TRAINING TIME AND HOLIDAY NO NO NO'S

December 2023| Issue 2023:9

IT'S ANNUAL CYBERSECURITY TRAINING TIME

An average organization gets hit by approximately 700 socially engineered attacks (such as phishing attacks) every year, according to iTBlueprint Solutions.

Instead of trying to bypass firewalls and breach security systems, hackers have discovered that it's easier to target employees. In fact, up to 90% of ALL cyber-attacks today are said to have a human component to them.

Thankfully thousands of state employees successfully complete annual cybersecurity training. At this writing, 71% of state network users have completed the mandatory training while 18% of K-12 employees have done the same.

This year's training consists of two modules. The first, **Make it a Habit - Report It,** is a three-minute read highlighting the Phish Alert Button. (PAB). The PAB provides a method for all of us to report suspicious emails or attachments.

The second module features **Kevin Mitnick, sometimes referred to as the world's most well-known hacker.** This module, featuring industry insiders will give you the valuable information that you need to identify and protect yourself and your organization from the techniques and tools that malevolent cyber actors use. You'll also get to see a demonstration of the inner workings of a cyberattack.

Everyone benefits from a cybersafety - educated workforce. Do your part to complete your training as soon as possible. The deadline is **January 5, 2024.**

Solomon Adote
Chief Security Officer

THE NAUGHTY LIST

The holiday season is a time of joy and celebration, but it's also a prime time for cybercriminals to take advantage of unsuspecting shoppers. In 2023, several major cyberscams have been identified that consumers should be aware of.

One of the most common scams involves lookalike shopping websites. These sites mimic legitimate online retailers, tricking consumers into providing their credit card information. Similarly, fake social media ads for popular holiday gifts are also prevalent. These ads often lead to fraudulent websites where consumers' personal and financial information is at risk.

Another widespread scam is the gift-giving pyramid scheme. These are often called Secret Sister or Secret Santa exchanges. The bottom line: Online gift exchanges are almost always a scam. If you want to be involved in one, find a local group or start an exchange with your friends, family, or coworkers.

Fraudulent charities and fundraising campaigns are also a significant concern. Scammers create fake charities or GoFundMe campaigns to trick generous individuals into sending money or sharing personal information. It's important to verify the legitimacy of a charity before making a donation.

Finally, spoofed delivery notification texts and emails have become increasingly common. These messages claim that a package has been delayed or that a fee needs to be paid before it can be delivered. In reality, these messages are attempts to steal personal information or money. Always verify such notifications with the delivery company directly to avoid falling victim to these scams. Stay vigilant and safe this holiday season!