Chapter Security Playbook

Chapter Security Playbook

PMI's Digital Security team is aware of a recent uptick in the volume and sophistication of phishing scams targeting various PMI accounts. We've seen these attempts via text, email, and even WhatsApp, including some messages to our community members seeking donations and gift cards.

With this uptick, we want to empower you to be more knowledgeable about identifying scams and you're safeguarding your information. If you have questions about this, please contact your Chapter Engagement Partner.

What is Phishing?

Phishing is a type of cyber-attack to deceive individuals into revealing sensitive information, such as usernames, passwords, credit card details, and other personal data. Phishing is achieved through fraudulent communications that appear to come from a trustworthy source, such as a well-known company, a bank, a government agency, or even friends and family members. The goal of phishing is usually to steal identities, commit financial fraud, or gain unauthorized access to systems.

Phishing attacks are commonly delivered via:

• Emails:

Email is the most prevalent medium for phishing. Attackers send emails that mimic the style and appearance of legitimate emails from credible organizations, often containing links to fake websites where victims are tricked into entering personal information.

• Text Messages (SMS):

Also known as "smishing," this method involves sending fraudulent messages that prompt recipients to provide personal data or click on malicious links.

• Messaging Apps and Social Media:

Phishing attempts can also occur through platforms like WhatsApp, Facebook Messenger, or other social media, where attackers impersonate acquaintances or reputable entities.

• Phone Calls:

Known as "vishing," this technique uses voice communication to trick individuals into divulging personal information directly over the phone.

Recognizing Phishing

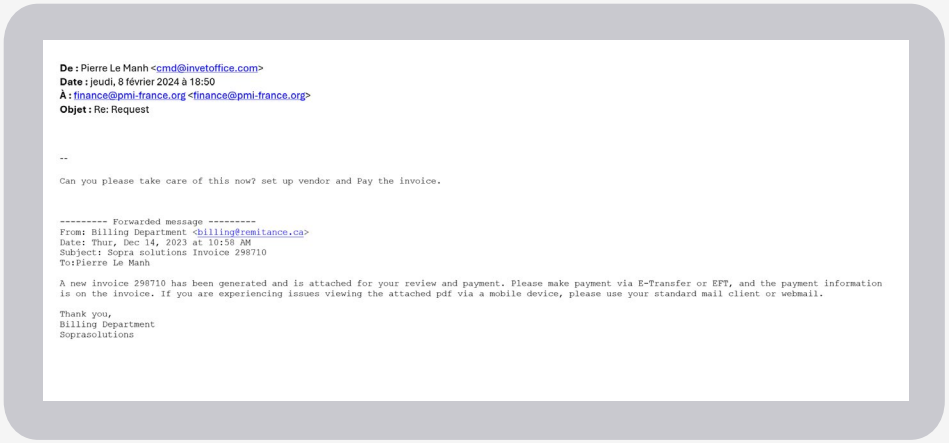
Phishing messages typically create a sense of urgency, fear, or curiosity to prompt immediate action. They often ask recipients to verify their accounts, change their passwords, or provide information to help resolve a supposed issue. Recognizing phishing attempts involves scrutinizing the sender's information, the quality of the communication, and being cautious with unsolicited requests for sensitive information.

To learn more about phishing, watch this YouTube video from IBM Technology.

To learn more about recognizing and reporting phishing, watch this YouTube video from the Cybersecurity & Infrastructure Security Agency.

Below, you'll find screenshots of recent scams targeting our chapters.

Scam Examples:



De : Pierre Le Manh <cmd@invetoffice.com>
Date : jeudi, 8 février 2024 à 18:50
À : finance@pmi-france.org <finance@pmi-france.org>
Objet : Re: Request

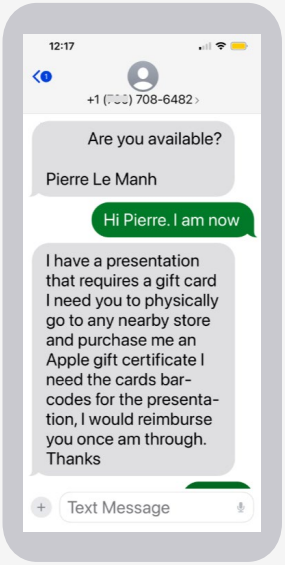
--

Can you please take care of this now? set up vendor and Pay the invoice.

--------- Forwarded message ---------
From: Billing Department <billing@remitance.ca>
Date: Thur, Dec 14, 2023 at 10:50 AM
Subject: Sopra solutions Invoice 298710
To:Pierre Le Manh

A new invoice 298710 has been generated and is attached for your review and payment. Please make payment via E-Transfer or EFT, and the payment information is on the invoice. If you are experiencing issues viewing the attached pdf via a mobile device, please use your standard mail client or webmail.

Thank you,
Billing Department
Soprasolutions

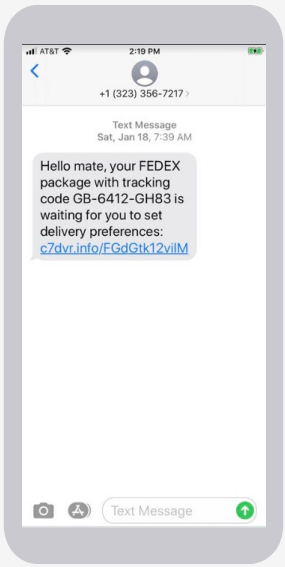


Chapter Security Tips:

1. Be Skeptical:

• Approach every email with caution, especially those from unknown senders.

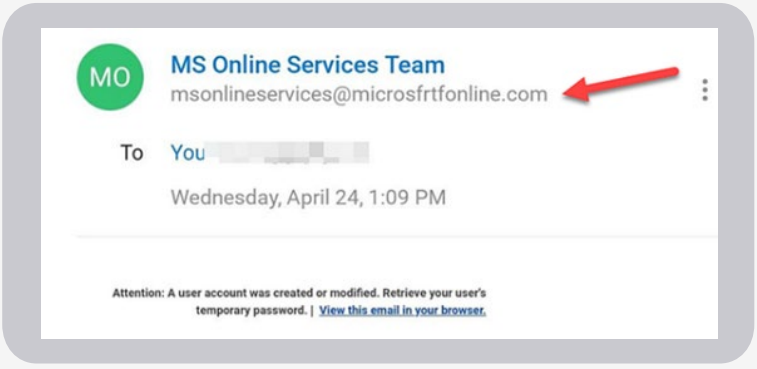
• Scrutinize unexpected emails, even if they appear to be from familiar contacts or reputable organizations.



2. Check the Sender's Email Address:

• Verify the sender's email address, especially if the email requests sensitive information or financial transactions.

• Watch out for subtle misspellings or variations in the sender's email address.



3. Be Wary of Urgent Requests:

• Cybercriminals often create a sense of urgency to pressure recipients into taking immediate action.

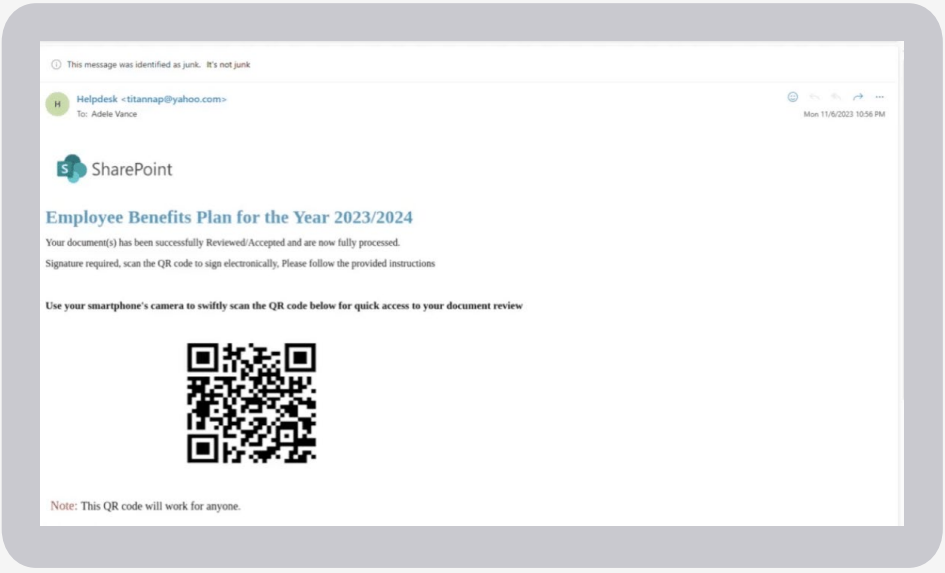
• Verify the authenticity of urgent requests through alternative communication channels before responding.

4. Hover Over Links to Verify:

• Hover your mouse over hyperlinks to preview the actual URL. Avoid clicking on links that look suspicious or lead to unfamiliar websites.

• Watch out for subtle misspellings or variations in the sender's email address.

• Be aware of QR codes that are received via email. These can be previewed via hovering over with your phone or a phone App such as Google Lens or Trend Micro™ QR Scanner.



5. Be mindful of personal information:

• Use a second form of communication to verify any email requests for personal data, money, or bill payments before responding. For example, if the email is from someone you know, call them to verify the request before responding via email. Legitimate organizations usually don't request such information via email.

• PMI will never ask you to randomly sign documents or transfer money. Beware of DocuSign, E-Signature, or other sign-and-return requests, as well as unexpected attachments.

• Donations are only accepted on the PMIEF website: https://www.pmi.org/pmi-educational-foundation.

6. Follow chapter financial policies for the financial security of the chapter:

• A policy requiring dual signatories will enhance the security of your financial assets.

• Learn More in the Chapter Leader Guide for Financial Management.

What to do if you fall victim to a Phishing attempt

• Secure Your Accounts

Change the passwords for any compromised accounts immediately. Use strong, unique passwords for each account. If you do not use MFA (Multi-Factor Authentication) enable it immediately or reset your MFA with the suspected account.

If received via Text or Phone call, stop responding and block the number. Be wary of future attempts.

• Report the Phishing Attempt

Report the phishing email or message to authorities. This could be your email provider, the organization being impersonated, or your IT contact.

• Check for Malware

Run a thorough antivirus scan on your device to ensure no malware was installed during the phishing attempt.

• Monitor Your Accounts

Keep a close eye on your bank accounts, credit cards, and any other financial accounts for any unauthorized activity. Report any suspicious transactions immediately.

To make it easy for you, we've created email copy to share with chapter members and social media copy to share on social media pages.

• Contact PMI

In the event of a security compromise, please promptly email ChapterSupport@pmi.org and inform your chapter partner to ensure proper protocols are followed.

Email and social media templates:

Below are sample email and social media copy to use to share information with your chapter members:

Subject: Urgent: Beware of Phishing Scams and Secure Your Information

Dear Chapter Members,

We are writing to inform you about a critical matter that requires your immediate attention.

There has been a surge in phishing scams targeting individuals across various communication channels, including email, text messages, and social media platforms. These fraudulent attempts aim to deceive individuals into divulging sensitive information or engaging in malicious activities.

Be Vigilant and Cautious:

- *Approach all unexpected or suspicious messages with skepticism, regardless of the platform.*
- *Verify the authenticity of messages before responding or clicking on any links.*

Identifying Phishing Attempts:

- *Scrutinize sender details and verify email addresses or phone numbers.*
- *Exercise caution with urgent requests, especially those soliciting personal or financial information.*
- *Pay attention to grammatical errors or inconsistencies in the message content.*

Protect Your Information:

- *Refrain from sharing sensitive details such as passwords, Multi-Factor Authentication (MFA) codes, credit card information, or personal data via email or text.*
- *Implement two-factor authentication whenever feasible for enhanced security.*

Secure Communication Channels:

- *If uncertain, contact the sender through a trusted and verified method before taking any action.*
- *Utilize official websites or communication channels for sensitive transactions.*

Also, we emphasize that donations to PMI are accepted exclusively through the PMI Educational Foundation (PMIEF) website. We want to reassure you that we will never directly solicit donations via email or any other channel. Please visit the official PMIEF website at https://www.pmi.org/pmi-educational-foundation to make any contributions securely and legitimately.

Your vigilance and cooperation are paramount in ensuring the safety and security of our community. By adhering to these guidelines and exercising caution, we can collectively combat phishing attempts and protect our members from falling victim to fraudulent activities.

Thank you for your attention to this matter. Should you have any concerns or require further assistance, please do not hesitate to reach out to a chapter leader.

Warm regards,
[Your Name] [Your Position/Title] [Chapter Name]

Social Media Content:

IMPORTANT ANNOUNCEMENT 🚫

We're reaching out to inform you about the rising threat of phishing scams targeting individuals through various channels, including email, text messages, and social media platforms. Phishing attacks aim to trick you into disclosing sensitive information or engaging in malicious activities.

BE VIGILANT AND CAUTIOUS:

-Treat all unexpected or suspicious messages with caution, regardless of the platform.
-Verify the authenticity of messages before responding or clicking on any links.

IDENTIFYING PHISHING ATTEMPTS:

-Scrutinize sender details and verify email addresses or phone numbers.
-Be wary of urgent requests, especially those asking for personal or financial information.
-Check for grammatical errors or inconsistencies in the message content.

PROTECT YOUR INFORMATION:

-Never share sensitive details like passwords, credit card information, or personal data through email or text.
-Use two-factor authentication whenever possible for an added layer of security.

SECURE COMMUNICATION CHANNELS:

-When in doubt, contact the sender through a trusted and verified method before taking any action.
-Utilize official websites or communication channels for sensitive transactions.

DONATIONS ACCEPTED ONLY THROUGH PMIEF WEBSITE ✅

You will never be contacted directly asking for donations, and PMI only accepts donations through the PMIEF website.

OFFICIAL PMIEF WEBSITE 🌐

When making a donation or contributing to a PMI cause, please visit the official PMIEF website at https://www.pmi.org/pmi-educational-foundation. This platform guarantees a secure and legitimate channel for supporting our organization's initiatives.