Spearphishing -- A Story Behind The Numbers

By Danny Pehar

It's hard to read about cybercrime without seeing the term "phishing." This is where a hacker sends you a seemingly legitimate link, from a seemingly legitimate source. The problem, of course, being that the link in question was created for the sole purpose of stealing your money or your data.

This type of crime has been around for over 20 years, and as dangerous as that is, what's even more dangerous is something called spear phishing. Spear phishing is essentially a targeted and well-researched phishing attack.

A Cautionary Tale

Let's say I am a cybercriminal and have a company in mind that I would like to go after. It could be that this organization has the right combination of being big enough to have something worth stealing but not so big that it's taking its cybersecurity seriously. With so much information about companies online, researching a target list like this is very easy. Once I've made my choice regarding a company, I move on to a job title.

I start to make a list of the types of positions within the company that may have access to the things I'm looking to steal. Once I have the titles in mind, I can either look up the titles on the company website, look them up on LinkedIn or even call the front desk and ask for the name of the VP of something important.

Once I have a list of names that I believe could be the pathway to something good, I start to research their names. A simple Google search on just about anyone's name can pull up a wealth of information. Let's say the name of my desired target is Bob Important and by Googling his name I find out he has a Facebook account. I click on his Facebook account, but Bob Important was smart enough to know to lock down the privacy of his account, so I can't see anything just yet. But even though he locked down the privacy of his account, he didn't separately click on the "Who can see your Friends list?" and mark that as "friends only" or "private." Although I can’t see Bob’s info just yet, I can see who his friends are.

I pick one of his friends at random, we’ll call them Sally Friend, and I click on her account. Her account is private as well, but that’s OK because I don’t need her account — I just need to save her picture. I can save it right from Facebook or go to Google images, search her name and from there I can download her picture.

At this point, I create another Facebook account and call myself Sally Friend and I use Sally’s actual picture as my profile picture. Keep in mind, I didn’t need to actually hack Sally, Bob or anyone at this point. I’m simply making use of the information available to the public.

Once I’ve created my fake Sally Friend Facebook account, I send a friend request to Bob Important. After he accepts the fake Sally’s friend request, he now has two Sallys on his Facebook friends list. One is the real Sally and one is the cybercriminal.

Now as the cybercriminal, I see everything that I need to know about Bob to construct an effective spearphishing attack. I know whether or not he is married, his birthday, his interests, the names of his family members and what he did on the weekend. I can use that knowledge to send him a very convincing message. Not only that, but it's going to be a message from a trusted source.

“Hey Bob, I know you are excited about the Avengers movie. Check out this amazing new trailer.” And just like that, I can convince him to click on a link I added to the message that's designed for the sole purpose of creating havoc.

What Companies Can Do To Prevent Spear-Fishing Attacks

This is just one example of a spearphishing attack. It’s important to go over stories like this with your team to explain to them that the stories behind the breach numbers in the news are in fact very real. Cybercriminals love it when we glaze over the facts, fall into our usual routines and keep clicking on anything that comes our way. The only way we are going to win the fight against cybercrime is by first understanding that we are actually in a fight, and the best way to do that is by sharing stories as to how these scenarios play out.

In addition to awareness through stories, organizations should conduct regular searches to detect fraudulent emails. These attacks are so personalized that employees may not even recognize one if it takes place. And whether you are looking to protect your organization or just your individual accounts, it’s always a good idea to take advantage of multi-factor authentication. There are many free versions of this that provide an excellent layer of added security over a simple username and password. An example of this is when your social media platform of choice asks you for your phone number. It can then text you to verify you are in fact who you say you are.

With all of that said, the absolute best way to avoid spearphishing is to never click directly on a link sent to you — even if it seems to be from a friend. Open up a separate search window and research the link first. Ask yourself, "Was I expecting this? Does any of this make any sense?" And if the person emailing you is asking for some sensitive data, consider calling the person you think sent you the email and confirming with them that they are in fact the ones requesting the information.

When it comes to spearphishing, a few minutes of caution can save you hours, days and possibly even years of trouble.