800.956.6065
www.social-engineer.com

In the middle of the night, we called someone a half-a-world away. Our assignment was to obtain access to the client's network and use social engineering. This was one of Social-Engineer, LLC's services, a Security Assessment or Adversary Simulation.

In a Security Assessment or Adversary Simulation, first we perform the Open-Source Intelligence gathering, commonly referred to as OSINT. Then, we determine which people in the company might be most susceptible to a social engineering attack or vulnerable to influence techniques. Depending on what the client wants to be included or "in scope," we might send phishing emails or make some phishing phone calls, referred to as vishing, to obtain information. We might send text messages, utilizing the SMiShing attack vector, to a company-owned or managed phone. We might even show up at the company's door and find a way in.

The value of all of this effort appears in the final report and debrief. At the end of the engagement, we show all the information found, how it was used, what sensitive information or access was obtained, and then give recommendations on how to protect that information or prevent that access in the future.

To show how this is done, let's continue with the story.

OSINT and Phishing

Starting with OSINT, we learned from the company's Facebook page that the year before, a campaign asked employees to send in their "working from home" office photos (this was still before many companies returned to the office). We replicated that campaign and impersonated the employee who previously ran it. We sent an email to everyone in the company asking them for updated photos. The email instructed them to upload the photos to the company's internal portal site. This page was one that we created and hosted on our server. We made it look the same as an actual login page hosted by the client. Our portal was protected by what appeared to be the company's VPN login page. When people logged in to send their photos, they received an error message. Unknown to them, their submitted credentials were still safely captured.

At this point, we demonstrated a phishing risk to the company, evidenced by the captured credentials. We tested the credentials, and for one person, we were not able to log in. More on that in a minute.

Some people were so interested in the photo campaign that they replied to the phishing message (because they received an error message when they tried to log in) with their home office photos included. One of them was a high-value target in the company. Their photos gave additional insight and information useful for additional attacks.

Vishing Attacks

Working within scope, we could test whether users were vulnerable to vishing attacks (phone calls). With the phishing campaign building some degree of rapport and believability, one employee (we'll refer to this person as Bob) replied to our email saying they had a problem logging in to the site. Bob is also the person who submitted the credentials that didn't work for us.

For this attack, we used an IT-based pretext. We found the name of a person who worked on the company's help desk and then called Bob. On the call, we explained that the person running the photo campaign had forwarded their email about the login trouble, and we were calling to help.

Bob couldn't have been happier to receive our call. Calling as the ever-helpful help desk staffer, we suggested that Bob do a password update. In anticipation of this interaction, we created a password update page branded with the company logo. We read our domain to the employee, as the URL was just a hyphenated version of the company's domain. The target dutifully navigated to the site and entered their current and desired new passwords twice. On submission, Bob received a new error. Acting dumbfounded, we explained to Bob that we'd need to investigate and get back to them, but in the meantime, to keep using their old password, not the new one. We didn't want Bob to try using the new one and then call the IT department.
Armed with the submission from this attempted password change, we successfully logged in to our client's network, sent an email from the target's Outlook account, and read (and potentially sent) messages from their Teams account. This successful vishing attack showed a second vector of vulnerability to social engineering attacks.

Why Test?

We often hear the saying, "Defenders have to be right every time; attackers just have to be right once." This means that it only takes one vulnerability to get access. It only takes one employee to give their credentials. You might think, "Oh, no one would ever fall for that and give up their password!" But can you be sure without testing? Even if you believe that there is someone who might be vulnerable to social engineering attacks, do you know who?

Through Social-Engineer, LLC's Security Assessment, you can better understand who that is, which vectors they're vulnerable to, and even which influence techniques are most effective. Multiple employees shared their home office photos and network credentials in the engagement mentioned. This included the CEO, who emailed numerous detailed, high- resolution photos of their office. These photos included information that could be used in additional social engineering attacks.

Multiple studies have shown that 70-80% of business data breaches involve social engineering. Frequently, this attack stage is one of the first in the chain. Understanding and minimizing your risk at this stage can save time and money on investigations and mitigations.

Do you know your company's risk of social engineering attacks? A great way to find out is to have a Security Assessment performed on your company. We will work with you to identify the highest-risk targets and show how a malicious actor could target your company. In we also can evaluate your vulnerability to vishing, smishing, and unauthorized physical access. Contact Social-Engineer, LLC today to get started with a Social Engineering Risk Assessment or Adversary Simulation. Find those vulnerabilities at the head of the attack chain and stop them before data is breached.

1) https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

2) https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

TEST. EDUCATE. PROTECT.

For more information or a quote from Social-Engineer, visit our website at:

www.social-engineer.com