Top Three Ways Cyber Attackers Target You

Overview

Social engineering attacks, in which adversaries trick people into doing something they shouldn't, are one of the most common methods that cyber attackers use to target people. The concept has been used by con artists and scammers for thousands of years. What is new is that the Internet makes it very easy for a cyber-criminal anywhere in the world to pretend to be anyone they want and target anyone they want. Below are the three most common types of social engineering methods that cyber attackers will use to try to engage and fool you.

Phishing

Phishing is the most traditional social engineering attack; it is when cyber attackers send you an email attempting to trick you into taking an action you shouldn't do. It was originally called phishing because it was like fishing in a lake: You threw out a line and hook but had no idea what you would catch. The strategy behind this tactic was that the more phishing emails cyber-criminals sent, the more people fell victim. The phishing attacks of today have become both far more sophisticated and targeted (sometimes called spear phishing), with cyber attackers often customizing their phishing emails before sending them.

Smishing

Smishing is essentially SMS-based phishing, in which a text message is sent instead of an email. Cyber attackers send text messages to your phone on apps such as iMessage, Google Messages or WhatsApp. There are several reasons why smishing has become popular. The first is that it's much harder to filter out messaging attacks than it is to filter out email attacks. Second, the messages that cyber attackers send are often very short, meaning there is very little context which makes it much harder to determine if the message is legitimate or not. Third, messaging is often more informal and action-based, so people are used to quickly responding to or acting on messages. Finally, people are getting better and better at spotting phishing email attacks, so cyber attackers are simply shifting to a new method, messaging.

Vishing

Vishing, or voice-based phishing, is a tactic that uses a phone call or voice message rather than email or text message. Vishing attacks take far more time for the attacker to execute, as they talk directly to and interact with the victim. However, these types of attacks are also far more effective, as it is much easier to create strong emotions over the phone, such as a sense of urgency. Once a cyber attacker gets you on the phone, they will not let you get off the phone until they get what they want.

Spotting and Stopping These Attacks

Fortunately, it does not matter which of the three methods cyber attackers use, there are common clues you can spot:

- **Urgency**: Any message that creates a tremendous sense of urgency in which attackers are trying to rush you into taking quick action and making a mistake. An example is a message claiming to be from the government, stating your taxes are overdue and if you don't pay right away you will end up in jail.
- **Pressure**: Any message that pressures an employee to ignore or bypass company security policies and procedures.
- **Curiosity**: Any message that generates a tremendous amount of curiosity or seems too good to be true, such as an undelivered UPS package or a notice that you are receiving an Amazon refund.
- **Tone**: Any message that appears to be coming from someone you know such as a coworker, but the wording does not sound like them, or the overall tone or signature is wrong.
- **Sensitive Information**: Any message requesting highly sensitive information, such as your password or credit card.
- **Generic**: A message coming from a trusted organization but uses a generic salutation such as "Dear Customer". If Amazon has a package for you or phone service has a billing issue, they know your name.
- **Personal Email Address**: Any email that appears to come from a legitimate organization, vendor, or co-worker, but is using a personal email address like @gmail.com or @hotmail.com.

By looking for these common clues you can go a long way toward protecting yourself.

Guest Editor

Mary Jane Suarez Partain is the Program Director for Women in CyberSecurity (WiCyS). The focus of her role is to provide resources, initiatives and programming designed to recruit, retain and advance women in the field of cybersecurity. She is passionate about creating an inclusive environment where all feel valued, welcome and seen.

Resources

Stop The Phone Call Scams: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
Phishing Attacks Are Getting Trickier: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier
Emotional Triggers – How Cyber Attackers Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
I'm Hacked, Now What: https://www.sans.org/newsletters/ouch/im-hacked-now-what/