Help Your Employees Keep Up with the Latest Phishing Scams

cyber security phishing

Summary: As phishing attempts constantly evolve, CFIs must train their employees to keep up, such as regularly testing employees through simulated fake phishing campaigns. We share additional tips to help you develop the most effective cybersecurity training program you can to minimize these threats.

The little town of Islamorada in the Florida Keys owns the title of the “fishing capital” of the world, where perennially warm waters foster incredibly diverse ocean life. Fishermen are all but guaranteed to get a bite of either mahi-mahi, wahoo, kingfish, sailfish, marlin, or tuna. There are also prime spots for freshwater fishing, such as Thousand Islands in upstate New York on the eastern edge of Lake Ontario, where you can reel in bass, salmon, walleye, northern pike, and muskellunge.

Fishing is one of the biggest outdoor recreational sports in the US. Its homophone, phishing, has also earned the distinction of being the most common form of cybercrime. When it comes to today’s phishing scams, the latest cybersecurity technology just isn’t enough: it takes regular employee training to keep up with the constantly evolving threat and sheer volume of phishing scams.

Phishing attacks have come a long way from would-be thieves sending generic emails en masse, hoping some poor souls would be duped by a so-called business tycoon needing to transfer money to Nigeria. Now, more sophisticated phishers do their homework on selected targets via social media, or hack into a corporate computer system to gain access to the target’s email and information.

Even employees at community financial institutions (CFIs) can fall for requests to transfer funds from what seems like a real customer because the requests came from their actual corporate email address — though in reality, it was the hacker who was in control.

“If employees aren’t aware of this practice, they may not question why the CFO, who never reaches out to them directly, is asking them to transfer funds, or why someone in accounts payable is asking them to pay a vendor at a different account than what has been used before,” says Dror Liwer, CFO of Coro Cybersecurity. This is why CFIs must provide employees with continual education on phishing so they’ll know exactly what to look out for.

A CFI based in Mississippi, regularly tests whether its employees can spot the latest phishing scams by running simulated, fake phishing campaigns several times a year based on what hackers are actually attempting in the real world. If an employee is duped, the campaign redirects them to a website that educates them on the red flags they missed, or they can contact a special helpdesk manned by the CFI’s cybersecurity department. The tone is supportive — not disciplinary — in order to encourage employees to be vigilant and reach out whenever they have a concern or are unsure about an email or call.

If your CFI is looking to boost its employee training on phishing scams, look for a phishing simulation solution that can be customized to the particular needs and level of cybersecurity knowledge and savviness of your employee base. Make sure that the simulation solution can be integrated into your existing cybersecurity training program, as well. Given that simple mistakes and human error helps account for over 90% of security breaches, regular exposure to the different kinds of phishing out there will help your employees more easily spot a scam.

Here are additional tips for enhancing your training program:

- **Customize your training for each role within your institution.** The more relevant the training is to each particular role, the more likely the employee will pay attention and retain the information.
- **Make your training interactive and engaging.** In addition to simulations, consider games and quizzes about real-life scams to better capture the attention of employees — and increase the likelihood that they'll recognize similar scenarios if a phishing attempt actually happens.
- **Measure the effectiveness of your training.** Phishing simulation solutions have built-in analytics to determine whether employees are starting to "get it" over time by measuring average clicks on fake phishes. Your institution can also employ machine learning and artificial intelligence tools to measure the effectiveness of your training.

Phishing scams are ever-evolving. Make sure you constantly keep your employees updated with training, and consider routinely conducting simulations to test them. Customize your training to fit each role within your institution — and above all, make the training interactive and engaging to enhance its effectiveness.

HOW DO INTEREST RATE SWAPS BENEFIT MY INSTITUTION?

Business clients are expecting long-term, fixed rates from their financial institutions. See how you can meet both your needs and your borrower's needs with an interest rate swap using Borrower's Loan Protection® (BLP).

ECONOMY & RATES

Rates As Of: 07/24/2023 11:23AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.50	0.07	1.08
6M	5.53	0.06	0.77
1Y	5.36	-0.03	0.66
2Y	4.88	-0.02	0.45
5Y	4.13	-0.03	0.12
10Y	3.86	0.02	-0.02
30Y	3.91	0.05	-0.05

FF Market	FF Disc	IORB
5.08	5.25	5.15
SOFR	**Prime**	**OBFR**
5.05	8.25	5.07

Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.