



DIOCESE OF SACRAMENTO

Information Technology - Bits and Bytes

2110 Broadway • Sacramento, CA 95818-2541 • (916) 733-0299

To: **PASTORS and DIOCESAN STAFF**
From: Philip DeLeon: IT Help Desk
Re: Social Engineering Attacks, Text and Email Scams
Date: **Monday, November 30, 2020**

The Christmas season is upon us and email scams, text scams and phishing attacks are on the rise. These social engineered attacks are also leveraging the COVID-19 pandemic as a means of attracting victims to respond.

Fraudsters have been using tactics of social engineering to collect personal and/or corporate info by sending emails to unsuspecting victims that contain web links to nefarious websites or have attachments (such as PDF documents) with malware. The documents or links may also ask for your email or network credentials to authenticate your account. **DON'T BE TRICKED INTO DIVULGING YOUR PASSWORD, ACCOUNT INFO, or PERSONAL INFORMATION.**

Victims report receiving emails from scammers who impersonate an individual or a corporate identity with whom you are familiar. The scam uses a sense of urgency to lure a victim to immediately respond to a text or email. In some cases, the scammer is simply attempting to scam the victim out of money (like a gift card) or covertly collect personal and/or financial information for use at a later date. The scammer uses a familiar looking name with a phony email address and might even include a photograph.

The Diocese has received reports that texts and emails have been received from a scammer impersonating Bishop Soto and pastors of the Diocese. The scammer has most likely been cleverly collecting email addresses and mobile phone numbers from such things as parish bulletins and related websites. **PLEASE CAREFULLY SCRUITIZE THE ADDRESSES AND PHONE NUMBERS YOU RECEIVE VIA EMAIL AND TEXT.** If you are not absolutely certain the email or text request is authentic, try to respond to the sender in person or call the sender using a phone number you know is correct.

It can be difficult to readily identify fraudulent vs legitimate email. However, email recipients should exercise caution when responding (or clicking on web links) to emails in the days ahead.

To understand more about social engineered attacks, please see the attached SANS OUCH! November 2020 newsletter.

If you think you have been scammed or compromised via the internet, you should file an online complaint with the FBI's Internet Crime Complaint Center at <https://bec.ic3.gov>.

If you have any questions, don't hesitate to contact the Diocese by sending an email to the Chief Information Officer, Philip DeLeon, at pdeleon@scd.org or calling (916) 733-0299.

OUCH!

The Monthly Security Awareness Newsletter for You

Social Engineering Attacks

Overview

A common misconception about cyber attackers is that they use only highly advanced tools and techniques to hack into peoples' computers or accounts. Cyber attackers have learned that the easiest ways to steal your information, hack your accounts, or infect your systems is by simply tricking you into doing it for them using a technique called social engineering. Let's learn how these attacks work and what you can do to protect yourself.

What is Social Engineering

Social engineering is a psychological attack where an attacker tricks you into doing something you should not do through various manipulation techniques. Think of scammers or con artists; it is the same idea. However, today's technology makes it much easier for any attacker from anywhere in the world, to pretend to be anything or anyone they want, and target anyone around the world, including you. Let's take a look at two real-world examples:

You receive a phone call from someone claiming to be from the government informing you that your taxes are overdue and that if you do not pay them right away you will be fined or arrested. They then pressure you to pay over the phone with a credit card, gift card, or wire transfer warning you that if you don't pay you could go to jail. The caller is not really from the government, but an attacker attempting to trick you into giving them money.

Another example is an email attack called phishing. This is when attackers create an email that attempts to trick you into taking an action, such as opening an infected email attachment, clicking on a malicious link, or giving up sensitive information. Sometimes phishing emails are generic and easy to spot, such as pretending to come from a bank. Other times phishing emails can be highly customized and targeted as attackers research their targets first, such as a phishing email pretending to come from your boss or colleague.

Keep in mind, social engineering attacks like these are not limited to phone calls or email; they can happen in any form including text message, over social media, or even in person. The key is to know what clues to look out for.

Common Clues of a Social Engineering Attack

Fortunately, common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common clues include:

- A tremendous sense of urgency or crisis. The attackers are attempting to rush you into making a mistake. The greater the sense of urgency, the more likely it is an attack.
- Pressure to bypass or ignore security policies or procedures you are expected to follow at work.
- Requests for sensitive information they should not have access to or should already know, such as your account numbers.
- An email or message from a friend or coworker that you know, but the message does not sound like them - perhaps the wording is odd or the signature is not right.
- An email that appears to be from a coworker or legitimate company, but the email is sent using a personal email address such as @gmail.com.
- Playing on your curiosity or something too good to be true. For example, you are notified your package was delayed, even though you never ordered a package or that you've won a prize in a contest that you never entered.

If you suspect someone is trying to trick or fool you, do not communicate with the person anymore. Remember, common sense is your best defense.

Guest Editor

Christian Nicholson (@GuardianCosmos) is a SANS instructor for SANS SEC560 and SANS SEC504, as well as Partner/Cyber Lead at Indelible (<https://indelible.global>). Christian specializes in Application Security, Purple Teaming, and Automation for secure integration, programming and engineering.



Resources

Phone Call Attacks: <https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams>

Stop That Phish: <https://www.sans.org/security-awareness-training/resources/stop-phish>

CEO Fraud / BEC: <https://www.sans.org/security-awareness-training/resources/ceo-fraudbec>

Personalized Scams: <https://www.sans.org/security-awareness-training/resources/personalized-scams>

OUCH! Is published by SANS Security Awareness and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley