DIOCESE OF SACRAMENTO

2110 Broadway • Sacramento, California 95818 • 916/733-0200 • Fax 916/733-0215

OFFICE OF THE BISHOP

Memo

To: Pastor, Parochial Administrators, Parish Secretaries and Staff

From: Lois Locey, DMin, Chancellor

Date: November 2, 2018

Re: Recent email scam hitting Catholic parishes and entities

We received reports this past week of emails sent from a spammer impersonating a Gmail account of several pastors within our diocese. The subject of the email was typically GOD BLESS YOU and they requested a reply (often times, it was a request of a gift card, such as iTunes). A careful inspection of the return email address, in some of the cases, revealed an incorrect spelling of pastor's name. The emails seem to be sent to those who have an email listed on the respective parish's or Catholic entity's website (such as the staff directory or ministry leader directory). If you, any of your staff or parishioners receive this email, please do not respond. This is an example of the tactics used by spammers to receive money or personal information from you.

This particular spoofing email scam seems to be targeting Catholic parishes and dioceses throughout the United States for the past several months. Other dioceses have reported that the emails are sent repeatedly every few weeks or months. I have asked Philip DeLeon, Chief Information Officer of the Diocese of Sacrament's Office of Information Technology Services to provide some guidance on how to protect our parishes and Catholic entities from phishing and spoofed email. Attached is his guidance.

DIOCESE OF SACRAMENTO
Office of Information Technology Services
2110 Broadway • Sacramento, CA 95818-2541 • (916) 733-0299 • pdeleon@scd.org

Memo

To: Pastors and Parish Staff

From: Philip DeLeon, Chief Information Officer

Date: November 2, 2018

Re: Phishing and Spoofed Email

The Pastoral Center frequently receives notification from parish staff members that parishioners are receiving email from someone who is attempting to impersonate the pastor or another member of the clergy. It's usually in the form of a casual email where the sender sends a casual and brief note like, "Good morning John, I want to send some electronic gift cards to some needy members of the community." "Can you help?" The signature line uses a familiar name of the pastor, like "Fr Joe."

Unbeknownst to the email recipient, he or she then replies to an email address that is not the pastor's, but an imposter. This type of social engineered email occurs frequently and is commonly known as a *phishing email* or a *CEO Fraud* (the latter because the imposter usually uses the name of the CEO of an organization).

What is Phishing?
Phishing is an email or text message that will attempt to trick the recipient into responding by sending money, sharing a password, PIN, or something of value (could even be parish checking account, credit card account or the parish email and network account). Close examination of the sender's email address will reveal that the address is a phony. But, it could be easily overlooked because the imposter will take a legitimate email address (like FrJoe@gmail.com and use FrJoe@msn.com (email address looks very similar … yet, different).

The holidays are quickly approaching and we will start to see more of these phishing emails to try and trick the recipient into sending currency or something of value. We ask that parish staff members and parishioners be extremely cautious when responding to these types of emails. When responding to emails that request for money or something of a confidential matter, consider responding to the email request in person or by telephone to confirm the email is legitimate. Texting and email should only be used as a secondary method of validation.

Finally, we can all educate ourselves on Internet Security Awareness by going to the SANS website and looking at the OUCH! Monthly Newsletters. You may even subscribe to them. Ouch! is a monthly publication and each one is brief and interesting. Here is the website: https://www.sans.org/security-awareness-training/ouch-newsletter

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for Everyone

Stop That Phish

Overview

Email and messaging services (such as Skype, Twitter, or Snapchat) are one of the primary ways we communicate. We not only use these technologies every day for work, but also to stay in touch with friends and family. Since so many people around the world depend on these technologies, they have become one of the primary attack methods used by cyber attackers. This attack method is called phishing. Learn what phishing is and how you can spot and stop these attacks, regardless if you are at work or at home.

What Is Phishing

Phishing is a type of attack that uses email or a messaging service to fool you into taking an action you should not take, such as clicking on a malicious link, sharing your password, or opening an infected email attachment. Attackers work hard to make these messages convincing and tap your emotional triggers, such as urgency or curiosity. They can make them look like they came from someone or something you know, such as a friend or a trusted company you frequently use. They could even add logos of your bank or forge the email address so the message appears more legitimate. Attackers then send these messages to millions of people. They do not know who will take the bait, all they know is the more they send, the more people will fall victim.

Protecting Yourself

In almost all cases, opening and reading an email or message is fine. For a phishing attack to work, the bad guys need to trick you into doing something. Fortunately, there are clues that a message is an attack. Here are the most common ones:

- A tremendous sense of urgency that demands “immediate action” before something bad happens, like threatening to close an account or send you to jail. The attacker wants to rush you into making a mistake.
- Pressuring you to bypass or ignore your policies or procedures at work.
- A strong sense of curiosity or something that is too good to be true. (No, you did not win the lottery.)

- A generic salutation like “Dear Customer.” Most companies or friends contacting you know your name.
- Requesting highly sensitive information, such as your credit card number, password, or any other information that a legitimate sender should already know.
- The message says it comes from an official organization, but has poor grammar or spelling or uses a personal email address like @gmail.com.
- The message comes from an official email (such as your boss) but has a Reply-To address going to someone’s personal email account.
- You receive a message from someone you know, but the tone or wording just does not sound like him or her. If you are suspicious, call the sender to verify they sent it. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.

Ultimately, common sense is your best defense. If an email or message seems odd, suspicious, or too good to be true, it may be a phishing attack. Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Tonia Dudley has been developing and running Security Awareness programs since 2011, which includes building an award-winning phishing training program. You can find her at www.linkedin.com/in/toniadudley.

Resources

Social Engineering:	https://www.sans.org/u/Cb1
Helping Others Secure Themselves:	https://www.sans.org/u/Cb6
Email Do’s and Don’ts:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

License