United States {CYBERSECURITY} Magazine
A MULTI PLATFORM PUBLISHING PORTAL

Understanding the Threat

Social Phishing: How Hackers Trick You With Basic Sales Techniques

Tricia A. Howard

You are probably thinking "why on earth is there ANOTHER article about social phishing? Have we not drained that pond by now?" This is a common line of thought, but unfortunately, phishing attacks (leading to credential theft) are still one of the main ways that hackers access your information. However, the true kicker is that social phishing is really easy to do, just by using basic sales techniques.

The Mindset of a Sales-Person

Starting in the sales industry, I was strictly business development. As you all know, you have to find ways to stand to the customers. This is double true when you are just 1 of 1000 entry-level sales reps who "just wants to pick your brain." Getting those 3 net-new meetings a week became more and more difficult as the threat landscape (and thus the industry) has grown, and it is only going to get worse.

The best way to get around it was going to social media. Find a couple of interesting things about a target, call into a couple of people and get an email address, utilize that info found previously to create rapport, get meeting. It does not always work, but it was definitely more successful than just leaving voicemails that were never returned.

What is known as good salesmanship actually is known by another name, and a not-so-nice one at that: **Social Engineering**. Social Engineering is often noted for being "innovative and creative." Eventually, I found myself doing company-wide webinars effectively helping teach how to (legally) cyber-stalk people.

"That is great, but why do I care about how salespeople are getting more and more annoying?"

Because this is how you lose privileged account credentials.

Privileged accounts are not just admin creds, there are several people within the enterprise who have advanced levels of access. For example, let us look at Stevie Salesguy.

Social Phishing – A Case Study

Stevie is the ideal example of social phishing. Steve is a Director of Sales who runs the East Coast. He manages around 25-30 reps and works round the clock to keep it going. Imagine he has an "interview" with someone who wants to join the team who is actually a threat actor. The threat actor sees that Steve loves to fish, so he brings it up on the call – what types of fishing he usually does, where he likes to go, etc. The actor finds out that Steve is a member of Bass Pro's membership program and even has a trip coming up.

They get off the call and Hugh Hacker has all the info he needs. Hugh builds a quick landing page to look like Bass Pro. Then he sends an email asking to sign in to verify trip details. Just like that, social phishing has occurred. To make matters worse, since Steve uses the same password for everything, Hugh starts jet-setting through his financial data.

What to do?

I'm not suggesting we stop posting on social media or stop being friendly on first phone calls. Most of the people you will meet have good intentions, or do not even think in this way. However, until we finally get rid of passwords in their entirety, there are a couple of easy ways to help remedy this ever-growing issue

- Train your employees on security awareness – including fake social phishing attempts. If they are going to be clicked on, hopefully it is you who is orchestrating the attempt. The more customized the better. There are agencies who will put this in your pen-testing plan.
- Look at Privileged Account Management solutions – Especially if you are an enterprise or have lots of varying account levels. Having a manager that looks at forensic data can help keep lock down on weirdness going on in an account-level basis.