PROJECT CYBERSAFE™

NEWSLETTER

A QUARTERLY CYBERSECURITY PUBLICATION

RED FLAG AWARENESS WITH PHISHING EMAILS

Protecting yourself from falling for an email scam starts with analyzing the FROM field and the email signature for signs of impersonation.

1. Does the name in the FROM field and email address match that of the person you are expecting to interact with?
2. Does the email signature match the email address?

If you answer NO to either of these questions, there is a good chance this email is not legitimate and interaction with the email needs to be avoided.

3. DO NOT reply in any way to any calendar invites from unfamiliar email addresses at all.

DELETE and MOVE on!
Many times, responding in any way to these types of emails will let the cybercriminals know that a live user exists at your email address and they will continue to attempt to get you to engage now that they have confirmed someone is using that mailbox. The Federal Trade Commission (FTC) has guidance and resources for businesses, providing tips to recognize and avoid phishing scams. Visit the FTC website for more information.

BREAKING THE STIGMA

Does your company have a Simulated Phishing testing and training program? An independent survey by KnowBe4 reports that over 90% of employees agree that phishing simulations improves their security awareness. Read the KnowBe4 article here.

(from the article)
Five meaningful ways organizations can leverage phishing simulations:

1. **Make Simulations Relevant and Realistic:** Use personalized phishing tests that reflect real-world threats employees might encounter, rather than unrealistic or overly deceptive for the sake of catching people out.
2. **Focus on Education:** Use these situations as learning opportunities by providing immediate, constructive feedback that clarifies what went wrong and how to identify similar threats in the future and implement a fair escalation process if necessary.
3. **Provide Timely Follow-ups and Training:** When an employee interacts with a simulated phishing email, offer immediate guidance and micro-training on recognizing phishing attempts. Reinforce learning with periodic training sessions, rather than just tracking failures.
4. **Ensure Transparency and Fairness:** Let employees know that phishing simulations are part of the company's security awareness program. Avoid using overly deceptive tactics that feel like entrapment and ensure the difficulty level is appropriate.
5. **Reward Security Awareness:** Recognize and reward employees who report phishing attempts, whether simulated or real. This can be as simple as shout-outs in meetings, gamification, leaderboards, or small incentives to encourage vigilance.

A PROGRAM OF NSSF® The Firearm Industry Trade Association

WHY USING MULTIFACTOR AUTHENTICATOR APPS CAN BE MORE SECURE THAN SMS AUTHENTICATION

Roger Grimes, Data-Driven Defense Evangelist for KnowBe4, has an article about fake MFA Reset Warning Messages that people are receiving through SMS text messages. Using a Multifactor Authenticator App over SMS codes whenever possible can help defend you from having to rely on SMS MFA codes as little as possible.

It highlights the importance of not trusting notification URL's and "Going to The Source" by logging directly into the account through a browser or dedicated App to confirm any notifications.

What is Multi-Factor Authentication
Multi-Factor Authentication (MFA) is the process of a user or device providing two or more different types of proofs of control associated with a specific digital identity, in order to gain access to the associated permissions, rights, privileges, and memberships. Two-Factor Authentication (2FA) implies that exactly two proofs are required for a successful authentication, and is a subset of MFA.

What is SMS Authentication
SMS authentication is a simple type of 2FA or Multi-Factor Authentication (MFA). Users who sign in receive a text message with an authentication code. All they have to do is fill in the code on the platform to gain access. It is commonly used across major social sites like Twitter, Instagram, and Google.

FBI WARNS OF BADBOX 2.0 – A CYBERATTACK THAT TARGET HOME IoT DEVICES

Techreport shares an article about the recent warning issued by the FBI about a cyberattack that target home IoT (Internet of Things) devices.

3 tips provided in that article are a great start to help protect yourself and your home network from falling victim to this newest attack. Read the full article here.

1. **Only Buy from Reputable Providers**
   Most of the compromised devices come from China and go for sale under unknown or anonymous brand names.
2. **Do NOT Disable Google Play Protect**
   Play Protect scans apps on your phone for malicious behavior and warns you if any suspicious installation takes place. It also works for side-loading, i.e., installing apps outside of the Google Play Store.
3. **Check Network Traffic**
   Use a trusted network scanner app that will scan your local network and list all connected devices.

What is IoT (Internet of Things)?
IoT, or the Internet of Things, refers to a network of physical devices embedded with sensors and software that connect and exchange data over the internet. This technology allows everyday objects, from home appliances to industrial machines, to communicate and operate autonomously, enhancing efficiency and convenience.

KIDS CORNER

Social media Apps, like TikTok and Instagram, are being used as attack vectors by cybercriminals with promises of free crypto currency or enhanced features for popular Apps.

Make sure you explain the dangers that these free offers pose to your family's home network and financial security. BleepingComputer has an article about describing how cybercriminals are using these free offers to install infostealer malware on victim's devices. Read more.