When You Just Aren't Yourself: Combating Social Engineering Attacks

We Value Your Security | VOL. 1 NO. 1

It is the end of a long day and you finally get around to checking the voicemail left by an unknown number that called earlier. A voice informs you that you owe back taxes to the IRS and there is a warrant out for your arrest, so please call back. Did you remember to mail your local taxes? Did your mortgage company make that payment? Maybe it is someone with the same name? It has to be a mistake, but you need to know for sure. Do you call the number?

What is Social Engineering?

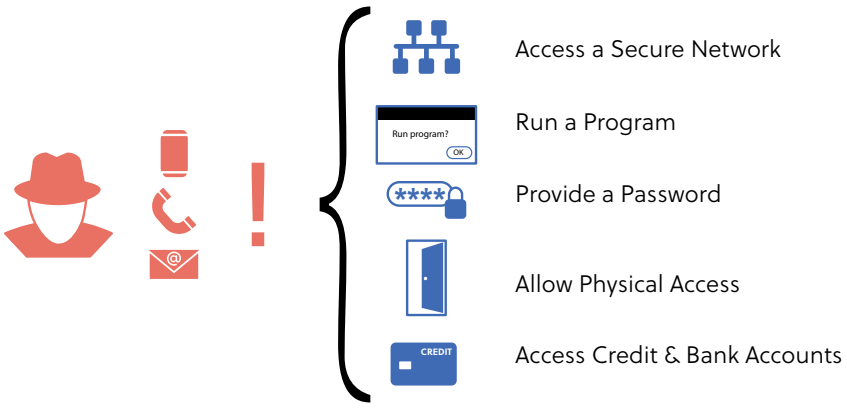
Social engineering is the art of capitalizing on relationships and social behavior to manipulate people into providing access, supplying information or performing an action. An attack can be as simple as an unsolicited email that appears to be from a friend pleading for help or as elaborate as a request from your supervisor directing you to perform an action immediately. In every case, people are the key to whether an attack succeeds or fails.

What Are Some Different Types Of Social Engineering?

Attacks are usually distinguished by the medium used or the type of pressure exerted on a victim. One of the most common examples are "phishing attacks." These emails look like legitimate requests and usually come with a degree of urgency to get a victim to act quickly. If a recipient accepts the email as legitimate, he or she may click on a link, provide confidential information, and continue about his or her business unaware that sensitive information is now in the hands of hackers. The access provided can allow hackers to lurk in a system, exploiting any information available to achieve their ultimate goal.

A simple phishing attack can be just the beginning. The more information hackers have about an individual or organization, the more they are able to make their attacks convincing, potentially leading to "spear phishing." Spear phishing is when hackers understand the relationships within an organization and send emails designed to mimic requests within the organization. Many people refuse to click on links in a strange email, but suppose it is an urgent request from supervisor? Many recipients are less likely to verify if the request is legitimate or an attack before reacting.

Social Engineering Attacks Exploit Any Type of Communication



Attacks are not limited to email communication or a specific tactic. Any mode of communication or predictable tendency can be exploited. Here is a list of some of the other common attacks:

- **"Vishing" (voice-phishing)** attacks are the same as both phishing and spear phishing attacks, but are done through telephone calls
- **"Smishing" (SMS-phishing)** attacks utilize text messages
- **"Pretexting"** presents victims with the false "pretext" of verifying their information
- **"Baiting"** offers victims a prize for information
- **"Tailgating"** takes advantage of holding a door open to compromise a secure location
- **"Quid Pro Quo"** attacks give victims a gift to make them feel obligated to respond

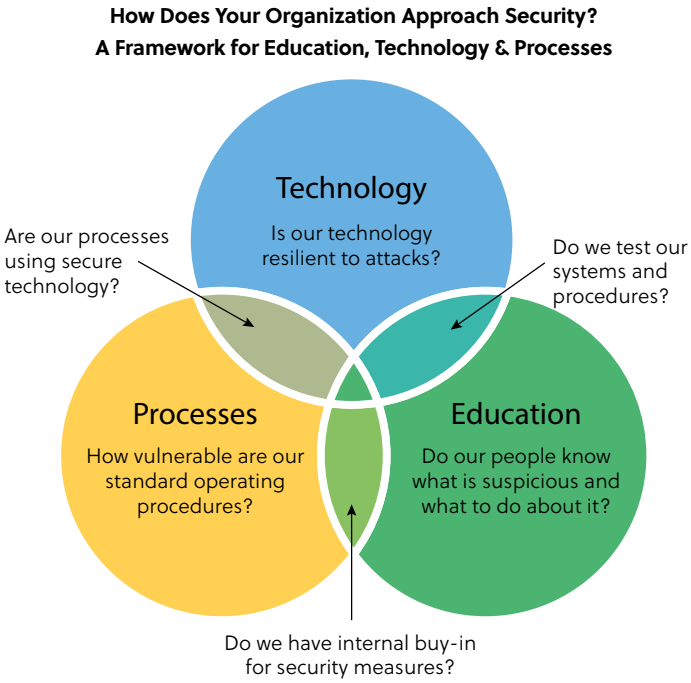
Ultimately, hackers employ these methods because they are much easier than trying to hack into software. Every software system is designed to be used by users, so the surest way to gain control is to manipulate the user.

How Can I Help Protect Against Social Engineering Attacks?

We encourage all of our clients to think about their readiness, specifically how your organization can prepare by deploying technology, processes and education designed to enhance security.

Attacks are a product of technology, but technology can also play a role in protection. For instance, spam filters are effective at stopping most phishing emails from reaching intended targets. Another tool is multi-factor authentication (MFA). MFA is a method of confirming a user's identity utilizing factors beyond the standard username and password. Sometimes simple procedures like regularly resetting passwords can limit damage or frustrate attacks.

Unfortunately, deploying more secure technology in an organization does not mean it gets used every time, a fact that highlights the importance of assessing organizational processes. Process assessment should extend to third-party service providers as well, and be understood by all parties, which leads to the final point.



Education should underpin any readiness effort. Any person with even low levels of access to data should have a basic knowledge of what attacks are possible through email, text or phone. Employees of public organizations face a unique challenge in that they are responsible for providing transparency but any information, such as organizational charts, contact information, and biographical information, could be used to hijack internal communications. Educational efforts should highlight what is possible and underscore the security reasons behind the processes and technology that employees execute or interact with on a daily basis.

How Does PFM Seek to Stop Social Engineering Attacks?

PFM has taken a proactive approach to addressing social engineering. That approach includes taking our own advice and mandating training for all PFM employees, regularly testing and assessing critical processes, and constantly seeking to maintain and enhance secure access to any client or employee data. PFM also offers

additional security tools like MFA for our client account portal, Easy Online Network (EON). We would be happy to guide you through the process and ensure it provides an added layer of protection against attacks. We take our role as an extension of your staff seriously by welcoming security-oriented conversations from formal due diligence checks to simply keeping us up-to-date on process or personnel changes. Understanding how your processes can dovetail with ours (and any other service providers) can help to keep communication secure and successfully flag suspicious requests. To us, looking out for our clients' best interest is not limited to the advice or services we offer, but extends to how we handle any sensitive client information.

If you would like to initiate a conversation about how we are working to protect you, please don't hesitate to contact your relationship manager.

In Conclusion, Do You Call Them Back?

We hope that after understanding the possibilities that technology has opened for both good and malicious purposes, you know that the best course is to delete the voicemail mentioned in this article's opening. If you wanted to go the extra step, you could contact the IRS directly, being careful not to use any contact information from the message. Although these attacks can be alarming, hackers using social engineering have no way to keep you from simply deleting an email or independently verifying any suspicious requests. PFM is always happy to discuss implementing education, processes or technology to help secure clients' interests against attacks.

"To us, looking out for our clients' best interest is not limited to the advice or services we offer, but extends to our handling of any sensitive client information."