PHISHING SCAMS

Be the one that got away

Phishing involves the use of an email, text message or phone call that appears to come from a trusted source or institution, vendor or company, but is actually from a third-party impostor. Phishing messages are intended to trick you into giving fraudsters your information by asking you to update or confirm personal or online account information. Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Fraudsters cast a wide net and make thousands of phishing attempts – they only need one or two dupes to make it pay off.

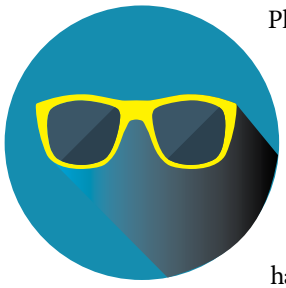
TIPS TO HELP YOU IDENTIFY A PHISHING EMAIL

- *An irregular salutation from someone you are familiar with, such as "Hello Mr. Smith," instead of "Hi Johnny."*
- *"…suspicious transaction," "…account outstanding": An alert to reset password or login to your account to review invoice or payment.*
- *"…your account has been hacked": A request to update your information and go to a website or attachment, then prompting you to enter your account number, password, and personal information.*
- *"…won a big prize," "…refund to you": A request to go to a website or open an attachment to claim monies.*
- *"…document I promised": Posing as someone you know who may send you documents, a request to open an attachment.*
- *A call from a fraudster claiming to be from a legitimate corporate or government entity saying that you owe money or face civil/criminal charges.*
- *Requesting payment in Bitcoin.*

Phishing is also becoming more sophisticated. Fraudsters can conduct research about you through the internet and other means to obtain information unique to you, including your practice area, your clients, and your personal life. A "spear" phishing attempt is a phishing message that is personally addressed to you, will appear to be from someone you already know (such as a senior partner at the same firm), and may include other detailed personalized information.

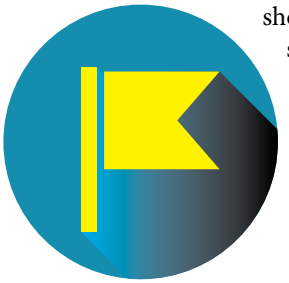
Fraudsters do their best to make phishing messages look official and legitimate. They will mimic real communications from the company or entity they are supposedly from by using the same layout, fonts, wording, message footers and copyright notices, etc. as official messages. They will often include corporate logos and even one or more links to the alleged sender's real website.

How to spot phishing messages



Phishing scams work because they are convincing and prey on your trust of the source. If you get a phishing message from a bank and you don't have an account there, you aren't likely to fall for the scam. However, if you have an account at that bank, the message may look legitimate to you and you are more likely to fall for the scam. Many phishing messages will include a link or attachment that you are asked to click so you can update your information. After doing so, the webpage or attachment you will see (which will also have text and logos to make it look official) will prompt you to enter your name, account number, password and other personal information – thereby giving it to fraudsters.

Red flags



- The link you are asked to visit is different from the company's usual website URL (place your mouse over the link and look at the taskbar in your window to see if the link matches. It should take you to the proper website).
- The main part of the sender's email address is not the same as the company's usual email address.
- Spelling and grammar mistakes.
- A sense of urgency – money has to be transferred quickly without the usual checks and balances.
- The promise of receiving money or another big prize.
- Anyone asking for money – even if you know them.

Don't take the bait

Never respond to phishing requests for personal information in the mail, over the phone or online. Most importantly – this is probably the most common way that personal information is stolen – never ever reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother's birth name or birthday), even if they appear to be from a known or trusted person or business. Legitimate businesses should never send you an email asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don't use the number in the email – it could be fake too!

Anyone can be targeted

Follow firm processes and procedures for the review and approval of financial transactions – and don't bypass them due to urgent circumstances. Never share confidential client or firm information without being sure it is appropriate to do so by getting confirmation from someone familiar with the file. Be on the lookout for and question any last minute changes on fund transfers or payments. ■