Phishing: The More Things Change…

Our utility strives to block malicious messages from hitting your inbox, but with the pace threat actors adapt their scams, it's often difficult for the email filters to keep up. As such, phishing emails do get through. To that point, in 2023 Cofense reported catching a **malicious email that bypassed its customers email filters EVERY MINUTE** – *that's a lot of phish!* While email is not the only method attackers use for phishing, year-after-year it's one of the most prominent and prolific.

Social engineering: *In the context of cybersecurity, social engineering exploits human emotions to ultimately obtain information that could be used to facilitate a cyber attack to commit fraud against or otherwise harm us or our utility.*

Phishing: *A social engineering technique for attempting to acquire sensitive data/information through a fraudulent solicitation in which the perpetrator masquerades as a legitimate business or reputable person.*

Given all the phish, we do our best to keep you aware of the various phishing themes, tactics, and subjects for you to watch out for. However, it's not practical, or even possible to keep you aware of everything, nor to expect you to remember it all. Despite all the phish and different ways threat actors use to trick us, there's one thing that's constant – **attackers try to elicit a hasty response based on emotion**. Fear, urgency, doubt, and curiosity are some of the most common emotions leveraged to pressure us into falling for a phish and the highest volume of themes designed to elicit those emotions are regarding finances, notifications, shipping, and responses.

Common Phishing Email Themes:

- **Finance**-themed emails typically have subjects relating to invoices, payments, pay slips, statements, orders, remittances, or receipts.
- **Notification**-themed emails typically have subjects relating to password expiration, reminders, messages, required actions, recent activities, or appointments.
- **Shipping**-themed emails typically have subjects relating to shipments, port information, arrival notices, cargo, or anything to do with DHL, FedEx, UPS, and USPS.
- **Response**-themed emails typically have subjects relating to any sort of response or sometimes forwarded messages as well as hijacked and spoofed email threads. While many threat actors spoof reply chain threads, the most advanced threat actors hijack pre-existing email threads.

Misspellings are a misnomer. While it used to be a dead giveaway, today's phishing messages are more carefully crafted and contain fewer spelling and grammar errors. You're more likely to receive a legitimate email with bad spelling than a poorly crafted phishing email. However, do pay attention to the *tone* of the message. **Trust your gut!** If an email or message appears to be coming from a coworker, manager, vendor, or other trusted partner, but the wording doesn't sound like them, or the overall tone or signature is wrong, it's likely a phish!

Report Phishing Emails – even if you're not sure if it's a phishing email, or even if you already opened or actioned it. Some organizations use phish report buttons integrated into the email client for easy reporting. Otherwise, report it to the helpdesk, tech support, or your manager/supervisor. Plus, **your reports help** us understand and block more messages and themes that are evading the email/spam filters. Additionally, if you believe you've personally been a victim of phishing, report the fraud to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov or the Federal Trade Commission at https://reportfraud.ftc.gov/.

CYBERSECURITY AWARENESS MONTH