Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services, LLC

Business customer article

3 Common Social Engineering Techniques Your Business Needs to Know

Social engineering, in the context of information security, refers to manipulating people into performing actions or divulging confidential information. Criminals routinely rely on our customer-service centric mindset to exploit information right out from under us. That information is then used to commit all types of fraud, usually leaving the victimized business with substantial financial losses and a damaged reputation.

Businesses who understand the tactics criminals use can form appropriate security protocols to ensure you are not the next victim of a social engineering attack. To that end, I've compiled what I believe are the top 3 social engineering techniques affecting businesses today. Please note that there are many, many other versions out there in play, probably right now. This isn't an exhaustive list.

Tailgating

Unlike fun pre-game parties, this form of tailgating exposes your business to a host of problems, including physical stealing from your business or employees. Tailgating occurs when someone poses as someone they are not, like a delivery person or new employee, in an attempt to gain the trust of an actual employee. The actual employee then allows this unauthorized person to tailgate or "piggyback" past your security into secure areas.

A common rouse is someone claiming to be a delivery person or working for the business's outsourced IT company. In both scams, the individual will look the part (i.e. a delivery person uniform can be purchased from any uniform supply company; old law enforcement uniforms can be purchased from many online sites). This person will claim they need access to secured areas and they will possess some information or some official looking document, such as a supposed letter from your IT company or even have a package they say must be delivered to your server room. The ruses are too numerous to discuss here.

Security firms employed by a business to test security weaknesses often use this ruse to see how far an unauthorized person can get into a business and what they can access. I know an officer of one security firm who used this technique at the request of a large CPA firm; he was able to set up shop in the server room for several hours, unaccompanied, and not monitored. The unsuspecting employee not only bought his story, but also showed him to the server room, propped open the door and offered him coffee. While technically he was there with executive management's approval, the employee's at the firm's office didn't know this. He could have been anyone with full access to the firm's client data and all other records on that server.

Phishing

Phishing sure isn't what it used to be just 5 short years ago. Yes, there are still sometimes demands for information and a sense of urgency, but phishing scams have become so much more sophisticated; it's often difficult to detect the scam.

Phishing emails no longer rely on you providing information; these emails often include fictitious links or attachments that are loaded with malicious software so they can steal information from the user, compromise the computer, spread infections to servers, etc.

Two of the largest security firms in the world both suffered these types of attacks in recent years. In one case, the phishing email appeared to come from the corporate's own HR department with a teaser subject line about bonuses and pay raises. Once the attachment was opened, malicious software was unleashed not only on the computer, but spreading through the entire network which ultimately allowed criminals to access highly proprietary information that ultimately affected thousands of their customers. This one email cost the business in many ways and hit international news very quickly.

Bogus Caller

This one also takes many forms, but the would-be scammer using this technique actually calls the business with their claim, attempting to gain more information or access to your network. Two versions targeting businesses today:

- Someone calls claiming to be a consultant working for your IT Department or outsourced IT company. It's easy to know which claim to make before they call you. I can tell this about your company just by looking at your company directory or your company profile on LinkedIn to see how many IT/IS related positions you have. If you only have 1 position, I bet you outsource most of your functions. If you have a fully staffed department of 20 people, then you're probably mostly in-house. Then I'll find your senior IT person, call your staff, and claim your senior IT person told me to call. Confidence established with my name dropping and superior tone when I call.

  Generally the caller needs your log-in credentials, claiming they are doing updates or that a virus was detected on your computer. Sometimes they will even require you to allow them remote access.

- Someone calls claiming they are with your bank stating you had a security violation the last time you logged into online banking. They need to verify your identity before discussing the supposed issue, and to do so they need your password and the code currently showing on your token. Don’t do it!!! This will seriously never happen legitimately. If you ever get a call like this, take their name, what the matter is referencing, and say you’ll call back. Then call your account officer or other individual within the bank you normally do business with using the number you know, not the one provided. Always report these types of incidents to your bank.

In Conclusion

Social engineering isn’t always easy to detect, but it’s essential all employees are aware of the threats and balance customer service with security. Here are a few tips on how your employees can avoid becoming a victim of these social engineering schemes:

- **Trust, but verify.** Many security researchers say “don’t open emails from untrusted or unknown sources.” Good advice, but frankly very difficult to implement in business. What if that email, from an unknown person, really is the business opportunity of a lifetime? What if it’s a potential new supplier who could save your business thousands? I don’t know about you, but it’s really hard for me to delete an email just because I don’t know the sender.

  My advice instead, use common sense. Free offers, too good to be true, non-sense emails (I get these all the time), emails demanding personal or business information, etc. are probably all scams. Don’t just delete them though! Mark them spam so you’ll see less of this junk in the future. If in doubt, proceed cautiously. If the email claims to be from someone you do business with, or from an internal source like the CEO or HR, but seems strange, pick up the phone and make a call before clicking or opening anything. Also, have internal procedures for posting things like open positions, mass communications, etc. so employees don’t have to guess if something is legit.

- **Invest in sophisticated security suites.** No security solution can defend against every threat that seeks to jeopardize users’ information or your business, but they can help protect against a lot. Businesses need a strong security suite that scans all emails, including attachments, and prompts warnings if you are being redirected to an unsecure or untrusted website when you click a link.

  A simple anti-virus won’t cut it. There are too many threats out there that go way beyond a virus. Your suite should include, at a minimum, anti-virus, anti-malware, anti-spyware, anti-botnet, email scanning, document scanning, and website authentication services. The more protections you have built in, the stronger your protections are.

- **Be polite, but don’t offer the farm.** Have documented internal processes for deliveries, visitors, new employees, IT services, etc. and stand firm on those procedures. If someone comes in, even with some official looking document, trying to smooth talk their way into your server room, park them in the waiting area and make some calls. They can drink their coffee there while you confirm their need to access restricted areas. People there legitimately will understand; scammers will get impatient and start making demands.

- **Clean desk.** Lock your laptop whenever you are away from your workstation, don’t leave any sensitive information lying around (or lock your office door), never throw confidential information in the trash, and lock up personal valuables like cell phones and purses at all times.

- **Sign on the dotted line.** Develop a comprehensive security policy and procedures, provide education on them, and then have all employees sign that they’ve read and understand the company’s policy. Let’s face it, most people take things more seriously when their John Hancock is required.

About the Author

Rayleen is the CEO of RP Payments Risk Consulting Services, based in Orrick, MO. She travels the country presenting at fraud, payments and security conferences on topics ranging from Mobile, fraud, payments risk management, and information security. Previously she was the Director of Compliance and Fraud at a regional payments association for 8 years, and worked financial crimes investigations for a community bank for 7 years. Rayleen has been writing and presenting for over 10 years.