SECURE OUR WORLD

Prepping for Cybersecurity Awareness Month

THIS MONTH'S TOPICS:

Phishing Defined

Defining different types of scams

Protect Yourself Online

The best practices to secure our world

Scam of the Month:

MFA Fatigue Scams...

Monthly Cyber News:

Recent News and Upcoming Dates...

Cybersecurity Awareness Month begins next week! In preparation for this cybersecurity holiday, we are going over the basics of the themes and topics that will be covered throughout the month.

In this month's newsletter, review the definitions of different types of phishing, learn about multi-factor authentication, password best practices, and implementing software updates. Now is the time to refresh on the cybersecurity habits that are important if you want to carry out this year's Cybersecurity Awareness Month theme: Secure Our World!

Phishing Defined

Think Before You Click!

Email Phishing

Attackers send emails that appear to be from trusted sources, such as banks or online services asking you to click on a link or download an attachment. Be cautious of emails that claim to be urgent and demand your information or payment details.

Spear Phishing

This is a targeted attack where the scammer tailors the message to a specific individual by gathering extensive research from data breaches or social media to craft personalized messages or calls that are full of the user's personal details.

Vishing

Vishing or voice phishing, involves attackers calling and pretending to know you or to be from a reputable organization to extract information or money. Do not share personal information over the phone unless you are certain of the caller's identity.

Smishing

Refers to phishing via text message. Attackers try to trick users into clicking on a malicious link or divulging personal information. These messages range from pretending to be from a business to posing as a random person texting the wrong number.

PROTECT YOURSELF ONLINE

This year’s theme, "Secure Our World," emphasizes the importance of taking proactive steps to protect our digital lives. Let's dive into three critical areas: passwords, multi-factor authentication, and updating software.

Strong Passwords

In brute force attacks, scammers simply try a variety of commonly used passwords to force their way into a user’s account. This is one of many reasons why it is important to use complex passwords. To create strong passwords, use a mix of letters, numbers, and special characters. It’s also important not to use the same password for multiple accounts in case one account is breached.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an extra layer of security beyond just a password. It requires two or more verification methods: something you know (like a password), something you have (like a smartphone), or something you are (like a fingerprint). Enable MFA on all accounts that offer it. Use Authentication apps for an even more secure MFA than SMS-based codes.

Update Software

Software updates are a set of changes to a certain program which are meant to fix or improve it in some way. They often include patches for security vulnerabilities. Delaying updates leaves your devices exposed to threats.

Use Security Software

While your organization likely provides security software for work devices, make sure your personal devices are also protected by security software such as antivirus protection. Security software can help protect devices from viruses and malware.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Miguel is a dedicated employee in the corporate offices of a department store chain. As part of his daily routine, he uses multi-factor authentication (MFA) to access his work applications. One morning, while he was focusing on a crucial project, his phone buzzed with a push notification asking him to approve an MFA request. Distracted, he declined the request, thinking it was a mistake. But the notifications kept coming—buzz after buzz, interrupting his workflow.

Frustrated by the barrage of alerts, Miguel approved one of the notifications, hoping it would stop the interruptions. The alerts did stop, but this was exactly what the attacker was counting on. A cybercriminal had obtained Miguel's login credentials through a phishing scam and was now using an MFA fatigue attack to gain access to his company's system. By the time Miguel realized his mistake, the attacker had already infiltrated the network, leading to a significant security breach.

Did you spot the red flags?

- Miguel should have discussed the issue with a manager or IT worker before approving the verification attempt.
- Miguel should not have approved the MFA request since he did not try to log into his account in the first place.

If you receive multiple unexpected MFA requests, do not approve them. Immediately report the incident to your IT department and change the related account's password.

Instead of using push notifications, try other types of MFA. Consider using biometric authentication (like face scans or fingerprints) or authenticator apps, which are less susceptible to MFA fatigue attacks.

CYBER NEWS

SEPTEMBER 2024

THE MOST SUCCESSFUL WORDS IN SCAMS

After analyzing large amounts of data, a recent study has identified a trend of common words that appear most frequently in scam messages that are successfully deceiving users. Here are the top 5:

1. Income
2. Investment
3. Money
4. Loan
5. Credit

Interestingly, the study found that “Free” was the most commonly used word in scam messages but was the least successful.

UPCOMING DATES

Cybersecurity Awareness Month is coming up in October. The theme is Secure Our World. Check out staysafeonline.org and CISA.gov for more information on how to celebrate and stay secure.

THE STATS BEHIND THE BEC SCAM

According to the FBI, BEC scams have cost users over $55 billion in the past ten years. From 2022 to 2023, there was a 9% increase in global losses. BEC, or business email compromise scams, typically occur when a cybercriminal poses as an employee or boss of a company in order to gain access to sensitive information. BEC scams have impacted users in over 187 countries. To avoid falling for BEC scams, always check the sender’s address to see if it matches the typical address they contact you from. Verify any strange requests from coworkers through a second method of communication.