately change your password on every site that uses that same password, and then read our article on password security.

If you suspect something may be wrong with one of your accounts, or if you are not sure, based on an email you received, you can always confirm it directly with the sender by calling them or visiting their website. DO NOT CLICK ON ANY LINKS UNTIL YOU CONFIRM THE EMAIL FIRST. To visit the sender's website, first close your email. Open a new internet browser window and type the name of the website you want to visit. For example, if you received an email claiming to be from Bank of America about a problem with your checking account, you would open a new browser window and type www.bankofamerica.com directly into the address field. This will take you to the real Bank of America website and not a fake site the attackers may have been luring you to. Once you are at the website, look for a green padlock that indicates the website is who they claim to be.

Using these steps along with good common sense will help keep all your personal information secure and private. Remember, if you run into trouble, Robb**LAW** is always here to help.