The Focus on.. Phishing

DID YOU KNOW?

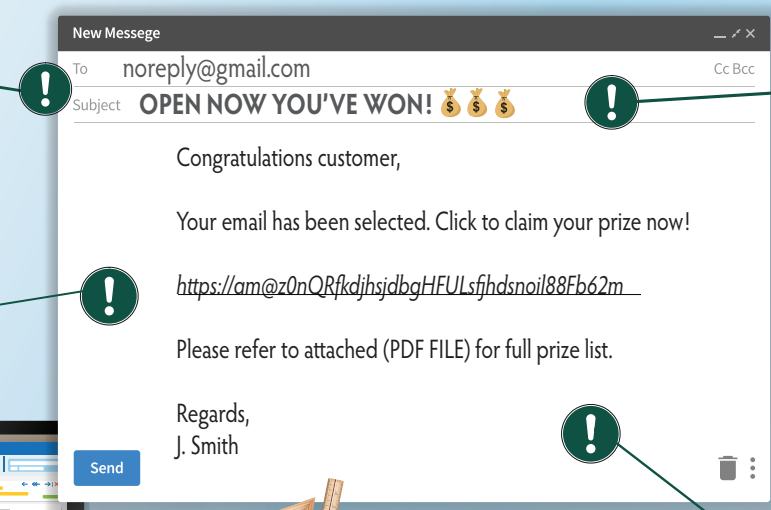
In 2021 businesses lost approximately $1.8 million *every minute* due to cybercrime!

X CHECK THE SENDER'S DOMAIN AND EMAIL ADDRESS

Legitimate companies send emails from their official domain, like "microsoft.com," not variants like "microsoft.business.com." If a domain looks odd, check the address on the sender's website.

X USE CAUTION IF A MESSAGE ASKS YOU TO LOG IN OR CLICK A LINK

Consider the links that a message asks you to click to see if they're going to the company's actual domain. When in doubt, log in to their site directly. Fraudulent password reset and log back in requests are a staple of phishing.



X CONSIDER THE SUBJECT LINE AND URGENCY OF THE EMAIL

Does the subject line seem a little "off" to you? Are there odd phrases, emojis, or unusual things in the subject line? Is the content conveying urgency, ramifications for not taking immediate action, or promising somethng too good to be true? If yes, it may indicate a phishing attempt.

X BE WARY OF UNEXPECTED ATTACHMENTS LIKE PDFS OR WORD DOCUMENTS

If you aren't expecting an attachment, the attachment has a strange name, it seems susicious, or out of place, it might be malware or ransonware which is frequently deployed through phishing.

About 25% of the emails that businesses receive from major brands like Amazon, Microsoft, or DHL are impersonations. Knowing how to spot these cleverly crafted phishing attempts could prevent a cybersecurity disaster for your organization.

ROUSE CONSULTING GROUP

(309) 762-3589 | www.go2rcg.com