

# Recognize & Avoid Phishing

Phishing emails have become one of the primary attack methods in the cyber criminal's playbook. These attacks try to trick you into taking an action, such as clicking a link, opening an attachment or responding with sensitive information. We're all a target, both at work and at home, because our information – and our devices – are worth good money to cyber criminals. Read on to learn how to spot phishing so you don't take the bait!

## PROTECTING YOURSELF – KNOW THE 'RED FLAGS' OF PHISHING

- ✓ **Check the sender.** Is the message from a generic address or one not associated with a legitimate company?
- ✓ **Dear Customer.** Did the email use a generic salutation such as 'Dear Customer' or nothing at all? Service providers usually know who you are and typically personalize emails with your name and the last few digits of your account number.
- ✓ **Bad spelling and grammar.** Legitimate businesses go out of their way to proofread their email. If an email has lots of spelling mistakes or improperly worded sentences, it's a red flag.
- ✓ **Urgent requests.** Messages of an urgent nature, or requesting an immediate action, are a common method used to rush people into making mistakes. Another indicator of a red flag.
- ✓ **Be careful with website links.** If you hover your mouse over a website link, you will see the actual destination of the website you're about to visit. If that location differs from the way the link is written in the email, it's a good indication of an attack.
- ✓ **Be suspicious of attachments.** If you don't know the sender, or receive something from a friend that looks suspicious, don't open the attachment. If it is from someone you know, you can always pick up the phone and give them a quick call to make sure they actually sent the email.
- ✓ **Requests for sensitive information.** Be suspicious of requests for sensitive information, such as user IDs and passwords, financial account numbers or social security numbers.
- ✓ **Sound too good to be true?** Sorry, you probably didn't just win the lottery or a new iPad.

## HANDLING A PHISH

Suspect a phish? If you've received an email that has red flags or looks suspicious, don't click or open anything. Simply delete it from your inbox.