ENJOY SAFER TECHNOLOGY®

SOCIAL ENGINEERING AND WHY IT HAPPENED TO YOU

Social engineering and why it happened to you

By Michael Aguilar, Technical Lead at ESET North America

In June 2015, nearly 22 million records of prospective and current federal employees were lost. These included items like fingerprints, personal information, even mental health records. The fallout is still being felt as people continue to receive letters from OPM (Office of Personnel Management) stating that their personal information has been lost. With this letter, you also win a free year of credit monitoring and access to a virtual browser. Yay. It makes you wonder how the attackers got access; perhaps with some new malware attack vector or undetected zero-day exploit kit used to bypass security. No, it was even more simple than that. The attackers most likely got access to networks via **social engineering**.

SE (social engineering), in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. Used for information gathering, fraud or system access, it differs from a traditional “con” in that it’s often one of many steps in a complex scheme.

SE is one of the oldest and most widely used attack vectors. You have something that an attacker wants, whether it be information, passwords, network topography or other data. Machines are cold, unforgiving and fairly difficult to break into. People, on the other hand, are malleable, trusting and always looking to help. You could not ask for a more plentiful attack vector. The two main types of attack are human-based social engineering and computer-based social engineering. Both involve the end user (human – most of the time), but the methods differ a bit.

Human-based social engineering is the perfection of persuasion, similar to Tom Sawyer convincing the neighborhood kids that whitewashing a fence is fun while he relaxes in the sun, eating an apple. There are many ways to get people to do what you want, and these six methods are used in this type of attack mechanism:

- **Reciprocation**—Isn’t it nice to give things! Give someone a keychain or some other item, hope to get a password or access in return! This is one of the easiest ways to make friends and have others feel obligated to complete some action for you.
- **Scarcity tactics**—Offering something that is difficult to obtain, like an unreleased movie, is another easy way to have a person want to help you in order to get this awesome offering!

- **Acting like an authority figure**—Do you ever say NO to your boss or your boss's boss?
- **Being likeable**—People always want to try to help others, which is what makes our species so great. This is also what makes us extremely gullible. Salespeople have said this for years: All it takes is a smile and a handshake! Studies also point out that people tend to do things for attractive people, so dress for success.
- **Going with the crowd**—People are like sheep and tend to move in flocks. Sheeple. If someone sees someone in the same role doing something, chances are, the behaviors are replicated.
- **Consistency**—People in the same roles tend to act the same. All of my tech friends, who are also nerds, love "Dr. Who," as I do. By acting similarly to other people in a scenario, it is easy to blend in.

Computer-based social engineering takes many forms, but I will focus on the most popular ones: **support scams**, **phishing** and **pop-ups**.

- **Support scams** are an older scam that's on the rise. They prey on users who simply answer the phone. Many times, I have talked to clients affected by these scams, where a phone call is received, a "technician" gets access to a system and then displays an event

viewer stating there is an infection. Once you agree you need assistance (which you don't), it will take "only" $400 to fix. That is really affordable considering there is absolutely nothing wrong with your computer.

- **Fake AV alerts/Pop-ups**—These are similar to the support scams, except software is developed to make you call them. This is accomplished through pop-ups or fake AV software that says your entire computer is infected. Once you call the fake software company or staff, again, for just the low price of up to $400, they can remove the fake alert. I have even had clients who declined the service only to have a BIOS password placed on the system to lock it up.
- **Phishing**—This technique utilizes email or other electronic methodology to exploit your machine and get info from you. Phishing examples include emails from your bank requesting you change a password; .zip archives that are actually infections leading to Cryptowall; or the famous but still functioning princely emails from foreign officials giving you a slice of their $3-billion-dollar empire in exchange for a routing number to your checking account.

Now for an example. Say I wanted to socially engineer a site. Your site. Your business. First, reconnaissance. Remember when you went on a hiring spree? Well, I used it to gather some insight into the technologies you use and the positions open, as well as staff emails and possibly a schema for the email addresses, just in case I wanted to sound official. Next, I may even apply for one of the jobs and come in for an interview, though I would use a pseudonym so no trail would lead directly to me.

Once on site, there are a few ways to progress. I could ask the receptionist, due to my running late, to print my resume. No one would know that my USB stick has an exploit to allow remote access. Sorry!

If the receptionist attack vector does not work, later (once I gauge the climate and routines of the staff) I could call back as an important user or new hire (remember the job I interviewed for) and ask to have a password reset. As shown in this example, three aspects of the business could have been used against itself. So how do you protect yourself?

Protection against these attacks is twofold, like the attack vectors themselves. To protect against human-based exploits:

- Having a good and effective security policy is key. By training your staff how to check visitors in, making sure they understand policy regarding appropriate computer usage, and enforcing badge check-in at doors, you will greatly reduce the potential threats that can be employed (pun intended).
    - —You should also have consequences for failure to adhere to these policies. It will train the employees to do the smart thing instead of being manipulated or allowing, say, an unauthorized user to access your workplace.
- One of the main things you can do to reduce the human threat is to foster an environment where people can feel free to escalate an issue or call someone if they are unsure of something. By having an open environment, users can ask questions instead of deciding what to do on their own.
- Have the service desk and possibly reception log all interactions, perhaps even including phone numbers, depending on the sensitivity of your work.

- Shred papers and burn them. Throwing them out and tossing water on them will not stop someone from gaining information by looking through the trash. You would be amazed the things people throw out!

To protect your digital assets:

- Employ antivirus software on your endpoints, and possibly encryption. The antivirus software will reduce fake antivirus alerts and possibly pop-ups while also removing malware that could cause a compromise. Encryption will keep data encoded and inaccessible to unauthorized users.
- Use antispam protection at the exchange level to remove and reduce the amount of spam emails that may allow a user to compromise your workplace.
- Use digital badging systems at various entry and exit points. It will allow you to track staff movement as well as reduce access to critical systems. You don’t still use a physical lock and key, do you?

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

*For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit **www.eset.com**.*

ENJOY SAFER TECHNOLOGY®