RISK NOTE

Subject: **Social Engineering: Best Practices for Prevention**

Introduction

With the increasing severity of losses and claims experienced by the Healthcare Protection Program related to social engineering, this document serves to raise awareness to our clients of the associated risks. For example, a scammer posing as a vendor may urgently demand payment of a service to an accounts payable clerk to wire transfer hundreds of thousands of dollars to a new bank account. The accounts payable clerk, confronted with this urgent demand, may oblige this scammer without pausing and verifying that request. What could have prevented this? We outline a brief summary, preventative measures and best practices with the goal of mitigating negative impacts that arise from social engineering attacks.

Background

Social engineering can be defined as the psychological manipulation of people into performing actions or divulging confidential information.[1] Bad actors will exploit a victim's psychological vulnerabilities including:

Using emotional appeals; Victims may take irrational or risky actions when in a heightened emotional state. Bad actors may convince the victim using fear, excitement, curiosity, anger, guilt or sadness. For example, you receive the following SMS text:

> ATTENTION! YOU HAVE BEEN AUDITED BY CRA AND OWE $1,234.56 IN LATE FILING FEES. FAILURE TO REMIT WILL RESULT IN PERSECUTION. CLICK HERE TO MAKE A PAYMENT.

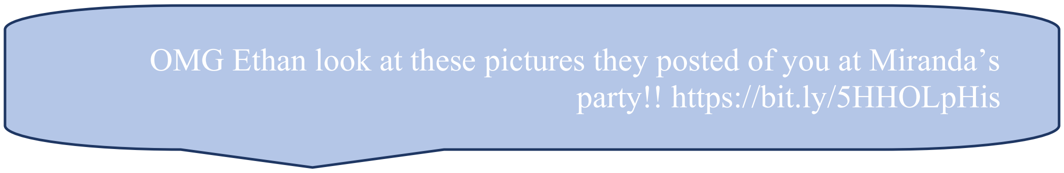
Urgency; Victims may be pressured to act and compromise themselves under the pretense of a serious problem that requires immediate action. Likewise, the victim may

[1] Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, page 17

be convinced of a prize or reward that may disappear if not acted on immediately. Both approaches attempt to override the victim's ability to think critically. For example you receive the following email in your inbox:

> **From:** "Lars, Harmann" Harmann.lars@2gov.bc.one
> **Sent:** Thursday, May 18, 2023 3:26pm
> **Subject: URGENT! IMMEDIATE ACTION REQUIRED**
>
> We will be Shutting Down your Account due to suspicious internet activity and login from different IP. Account will be suspended within 24 hours. To reinstate your account you will be required to CLICK THIS LINK now and submit login details. Your prompt attention is required.
>
> Regards
>
> System Administrator

Trust; Victims may not question or scrutinize a believable and confident social engineering attack. The bad actor may have done additional research on the victim to ensure a narrative that is unlikely to rouse suspicion. Here's an example you may receive on your instant messaging:



OMG Ethan look at these pictures they posted of you at Miranda's party!! https://bit.ly/5HHOLpHis

Types of Social Engineering Attacks

Bad actors may utilize the following social engineering scam tactics[2];

Email Phishing; Most common type of attack where the target receives spam email that spoofs, or impersonates a trusted company or organization. The email may contain a link to a phishing site designed to collect usernames and passwords.

Trojan Malware; A type of software that pretends to be something it is not. Trojan Malware is specifically designed to disrupt, damage or gain unauthorized access to a computer system by hiding in attachments. They may be hidden in email attachments that appear to originate from a trusted sender such as a co-worker, friend, family or company the target does business with.

Spear phishing; A type of phishing attack that targets one person or small group of people. Spear phishing requires some research and due diligence on the part of the bad actor. Bad actors may research the target's social media accounts and use information gleaned from photos, relationship statuses, birthdates, places lived, job history and any other public information they can use to give credence to their scam.

[2] "Social Engineering," Malwarebyes, 2023, https://www.malwarebytes.com/social-engineering, accessed February 16, 2023

Smishing (SMS Text phishing); A type of phishing attack that occurs outside of emails, such as your tablet, smartphone or smartwatch. Victims typically receive a text message from an unknown sender informing some special offer or contest they've won. Likewise, it may be a text message threatening legal action unless a penalty fee is paid. The text includes a link to a spoofed site designed to harvest login credentials.

Vishing (Voice phishing); Also known as robocalls or scam calls, the bad actor may use a computerized telephone dialing system that either connects to a live scammer or plays a pre-recorded message when the call is answered. The interaction involves some ploy to steal the victim's money, user credentials, or identity.

Tech support scams; Malicious websites that are run by bad actors. These websites lure victims to click on them only to be locked out of their browser, preventing the victim from closing out or navigating to another site. This is followed up by malicious advertising, or "malvertising," which is designed to fool the victim into thinking that their computer is infected with malware. The bad actor then attempts to extort money from the victim, offering them a way to "fix" the fake malware.

Prevention and Best Practices

Social Engineer bad actors manipulate human feelings to carry out their scam and draw victims into their scams. Whether its phone, text, email or websites[3];

Be wary of emotional appeals to act.

Pause and take the time to consider highly urgent requests from unknown sources.

Verify the story being told before acting.

Here are some additional preventative and best practices to consider[4];

Don't click on the unknown; Do not click on links sent by unknown people. Hover over the link and examine the url address to verify that it is a trusted site.

Avoid unknown senders; Avoid opening attachments within emails from senders you do not recognize.

Be wary of giving information; Be wary of texts, emails or phone calls requesting account information or account verification.

Verify requests; Always independently verify any information request from a legitimate source.

Verify web addresses; Check legitimate websites and manually type them into your browser.

[3] "What is Social Engineering?", Kasperksy Lab, 2023, https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering, accessed February 16, 2023

[4] "What is Social Engineering? Attacks and Prevention," Crowdstrike, 2023, https://www.crowdstrike.com/cybersecurity-101/social-engineering-attacks, accessed February 17, 2023

Check for spelling; misspellings, poor grammar or improper domains within a link may be a sign of a bad actor.

Verify calls; Don't transfer money or information until verified by another source such a by voice or video call.

Be alert to counterfeit items; Question ads and people that sell products such as sanitizing products and personal protective equipment that claim to prevent, treat, diagnose or cure COVID-19.

Conclusion

In an increasingly technological landscape of how we work, securing our information against social engineering fraudsters is crucial. Our behavior plays a large impact on defending against social engineering attacks. Do not be flustered by emotional or urgent requests and verify them accordingly. Ultimately, being aware of human elements, and attempts to undermine them, will secure and protect both personal and your organization's information.

Additional Resources

For more information visit the Government of British Columbia's website on Information Security and Cyber Threats at:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/cyber-threats

Published by the Health Care Protection Program

This document and the information contained within is not legal advice and is provided for guidance from a risk management perspective only. It is not intended as a comprehensive or exhaustive review of the law and readers are advised to seek independent legal advice where appropriate. If you have any questions about the content of this Risk Note please contact your organization's risk manager or chief risk officer to discuss.