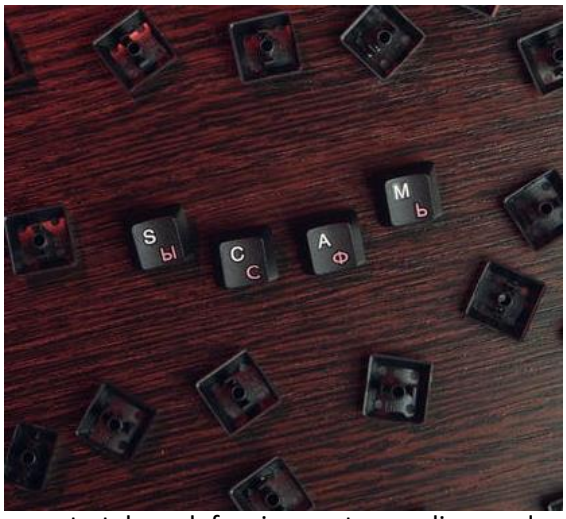
Here Phishy Phishy

Social Engineering and Cyber Attacks



Social engineering encompasses a broad range of malicious online activities that focus on exploiting human vulnerabilities by prompting users to make common mistakes and reveal sensitive data like passwords, personal information, or otherwise grant wider systems access permission.

In this fast-paced world of constant connection, much of our communication is done on the go and while multi-tasking. Cyber criminals can and do exploit users who are not giving cyber security their full attention. In most cases, this discussion reaches further than your IT or systems administration team, as cyber criminals could potentially target anyone with systems access to gain system entry. Therefore, it is wise to empower employees to take a defensive posture online, and train them to question anything that doesn't look right. Failure to implement technological defenses and employee training can greatly increase the risk of a data breach if your organization is attacked, leading to costly outcomes for Members.

Claim Arising from Social Engineering

A metro area district recently fell victim to a phishing incident. A sophisticated email request came to the district office, appearing to be from a construction company they had hired to complete a project. The email, complete with a forged signature, requested a change to routing information for payments. The email was a spoofed email. A spoofed email contains forged elements, such as a company standard heading or signature, to appear as if coming from a trusted source. The district, believing this request came from their construction company, processed the routing change and made three monthly payments to a fraudulent account. The district was scammed out of $850,000.

Types of Social Engineering

Cyber attackers constantly adapt their methods to keep ahead of cybersecurity advances. We have compiled a list of common social engineering schemes below. But remember, this is not an exhaustive list. Always be on alert when interacting with others online.

Phishing

The term "phishing" is a catch-all for any scam that uses email to trick a user into revealing personal or confidential information. These emails often create a sense of urgency, such as an account disabling or suspension, overdue account, pending legal action, or expiring offer. Other phishing "red flags" include unrecognized sender addresses, poor grammar and/or spelling, unusual wording, and inconsistent or missing contact information.

Here Phishy Phishy

Mass Marketing
The most common type of phishing, mass marketing phishing involves sending a malicious email to a wide audience. Mass marketing attacks are often non-specific, but attackers hope sheer numbers will go in their favor, and at least one recipient may click a malicious web link, download a file containing malware, or provide sensitive data.

Spear Phishing
Spear phishing is a targeted phishing approach where cyber attackers impersonate a specific trustworthy individual or organization to gain a target's full confidence quickly. Attackers sometimes pose as a vendor you often work with, an individual you contact regularly, or even someone within your organization. Because these emails appear to be from a trusted sender, recipients are often easily persuaded into clicking a nefarious link or providing ample information to carry out a breach. Spear phishing campaigns have been attributed to some widely publicized breaches involving Target, Home Depot, JP Morgan, and even the Pentagon.

Whaling
Whaling is even more specific. Technically a form of spear phishing, "whalers" hunt high value targets such as officers and executives who are likely to have lucrative information and systems access. Oftentimes these schemes are exceedingly difficult to detect, as attackers work to make links, signatures, and other email elements as accurate as possible to increase the chance that a high-value target will divulge useful information.

Vishing
Vishing or "voice phishing" avoids email entirely, instead using voicemail and robocalls to collect sensitive information. Oftentimes vishing calls attempt to provoke immediate action by claiming to be from a government agency or threaten the expiration of a target's cars warranty. Attackers even sometimes impersonate family members or friends requesting immediate assistance. Vishing attackers not only collect personal or financial information from these calls, but sometimes even record a target's voice for use in future scams.

Avoid "Taking the Bait"
Security software can help filter out social engineering attempts, but as attacks gain sophistication, the risk of security system evasion raises. User awareness and training is the best way to prevent social engineering cybercrimes. Always encourage staff to slow down and properly vet all email correspondence, no matter how urgent. The following checklist can help identify problematic communications:

- Be aware if a communication contains egregious grammatical or spelling errors.
- Unless certain of the sender's identity, don't rely solely on the name appearing in the email. To check the sender, you can compare the email address with previous legitimate communications or go to their site from a new web browser.
- Never click links or attachments within a suspicious communication. These can contain malware, which can track your activity and keystrokes.
- Pick up the phone and call the contact at a known number or one obtained from a legitimate company website.
- Never provide confidential information via email or forms embedded within an email.

303.722.2600
www.csdsip.org
: @CSDSIP

Here Phishy Phishy

- Never send financial information via email. It is impossible to verify the security practices of the recipient or if they can eventually be compromised.
- Never accept social media invites from unknown persons.
- Avoid entering personal information or clicking links in a pop-up screen.
- If you receive an unidentified call, proceed with extreme caution and ask to be placed on the national do not call registry list.
- Review account statements regularly to ensure information is correct.

Additional resources
https://www.ic3.gov/default.aspx
https://k12cybersecure.com/
www.FTC.gov/complaint
https://www.us-cert.gov/report-phishing

303.722.2600
www.csdsip.org
: @CSDSIP