Cybersecurity Awareness Month 2022: Recognizing & Reporting Phishing

October 24, 2022
By: Marian Merritt
https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-recognizing-reporting-phishing

This blog will officially wrap up our 2022 Cybersecurity Awareness Month blog series — today we have a special interview from Marian Merritt, deputy director, lead for industry engagement for the National Initiative for Cybersecurity Education (NICE)! Marian will be discussing the importance of recognizing and reporting phishing incidents in detail. A phishing attack is an attempt to fool an individual into sharing private information or taking an action that gives criminals access to your accounts, your computer, login credentials or even your network.

Phishing is a good example of a fundamentally important topic. Our approach this year took us into a new direction. We got really creative and worked with NIST's Emmy-award-winning video team to craft some wonderful, animated films. One of them features some very cute little koi — actual fish — to help us tell the story of a small business owner whose experience with phishing could potentially help someone else avoid falling victim. The phishing video, along with two others, one on ransomware and the other on multi-factor authentication — have companion, downloadable discussion guides that an employer or manager could use to start a business-wide conversation on the topic. We hope that a business owner might send the video link to their team or start a lunch and learn series or share it during a staff meeting — October is the perfect time for that!

What is the easiest way to stay safe online?

I'm not sure there is ever going to be an easy way — but we can all do better — I'm sure! Passwords continue to be a basic must-have on every device we use. And using NIST guidance for setting passwords is a good start. I use a password manager, which helps me a lot.

I am also very suspicious, not by nature really but by virtue of my over 25 years of experience working in cybersecurity. I assume that any out-of-character online post by a friend, a “friend request” from someone I’ve been friends with for years, an odd reposting of a bizarre news story, a text they wouldn’t normally send me, an unexpected message from my manager asking me to “run to the store for gift cards” — any of the aforementioned items might not be legitimate and should give me reason to pause. (The gift card scam actually happened to me twice.) The real work ahead for all of us is to make sure that people outside of the cybersecurity sector learn to hit pause in that same way, without needing to wait 25 years. Too many small business owners, their employees and all our family members are at risk from scams, including phishing, ransomware, romance and business scams.

It’s crucial that any small business owner consider who has access to company financial systems, including payroll and banking, and provides them with additional training. They must be instructed to be on the lookout for suspicious messages that may arrive in numerous ways: by live telephone call, by voice mail, text, fax, even on social media. They should be reminded that these messages will come with a sense of urgency; will arrive late on a Friday or before a holiday shutdown. The scammers know how to make their demands seem real and push people to make poor decisions. That’s why the business must implement measures to ensure that their team (including their banking partners) know to protect them. It’s remarkably easy for someone to research the company staff at a small business, then call and pretend to be the partner of the owner who is “on vacation” and needs money wired to pay their hotel bill.

What are three things you can do to minimize cybersecurity risks to a person or businesses?

Using the five functions of the NIST Cybersecurity Framework as your model is always a good plan: Identify, Protect, Detect, Respond and Recover. No matter how big or small your business, it just works. Learn more with the NIST Cybersecurity Framework: A Quick Start Guide.

- Protect - Passwords and Multi-Factor Authentication – Use every method available to keep unauthorized users off your devices and out of your accounts. On your phone use passwords or face recognition to lock the screen. Make sure computer screens are locked when not in active use. Use physical tokens and other methods to keep upping the levels of security to make sure only the right people get into the systems and the bad guys stay out.
- Detect - Install antivirus, security software and firewalls and keep them and operating systems and applications patched and updated.
- Recover - Backup - Make full and regular backups of important business information; test those backups regularly to be sure they are complete and functional.