The Next Evolution in Social Engineering:

Back to Basics

Phishing. Email spoofing. Bots. DDOS attacks.

Ten years ago these words were the argot of Coders, Hackers, and Network Security Specialists. Today we teach our middle-schoolers these words and their consequences in Internet Safety classes. Most companies include social engineering awareness in employee orientation and training. Still our spam folders overflow with proof that somewhere, there must still be someone naïve enough to take the bait and make fraud and malware profitable.

XO Communications employees aren't fooled by email from a spoofed address. We know our banks and credit card companies don't really send links and ask us to re-input all of our critical personal data. We no longer let people we don't know walk behind us into our building on the swipe of our magnetic security card. We know when we get impersonal emails from our friends insisting that we watch a cool or topical video there might be a malware installation triggered by clicking the hyperlink or pressing the play button on a video viewer.

Or do we?

Immediately following the death of Osama bin Laden, the FBI sent out communications warning that the media popularity of the topical event almost ensured that phishing, spoofing, and malware would piggyback on curiosity surrounding the military operation. Sure enough, a malware-laden video purporting to show the raid (originating from Brazil) vectored across Facebook and Twitter with the speed of a brushfire.

It was the right scam at the right moment of emotional vulnerability; The "oldest trick in the book" and it worked like a charm.

Recently RSA, one of the premier names in Network Security had their most sensitive security "seed file" algorithms stolen by hackers. Many companies and governments rely on RSA's authentication products for the security of their network components, XO included. Aside from public embarrassment and damage to their reputation, RSA had to incur a tremendous financial burden as they replaced millions of units of software and hardware.

One of the top players in Network Security took a devastating hit to their reputation and their bottom line. Hacked. And how? How did this security industry giant succumb to hackers? A spoofed email addressed from the RSA company titled "2011 Recruitment plan." RSA's spam filter recognized the spoof and sent the email into the employees' spam folders. A single employee was checking their spam folder, saw the spoofed email, and opened a spreadsheet attachment within.

A simple spoofed email. The employee who opened it had an acquaintance looking for a job. Hackers knew of a temporary exploit that follows the installation of a popular software package and, based on a few logical assumptions… Bingo. The hacker's social engineering led them to a well-meaning employee, which led them to a vulnerable piece of popular commercial software, which allowed them to get their first piece of malware inside the firewall of RSA.

It was the right scam at the right moment of emotional vulnerability; The "oldest trick in the book" and it worked like a charm.

In another classic scenario, the gateway past the company network security starts with a simple phone call to the front desk receptionist. The receptionist is merely trying to help someone she perceives to be a local contracting company rep get in touch with one of the temporary workers he just placed. The hacker/caller seems to stumble to remember the name of the new hire, and the receptionist offers up a name. Moments later that new employee gets a spoofed email with a trojan malware attachment. The employee is new. Their mailbox is almost empty. An action item pops up in front of them. "Open this." It is the right scam at the right moment of emotional vulnerability; The "oldest trick in the book" and it works like a charm.

Who hasn't received a misdirected call on their work phone? Who hasn't at some point tried to help an anonymous stranger get forwarded to the right XO employee or an XO associate who took over the job responsibility of a former XO employee? We want to provide exceptional service to our customers. We're trained to go the extra mile. It's this helpful undercurrent of "can do" in our company culture that also makes seasoned, cautious XO employees emotionally vulnerable to some of the oldest tricks in the book.

So, while we are all inured to constant reminders and cautions sent by XO IT, Human Resources, and Network Security warning us to be wary of the latest social engineering probes and scams, it's worth taking a moment to ask yourself some quick questions at moments when you are asked to perform some task by a potential stranger at a moment of emotional vulnerability.

- "I recognize the email address, but what is my certainty that I am communicating with whom I think I am communicating, and not a spoofed imposter?"
- "Is the email or posting or communication prompting me to perform an action or click a hyperlink that I otherwise might not be inclined to do?"
- "Is the email or communication associated with some trending topic that is probably not really work related?"
- "Is the email or posting or communication or phone call requesting sensitive information which the sender either already should have, or doesn't need to know?"
- "Am I helping a theoretical customer or vendor get an answer? Or am I providing them with information outside the scope of their stated needs? Does the customer need to know the first and last names or the status of our XO employees to resolve their issue? Why would our customer need to understand our hierarchy of management or the Org Chart in order to get an answer to their question?"

An awareness. A recommitment to basic principles of common sense. The appropriate balance of skepticism and helpfulness. As a growing communications carrier, XO becomes a bigger target for hackers, probers, and social engineers every day. We have a crack team of IT specialists and Network Security experts constantly working to harden all of our networks to outside attack. But while we keep abreast of the latest coding trends and software exploits, the most sophisticated Network Security in the industry becomes moot if a single XO employee falls for one of the oldest tricks in the book.

As hackers return to basics to hurt us, so should we return to basics of common sense and heightened awareness when dealing with vendors, unfamiliar customers, and outsiders.