1847Financial | HTK

Top cyber threats and scams for financial professionals to look out for

1. PHISHING

Phishing can occur through email, social media, text (i.e. smishing) and even phone calls (i.e. vishing.)

Cyber-criminals and fraudsters use your human nature and your willingness to help and trust others. Specifically, they will often use social engineering to "trick" you into doing something that benefits the criminal such as:

- Clicking on a malicious link
- Opening a malicious document attachment
- Providing confidential or personal information such as financial or login information

Targeted phishing emails sent from Compromised email accounts

Did you know that trusted colleagues, clients, vendors and people you do regular business with may have their email accounts compromised (or hacked) and the criminals may then use those compromised emails accounts to send targeted phishing emails to you?

Unfortunately, it is happening in our industry. Criminals will often send targeted phishing emails from these compromised accounts that look like invoice requests, voicemails, document sharing, and secure emails. This really highlights that you cannot trust a known email simply because you recognize the sender's name or email address.

Phishing useful safeguards and actions:

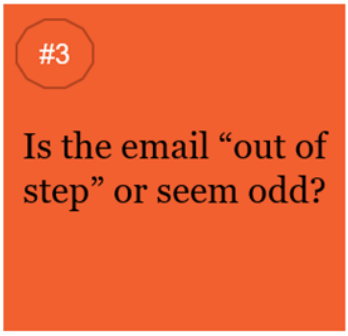
- Always verify any unexpected or unusual requests by calling the sender using the phone number you have on file. Many times people do not know there email account has been compromised until they received a phone call from you.
- Look for warning signs and if the request is using scare tactics or seems to be urgent – don't react or respond based on your emotions.
- Always go the official website you know and trust versus clicking on a link in any email.
    - Criminals are very good at creating fake websites by altering spelling, using different fonts, and using different web domains that mimic the official website. Some examples:
        - You are expecting ".com" and you see ".net"
        - You are being directed to a non-US website such as "www.website.ru". This is the country code for Russia etc.
- Verify any unexpected or unusual requests by calling the sender using the phone number you have on file.
    - Never confirm an email by sending an email. The email account could be compromised and the criminal may have access to that email account.
- Report all suspected phishing emails to your email provider, if feature is available.

Last reviewed: 11/2024

7254362RG_Nov26

Many real threats sent from compromised email accounts are not addressed to people at our company. If you do not see your email address – you should proceed with caution. Call the sender to verify the email.

Many real threats sent from compromised email accounts prompt you to click on a link or enter your login information to view documents or request. Looking at previous emails can help you determine that the email is out of character and you should call the sender to verify the email.



Many real threats from compromised email accounts may not be consistent with previous conversations or interactions you have had with the sender. Unexpected emails or emails that are out of character for the sender should be verified by calling the sender.

2. RANSOMWARE

Ransomware is often spread through phishing emails that contain malicious links or document attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge. Today, most users know what a ransomware attack is because it continues to be in the news and when the ransomware is activated, it encrypts all the files on the system where it was launched and will try to encrypt files on shared drives mapped on the system.

Ransomware useful safeguards and actions:

- Do not click on links or open document attachments unless you are certain the email is safe.
- Do not browse or download files from untrusted web sites.
- Keep your business operations separate from your personal resources and activity.
- Avoid websites with low reputation or websites containing a large number of advertisements.
- Configure your devices to automatically apply software updates.
- Install and maintain anti-virus, anti-malware and configure automated scans.
- The encryption prevents users from accessing their own files and the files on their shared drives until a payment is made, or the files are decrypted (via a key). It is easy to see how this can disrupt normal operations. Remember, criminals are not trustworthy. They may not send the decryption key or they may publish the user's or client's data even if the ransom payment is made.

3. TECHNICAL SUPPORT SCAMS

Our financial professionals and their staff continue to be targeted by technical support scams. This often happens when a cyber-criminal states your computer has a virus or an error occurs and prompts you (the victim) to call or go to a website for technical assistance. Unfortunately, some financial professionals have clicked, called and almost permitted unauthorized parties remote access to "FIX" their computers.

Last reviewed: 11/2024

7254362RG_Nov26

Technical Support Scams useful safeguards and actions:

- Never allow anyone remote access to your personal computer based on a phone call, pop-up alert, etc.
- Reach out to a trusted vendor for assistance with your personal computer and devices.
- Bad actors or criminals will often try to gain your trust by stating that they are from Penn Mutual or legitimate companies such as Comcast, Microsoft, or Apple before offering you free support by phone, chat or website.

Failing to remain vigilant can expose you and your business to malware and data loss, and could be considered a reportable incident according to the applicable State or Federal laws and regulations.

4. PHONE CALL SCAMS

Phone call scams involve fraudsters making deceptive calls to you, posing as trusted entities like government agencies, tech support, your clients, or your vendors. The fraudster's goal could be to obtain sensitive or personal information about you, gain access to your devices, update mailing addresses, change banking information on direct deposits, or to receive payments. Common types include impersonation, phishing, robocalls, and tech support scams. Criminals are now using Artificial Intelligence (AI) to use voice recording available on social media and other websites to impersonate family, leaders, and trusted colleagues as well.

Phone Call Scam useful safeguards and actions:

- To avoid falling victim, individuals should be cautious of all unsolicited calls.
- Always verify the caller's identity, ask questions, consider calling the person back using the phone number you have on file, and refrain from sharing personal or financial information over the phone.

Here are some links to videos that highlight some recent phone scams.

- "Say Yes" phone scam
- How phone scammers are using AI to imitate voices
- This is how hackers hack you using simple social engineering (phishing phone call)