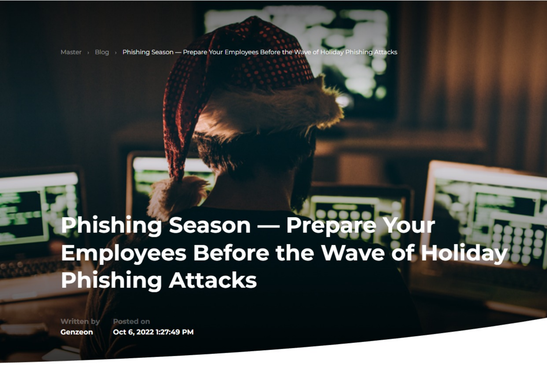


Phishing Season — Prepare Your Employees Before the Wave of Holiday Phishing Attacks

Written by
Genzeon

Posted on
Oct 6, 2022 1:27:49 PM

Could one of your employees compromise your organization's cybersecurity during the holidays?

Imagine. A busy week is rolling to its end on a Friday afternoon in December. Though your staff has been working hard, many of them have also been buzzing with the pursuits of the holiday season—there are parties to plan, decorations to hang, and presents to buy. One of your employees checks his email quickly before leaving the office early to gift shop. An invitation for a special holiday office party catches his eye. He's told he must RVSP today. He fails to notice a few typos and the sender's unfamiliar email domain that suggests this could be fraudulent. He clicks the link. He enters his company login credentials when prompted to complete the RSVP. He's just given a cybercriminal access to his device. Your network and data are now compromised.

This is just one example of how bad actors use phishing to reel in victims during the holiday season. Phishing—in all its variations—continues to be a lucrative method for cyber thieves throughout the year, but during the winter season, they like to pursue their crimes with a holiday twist. And the criminals don't just target individuals; organizations are in their sights, too. Between 2015 and 2021, phishing attack costs quadrupled from $3.8 million to $14.8 million for large U.S. businesses. Just in 2021, business email compromise (BEC) shot up 20 percent from 2020.

As cyber criminals refine and evolve their tactics, it's essential to keep your staff educated and current on the latest phishing tactics and prevention measures.

Is My Organization Really at Risk for Phishing Attacks?

Yes. Many still believe phishing is a financial crime that preys on individuals rather than businesses—but companies are at risk. More employees are now working remotely, and the expansion of remote working has connected more personal devices to enterprise networks. If an employee falls victim to a phishing scam on that device, all company network connections and data are now compromised.

Another example of increased phishing risks is the enduring popularity of virtual work events and parties—especially around the holidays—unwrapping more festive ways for phishers to target businesses.

More Phishing in December

Since 2020, 80 percent of organizations have endured a rise in phishing activity, setting email phishing as the top concern for IT leaders. During the holidays, the risk of phishing attacks only mounts—in December 2021, phishing scams surged a whopping 52 percent. Cybercriminals know people are distracted that time of year and may not be as scrutinizing of bogus emails, phone calls, or texts—and they use that distraction to their advantage.

Source: Barracuda: Phishing attacks spike just before the holidays: Are you prepared?

Phishing and prevention training for your employees is critical for your organization's security—it's only as strong as your weakest worker. Security awareness training can reduce financial damages from phishing attacks by more than 50 percent on average.

Here are some valuable tips and information to help you bolster your employees' phishing knowledge and ward off data breaches.

Want to Test Your Employees?

CompliancePro Solutions has partnered with best-in-class security training provider, KnowBe4, to provide comprehensive security training and phishing exercises. Don't wait for the holidays - make sure to test how phishable your employees are.

The KnowBe4 Phishing Tool is completely free and secure, without any additional commitment.

Free Phishing Tool Information

Prepare Your Employees for Phishing Season

6 Common Ways Criminal Phishers Troll Victims During the Holidays

Cyber thieves can use any type of phishing—email, SMS, or phone—to perpetrate the following types of attacks, though email holds steady as a favorite. Of course, this isn't an exhaustive list, and bad actors are always scheming new approaches. Don't let your guard down if a communication doesn't fall under one of these five.

1. **Bogus Holiday Events**

   Virtual holiday parties and events have built momentum in the past couple of years, and bad actors are capitalizing on that trend. Capturing credit card and billing info is often the goal.

2. **Fake Customer Surveys**

   Consumers like to share their opinions about services and products, and cyber scammers know it. Bad actors are looking for personal and financial information with this phishing bait. The holiday twist often comes in the form of a text or email offering a holiday deal or discount for completing a survey, often from a seemingly well-known retailer.

3. **False Order Confirmations**

   False order confirmations are common lures. And cybercriminals ramp it up during the holidays when many people are preoccupied and easily lose track of their purchases. Credit card and bank info are often the targets.

4. **Phony Shipping Notifications**

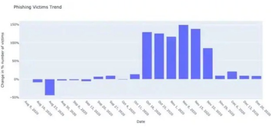
   In the same mindset as false order confirmations, scammers intend to exploit busy, distracted consumers to their favor. The Better Business Bureau even warned customers in 2020 of this popular method.

5. **Fictitious Email Promotions**

   Email promos inundate many inboxes during the holiday season. Gift-givers with eyes for a good deal don't always scrutinize the sleigh-full of offers they receive and easily fall victim to fake promotions to save a little money.

6. **Fake Gift Cards**

   Gifts cards no longer carry the impersonal stigma from years ago. In 2020, the global prepaid cards market was estimated around US$1.6 trillion—and is expected to hit US$2.7 trillion by 2027. Consumers are buying up gift cards and phishers know it. Bogus gift card offers have become an affected lure.



Source: Global Data: Phishing Trends Over the Holiday Season

Tips to Avoid Becoming a Phishing Victim

- Read all texts and emails carefully, looking for warning signs
- Check the sender's email domain to ensure it matches the organization
- Always hover over links in suspicious emails before clicking to see if the URL matches the sender's supposed organization
- Never click on text links from unknown senders
- Don't open attachments you're not expecting
- Use strong passwords and never use the same password for multiple accounts
- Never give personal information over the phone without verification; hang up and call the organization directly
- Never stay on a fraudulent call long—the criminal could record your voice for authorization

Cybersecurity Training is Your Greatest Gift

Social engineering and phishing have caused 70-90% of all data breaches. Cybersecurity training for your staff is a critical brick in your proverbial firewall. Even if you've conducted cybersecurity training in the past, refresher sessions keep security at the forefront of employees' minds—especially around the holidays when staff can get distracted with the bustle and excitement of the season. Educate your staff before the phishers cast their lures.

To learn more about fortifying your cybersecurity with employee awareness training, visit CompliancePro Solutions.

Start Your Free Phishing Security Test

Not sure how susceptible your employees are? Find out what percentage of your employees are Phish-prone™ with a free phishing security test from our partners at Know. Plus, see how you stack up against your peers with the new phishing Industry Benchmarks!

Free Phishing Tool Information