Social Engineer Yourself

Social engineering is still one of the most common security issues that can occur to individuals and businesses. The reason for that is because most social engineering focuses on psychology and the behaviors of people to influence them to take certain actions that benefit the scammer.

For your security awareness program social engineering yourself can be one of the most effective ways to educate employees on how to not fall victim to someone attempting to collect information from them. This idea guide and checklist will provide you with some ideas to implement into your awareness program that educates your employees on social engineering and how to stay safe online

Spot the phish

Send fictitious emails to employees and document employees that fall for them. You can provide immediate feedback and require additional awareness training on phishing to educate those who click suspicious links or enter credentials.

Social media intel challenge

Have your employees attempt to gather intel on a fake online persona using only publicly available social media information. They can report on the information they found as a demonstration on the risks of oversharing online.

Is this legit?

Create real-world scenarios and situations where an employee may need to verify something before proceeding in the event of a social engineering incident. You can do this by creating simulated fake websites for employees to show them fake websites via typosquatting issues. You can also have them review more sophisticated social engineering attacks that service from vendor or business email compromises by having them spot the legitimacy of the contact.

Guess the user

Put together a “guess who” style game that presents fake characters and employees are given specific information about them and they have to guess the user information. For example, you can have employees ask questions about the characters such as what is their occupation and do they have a pet? From the information given they have to attempt to guess user information about the character.

Deep Fake Detective

Educate and train employees on real and AI-generated videos of executives to practice identifying potential voice/video manipulation. As the advancement of AI has grown, so have the issues surrounding deep fakes in an effort to social engineer employees and gain access to sensitive company information.

Employee Checklist for Social Engineering

Social engineering can happen to anybody. Hackers are skilled at being able to trick people into taking quick actions on their communication to those they target. However, you can be the first line of defense to help prevent social engineering tactics by attackers from achieving success in their schemes. Here are some questions to ask yourself when you may believe you are being targeted via social engineering.

Does this request make sense?

If you receive a request for information via email or other form of communication, ask yourself "does this request make sense?" For instance, you receive an email at 4 PM on a Friday from someone that appears to be a leader in your organization making an uncommon request of you. The email body appears to be legitimate, but the information or action requested does not then you should question it. If it's a request for money, credential information, gift cards, or other for payment, it's likely a social engineering attempt. Verify with the party over the phone or within another communication channel before complying with their request.

Am I sharing too much information?

Social engineers are highly-skilled at picking up on small details and behaviors of their targets. It can be important for you to pay attention to communication that is asking for information beyond public knowledge. It can be all too easy to be in the midst of a conversation and realizing that you could be manipulated into sharing proprietary information about yourself, your role, and the company. It's key to remind ourselves that too much information sharing can still be used against us and companies.

Have I verified the sender?

Spam filters don't pick up every spam or scam email that may come in. Unfortunately social engineers are skilled at spoofing email addresses to appear legitimate. If it looks as if it's the first time this sender has contacted you and the request seems uncommon for the sender, it's crucial to verify in another manner if it's truly that sender. Once verified then you can proceed with the request.

Why is this time-sensitive?

Due dates and deadlines are necessary for all businesses. However, it's not regularly common for some requests to be so time-sensitive. For example, if an email invoice comes in from a vendor but the payment is being requested outside of the normal billing cycle, you may want to verify it directly with the vendor. Phishing attacks are most successful when the request is unexpectedly time-sensitive and requires action as soon as possible.

Is this a valid link?

Social engineering attacks through email, social media, texting, and more will often include embedded links requesting you to click them to take action. It's important that any links embedded in communication channels be hovered over or verified with a link verification tool to confirm it's not malicious. Malicious links are often embedded and disguised as valid when in fact they may be deploying malware or ransomware on the device or system in the background. When in doubt, don't click the link.