The Merits OF Phishing Your Own Employees

cyber security risk management

Summary: Phishing is still a big problem. One of the best ways to educate people within your bank about the risks is to actually phish them on an ongoing basis.

Fishing is one of the most popular outdoor recreational activities in the US, but you may not know these interesting facts from The Fish Site we uncovered: catfish have 27,000 taste buds vs. 9,000 for humans; lobsters have longer life spans than cats or dogs and live 20Ys; and the typical fish brain is about 1/15 the mass of a similarly sized bird or mammal. Meanwhile, Statista reports that in 2017, more than 49mm Americans participated in freshwater, saltwater and fly fishing.

Many people like to fish it seems, but phishing of another variety is not so popular in banking circles. Despite the increasing complexity of the measures that cybercriminals use, phishing emails still remain one of their most effective tactics.

While the majority of spam and phishing emails people get remain easy enough to identify (simple misspellings, poor English, poor structure), it only takes one person to click to cause a cascading nightmare.

Sadly, not all phishing emails are so easy to spot, especially with the increasing use of legitimate contact software and apps sending email updates. Adding to the email chaos is the fact that cybercriminals have stepped up their game by taking the time to learn about specific individuals or groups by using more targeted efforts. This ups the ante and the risk.

One of the best ways to educate people within your bank about the risks is to actually phish them on an ongoing basis. To do this, start with your Risk and IT departments and send "test" phishing emails to employees. This will give you a good idea what could happen if a real phishing email came in, with response rates, and offer the opportunity to increase awareness and training.

It is also important to teach employees that phishing risks are not just limited to work e-mail accounts, but can also come from social media accounts and personal emails too. This is particularly true when people use the same or similar passwords for both personal and work accounts, or if such accounts are linked to work accounts.

According to a CPA and cybersecurity advisory firm, 90% of the world's cyber attacks begin with phishing emails. Among the types of phishing messages that employees most commonly click on are: messages from human resources; voicemail notifications; notifications from regulatory agencies, vendors or associations; and social media messages.

Another area that may help is to train your staff what not to put in their regular emails. Providing some internal guidance here could reduce the anxiety about the legitimate emails sent in the scope of regular business activities, while learning about the pitfalls of the illegitimate kind.

Some tips here include: tell people ahead of time that you will send an email; if possible, put the complete message in the email vs an attachment or link to avoid any unnecessary concern.

Of course, cybersecurity and employee training require constant updates and review, especially with new employees, but that isn't where it ends. It is also critical to remind even tech-savvy, seasoned employees too, because no one is immune. The attacks are relentless and it only takes one click to cause a significant and possibly expensive issue for the bank.

WHITE PAPER: TRANSITIONING TO SOFR

Bankers have heard that SOFR will replace LIBOR as a benchmark in 2021. But, what is involved in this transition? To learn more about the impact and how your bank can plan for it, download our white paper, "Moving from LIBOR to SOFR: Smoothing the Transition for your Financial Institution" now.