CYBERSCOUT®

PHISHING PROTECTION TIPS

How to steer clear of threats

Watch for communications from unknown or untrusted senders. Be wary if you are receiving communications from anyone that you do not know personally or do business with. Pay close attention to the content since it is possible that a friend or family member's account could have been hacked. If they are asking for money, contact your friend or family member by phone to verify the request. Check to see if the displayed link matches the underlying hyperlink. Place your cursor over the link in the email, does the pop-up address match the link in email?

Pay attention to expressions of urgency or immediate requests for action. Scammers will try to make you act quickly by saying that your account will be closed or a purchase will be cancelled if you do not act immediately. They want you to act before you think. Don't fall for it.

Look for requests for sensitive personal information. Banks, merchants, and other reputable institutions will never ask for your personal or account information by email, so never provide it. If you have any concerns, call the organization directly to verify the legitimacy of the communication.

Check for spelling or grammatical errors. Many of the phishers are from outside of the United States, so they don't have a strong grasp of the English language. If you see misspelled words, wrong use of pronouns and tenses or other grammatical issues, it could be a phish.

Remember, if it is too good to be true, it probably is! If you receive a communication out of the blue saying that you won the lottery or are heir to a foreign fortune you might want to think twice before claiming your reward.

Always use updated anti-virus software. Especially one with an anti-phishing filter.

What should I do if I believe I am a victim?

If you have clicked on or downloaded anything that might infect your system, then make sure you install or update anti-virus software and run a full scan of your system. If you have sent funds make sure that you contact your financial institution immediately to report the situation.

If you have reason to believe that any of your email or social media accounts are compromised make sure you change the passwords immediately. If you have disclosed any personal information contact CyberScout so we can assist you in checking your credit reports and with taking precautionary measures to protect your credit profile.