If You Use Social Media You Are a Target for Spear-Phishing

January 25, 2017 - Just about everyone knows what phishing is. And just about anyone with an email account has received at least a few phishing emails. But spear-phishing is a new form of the scam. Unlike traditional phishing email attacks which cast a wide net, spear-phishing is a very targeted attack focused on a specific person. And because the culprits behind these attacks use personal information obtained from the victim's social media accounts, there is a much higher probability that the attack will be successful. Here is what you need to know to protect yourself.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Traditional phishing attacks usually are usually sent in mass. For instance, you might receive an email from someone who claims to be in Nigeria who claims to need your help getting money out of the country. Often, these types of messages won't use you name in the salutation line. Instead, they will read "Dear sir" or skip the salutation line entirely. In other cases, your name may appear but that is the extent of the personalization.

On the other hand, spear-phishing emails are highly personalized. They may come from an email address that you are familiar withâ€¦ either from a company or an acquaintance. The message body will probably use your name, and it may very well contain information about your friends or family. For instance, let's say you went to a party at a friend's house last month and then posted some pictures and information on a social media account. Then let's a friend of yours named Alice responded to your posting. Let's also assume that someplace else on your social media profile, you mention what you do for a living. For our purposes, we'll say that you own your own computer repair business.

A spear-phishing attack may say something like, "I was talking to my friend Alice and she mentioned the party that she attended with you last month. She mentioned to me that you have a computer repair business. I sell computer parts and thought we might be able to do some business together. You can take a look at my website by clicking on the link below."

If you received such a message, how likely would you be to click on the link? After all, the person writing to you seems to know a lot about you. And you have a mutual friend.

If you fall for this, you could be in real trouble. Once you click on the link, your computer could become infected with a virus or held hostage by ransomware. Or you could strike up an online dialogue that eventually gets you to make a purchase for nonexistent computer parts. If that's the case, you'll probably have given the person behind the attack a credit card number and other personal details. By the time you find out that you've been scammed, it will be too late. You'll be a victim of fraud and potential identity theft.

But the attack may not come from an individual. It may come from a company that you trust and do business with. For instance, if you mention who your work for or where you bank in a social media posting, a spear-phishing attack might appear to come from one of these companies.

If you have an online presence, you are a potential victim of spear-phishing, but there are things you can do to help protect yourself. First, take a look at your social media profiles and postings. Does all of the information you post online really need to be out there for the world to see? If the answer is "no" then you should delete the items that are unnecessary.

You may also be able to set your social media profiles only to be viewed by your direct connections. Of course, if you are using social media for business purposes, that may not be possible.

Alternatively, you may determine that your only way to deal with spear-phishing is to be very careful. In the example above, a quick email or call to your friend Alice to confirm the legitimacy of the email might have been all that was required to avoid becoming a victim.

As always, making sure that your computer virus definitions are up to date will help to keep you safe too.
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