Social Engineering Remains a Top Cybersecurity Concern

Michael Buckbee

3 min read

Published January 21, 2016

Last updated October 14, 2022

In 2016, the top cyberthreat for IT pros, at least according to ISACA's Cybersecurity Snapshot, is social engineering. It has always been a classic exploit amongst the hackerati. But in recent years it has become a preferred entry technique.

Instead of breaking into a network, an attacker merely has to manipulate those who have access to the victim's data, even the victim to give away credentials – "Is your Requester Code 36472? No, it's 62883." This is technically a salami attack that works by fooling several people, so the attacker has enough slices of information to piece together the credentials needed to access the user's account.

In previous blog posts, we've covered a few ways to help guard against social engineering. But because social engineering can't be blocked by technology alone, humans remain the weakest link in this security problem.

"People inherently want to be helpful and therefore are easily duped," said Kevin Mitnick, who was once the country's most wanted computer criminal. "They assume a level of trust in order to avoid conflict."

As IT security groups allocate their resources to defend themselves against major security threats, they shouldn't forget to continuously educate end users on social engineering method so they don't become easy targets to exploit.

Let's review the most common forms of social engineering:

1. Phishing

One of the easiest ways to become infected with malware –Ransomware anyone? – is through phishing. With a phishing attack, the bait is an email containing personal information hackers have collected through prior reconnaissance. Crafted to look like an official communication from a legitimate source (Fedex, UPS), the phish mail is intended to catch the victims off guard, duping them to click on a link that takes them to a non-legitimate web site or opening a file attachment containing a malware payload.

Often the hackers will focus on high-value targets, bamboozling executives and other

C-levels. The goal in “whale phishing” is usually to extract IP or other very confidential and possibly embarrassing information.

Educate your staff! Don’t click on links or open attachments or emails from people you don’t know or companies you don’t do business with.

Related Phishing Blog Posts:

Phishing Attacks Classified: Big Phish vs. Little Phishes

2. Pretexting aka Impersonation

Pretexting is really a more direct instance of phishing that relies on old-fashioned person-to-person interactions. Typically, a phone call is involved. Fun fact: Hannibal Lecter knew how to pretext!

While Anthony Hopkins may have impersonated a temporary employee from his jail cell, real-life pretexters can impersonate a fellow employee, IT representative, or vendor. Their goal is to gather confidential or other sensitive information – SSN, bank account, mother’s maiden name, or the size of your savings and investment accounts. Today, attackers are also outsourcing the pretexting work to companies that will make the calls for them. Talk about progress!

Pretexting had become such a problem that in 1999 the Gramm-Leach-Bliley Act (GLBA), better known for improving financial data security, flat out made pretexting illegal.

The statute applies to all organizations that handle financial data, including banks, brokerages, credit unions, income tax preparers, debt collection agencies, real estate firms and credit reporting agencies. Take that Hannibal Lecter.

However, GLBA has not stopped a new generation of pretexters from selling the data they’ve collected to data brokers, who may then resell it to private investigators or even insurance companies.

3. Baiting

Baiting is like a phishing, but the attacker dangles and entices the victim with an exciting offer. It could be in the form of a free download – music, movie, book — or a USB flash drive with a logo labeled, “Confidential Company Roadmap”.

Once the victim’s curiosity or greed leads to a download or use of a device, the victim’s computer gets inflected with malware, enabling the attacker to infiltrate the network.

4. Quid Pro Quo (This for That)

Similar to baiting, a Quid Pro Quo also lures but with a practical benefit – usually a service – such as “Please help me with my computer!” Instead of fixing the problem, the attacker installs malware on the victim’s computer.

5. Piggybacking (or Tailgating)

Piggybacking happens in the non-virtual world, involving a person tagging along with a legitimate employee who is authorized to enter a restricted area.

Solution? Implement one of the most basic security tips: set your PC to lock after inactivity!

Want to guard against social engineering? Make sure least privilege is in its authorization processes.

Image source: ISAC’s January 2016 Cybersecurity Snapshot, Global Data

What you should do now

Below are three ways we can help you begin your journey to reducing data risk at your company:

1. **Schedule a demo session with us**, where we can show you around, answer your questions, and help you see if Varonis is right for you.
2. **Download our free report** and learn the risks associated with SaaS data exposure.
3. Share this blog post with someone you know who'd enjoy reading it. Share it with them via **email, LinkedIn, Reddit,** or **Facebook.**

Michael Buckbee

Michael has worked as a sysadmin and software developer for Silicon Valley startups, the US Navy, and everything in between.

Keep reading