WHAT IS SOCIAL ENGINEERING?

Social engineering is commonly defined as using social and behavioral observations to trick an individual into doing something they should not, such as performing a transaction or divulging sensitive information. Social engineering can take place using social media, telephone, text, email, and even in person. Fraudsters may target random individuals, but frequently conduct extensive research on individuals or corporations to tailor their approach to match the target.

HOW TO AVOID SOCIAL ENGINEERING

DOES THE EMAIL OR TEXT SEEM SUSPICIOUS?

A phishing email or smishing text message often impersonates a company and may appear to be legitimate; however, they are fraudulent and are after your credentials or other personal information. Sometimes emails are constructed from captured original emails, so if it looks odd, be suspicious. Email addresses or mobile numbers also may be spoofed, appearing to be legitimate, but in reality originate from another address or number.

IS THE GREETING GENERIC OR DOES IT ASK FOR INFORMATION?

If an email or text doesn't have specific information, it could be phishing or smishing. Companies should never ask you to provide personal information via text, so it's prudent to not respond to those asking for information. Always be aware of the information you provide and to whom you provide it.

DOES THE EMAIL OR TEXT CONTAIN A HYPERLINK OR ATTACHMENTS?

Many legitimate emails or texts contain hyperlinks. Know that the displayed text in a hyperlink does not have to match the actual hyperlink location. Attackers will use current events or entertaining topics to convince individuals to click. Hovering over the hyperlink will sometimes display the actual URL in the bottom of your screen. Attachments are not as common in legitimate emails or texts. Never open a link or attachment when you do not know the sender or are suspicious of the sender, as both are common ways to spread malware.

IS IT A PROFESSIONAL MESSAGE?

Look for signs of hastily constructed email or text messages, such as formatting errors, misspelled words, grammatical errors, and distorted corporate logos and images. If a government official, executive of a bank or other individual suddenly contacts you referencing an unknown inheritance or sudden, favorable award, be suspicious.

DOES THE MESSAGE REQUIRE AN IMMEDIATE RESPONSE?

Fraudsters use time pressures to force individuals to respond without thinking it through.

DO YOU KNOW TO WHOM YOU ARE TALKING?

Fraudulent phone calls, or vishing, are another form of social engineering. If you receive a call from an individual claiming to represent PNC, call the number (800-685-4039) on the back of your credit/debit card and speak to a representative about the previous call. Never provide information to anyone over the phone unless you have confirmed the caller.

DO YOU KNOW THE PERSON YOU ARE "FRIENDING"?

Don't accept friend requests or follow invitations from individuals you do not know, even if you see that you and the individual have some mutual friends. The requester may not be honest about their true identity and lead you to unknowingly divulge personal information. Simple small talk about family pets or where you grew up are potential answers to security questions. Users should likewise be cautious of sharing personal information when responding to online surveys or quizzes appearing in their social media feeds.

DOES THE OFFER SEEM TOO GOOD TO BE TRUE?

Social media is an ideal place for sharing current events, videos, and must-read articles, but be cautious of where you click. Links on social media can lead to malware or credential-stealing websites. If you see the offer of a lifetime asking you to use your email to sign up, decline it.

HOW CAN YOU PROTECT YOURSELF AT WORK AND AT HOME?

Be sure your home computer's malware and firewall protection is up to date. Remember to never use your PNC or other financial institution passwords for any non-PNC or financial institution accounts, especially social media.

Never let anyone remote into your computer unless you have contacted the source directly to fix an issue. Do not click on links in emails or texts even if they seem appealing. Find the site by navigating to the legitimate company page or contacting customer service.

If you receive any suspicious emails or texts claiming to be from PNC, forward the email and/or text and a description of the information exposed to PNC Cyber Defense at abuse@pnc.com.

CON PDF 0319-0172

PNC BANK