
Getty Images

SECURITY > THREAT MANAGEMENT

Protecting Your Company From Social Engineering Attacks

Prepare for inevitable social engineering attacks by taking a multipronged approach that includes bringing in an ethical hacker.

Karen D. Schwartz | Dec 05, 2019

When employees got the email from a local college student asking about an internship program, nobody thought much of it. After all, these kinds of emails come in once in a while. The company replied back indicating that there were no current internships. With that innocent reply, the company put itself at risk; it was

company was lucky, the "student" was in fact ethical hacker Stephanie Carruthers, who does this for a living as IBM's X-Force Red's chief people hacker.

What Carruthers accomplished with that email is becoming more common. It's just one example of how social engineering attacks—persuading someone to perform an action or provide information—have become the scourge of organizations everywhere. They are so prevalent that one recent report found that about one in three cyberattacks today involves some type of social engineering.

There are many types of social engineering attacks, but they can be boiled down to three basic types: phishing, vishing and physical. Phishing is typically done by sending unwitting participants emails with seemingly legitimate attachments that carry a malicious payload. These emails run the gamut, from asking for a favor to notifying people that they are due a refund to requesting users to change user IDs and passwords. The goal is getting that email signature, to be used later in a mass phishing campaign. According to a report from Proofpoint, 83% of information security professionals experienced phishing attacks in 2018, an increase of 76% over 2017.

Voice phishing, often called "vishing," is another growing area of concern. Typically, it involves scammers calling employees over the phone under the pretext that something bad has already occurred. They might, for example, ask an employee to provide information, such as a name or date of birth, to "help" fix the problem. According to recent research, about half of information security professionals have experienced vishing and/or smishing (SMS/text phishing) over the past year. And it's not just run-of-the-mill employees or businesses falling for vishing—it happens to professionals who should know better. David Howard, a Cincinnati, Ohio-based security specialist and certified ethical hacker with significant expertise in the healthcare sector, said it even happens at medical facilities, where Health Insurance Portability and Accountability Act (HIPAA) laws are stringent.

data and systems. They can take the persona of anyone from HVAC technicians to auditors. These scammers use every trick in the book, from badge cloning to steal badge credentials to freebie gifts with wireless receivers embedded, which can sniff a company's wireless traffic via Bluetooth.

So why are social engineering attacks increasing at such a fast pace? Because they pay off.

"Yes, social engineering is a lot of work, but these methods work very, very well," Carruthers said. "If they can get someone on the phone and gain their trust, the sky is the limit."

Another reason for the continued success of social engineering attacks is because of what organizations aren't doing—or aren't doing well enough. Simply put, employees often don't know how to spot suspicious emails, calls or people. A report from Positive Technologies found that 27% of employees click on phishing links, often failing to look at the website address for obvious signs of problems. That same report found that employees often open unknown files, click suspicious links and even correspond with attackers. Perhaps more shockingly, 35% of working adults in the United States still can't define phishing from a multiple choice list of possibilities, according to the Proofpoint report.

Sometimes, it's the companies' own processes and procedures that are setting them up to fail. Take the help desk, whose personnel are often measured on how fast they can resolve issues. Those goals may cause help desk personnel to respond to requests too quickly to consider whether they may be malicious.

The proliferation of social media is another problem area. In many cases, social media is a goldmine for hackers. Employees who don't know any better often post details on social media sites that might be better left unposted, Carruthers said. For example, an employee might post a photo with a hashtag like #CompanyName. If

Instagram that can be problems. Even sites like Glassdoor can be a problem, since they sometimes post fairly detailed information about companies.

Tackling the Social Engineering Problem Head-On

While social engineering attacks will never disappear, they can be greatly reduced by taking a multipronged approach.

The first step is assessing both the digital and physical environments to expose vulnerabilities. Both Carruthers and Howard recommend bringing in an external party to perform the assessment. These ethical hackers are tasked with doing whatever they can to compromise the employees, systems, applications and anything else considered sensitive by the organization. Using many of the same tactics and methodologies as hackers, these ethical hackers see how employees and internal incident response teams handle breaches. The result is an assessment the company can use to fix vulnerabilities before they are exploited.

To test phishing and vishing, experts will send out emails and make calls, attempting to get employees to click on links and provide information. Testing physical infrastructure takes a bit more creativity, but both Howard and Carruthers admit to looking forward to these tasks.

Carruthers recalled a client that had just opened up a headquarters in Europe and wanted to test its physical security. Typical measures weren't working because it was a new building, so there wasn't much information online. So she had to get creative.

"I went back to my hotel room and found some information online about their new investors, so I spoofed my phone number and called, pretending I was from the Americas location," she said. "I told them we were sending out an investor relations manager for a tour of the facility. When I showed up, they didn't ask any questions.

in as HVAC technicians, and they point us right to the HVAC closet," he said. "And typically, that particular closet will be in the same room or right next to the computer equipment. That gives us a way to place physical devices close enough to monitor their networks."

After the assessment is complete, it's easier to spot what needs fixing. That normally takes two forms: a tool upgrade and employee training. Assessments usually reveal the need to add or upgrade a variety of tools. Some of the most important center around monitoring and analytics, which are critical to tracking how files are downloaded or shared, along with user behaviors. If not already implemented, assessments also can uncover the need for multifactor authentication, spam firewalls and web filters, and secure web browser and mobile device management solutions.

Conducting comprehensive security awareness training on a regular basis is another critical step. Done correctly, it allows employees to more fully understand what attacks look like and how to report them.

The more granular you can get with training, the better, Howard said.

"It should get down to the level of how to read email addresses and URLs," he explained. "A lot of training will teach employees to look for common misspellings or bad grammar, but they are rarely taught how to actually read URLs or figure out where links are really going to take them," he explained. "If you incorporate that kind of training, you'll just about never get ransomware."

And it's not one and done. Assessments and training should be repeated regularly—not only because hackers continually come up with new methods, but because of staff turnover and complacency. When repeated often, Carruthers said she sees that employees are getting smarter and reporting more issues.

“When companies or employees themselves overshare, it can be a detriment. I'll see job postings on LinkedIn that give away different types of technology in use, or employees posting selfies with a picture of their employee badge,” Carruthers said. Hackers could easily use the image of that badge to create their own and infiltrate the company.

Finally, don’t overlook the obvious. One example is the fax—not used by all companies anymore but in wide enough use to be a problem. While most people don’t think of faxes as security risks, they are dead wrong, Howard said.

“I could call you, establish a rapport and ask you to fax me whatever information I’m asking for. But I’ll be giving you a standard Internet fax number that comes right to my Yahoo or Gmail account that I created 10 minutes ago, when you might think you’re sending it to a doctor’s office or law firm. It’s a very easy way to trick people into sending hard copies of information about their company.”

It's clear that social engineering attacks aren't going away anytime soon, because they are an effective entry point for data breaches. But it will change over time, Carruthers believes.

"I think we're going to see a lot less of the spray-and-pray campaigns like mass emails that are very generic, and more targeted campaigns. Attackers are going to be going out doing their homework, and things are going to be a lot more customized to their targets," she said.

Cloud Threat Report Shows Need for Consistent DevSecOps
FEB 14, 2020

5G Adoption Should Change How Organizations Approach Security
FEB 08, 2020