Inspired eLearning December Newsletter

SOCIAL MEDIA BEST PRACTICES WHEN TRAVELING

Watch this video to find out what happens when you don't think before you post.

DOWNLOAD NOW

DECREASE PHISHING EMAIL CLICK RATES

This report examines the trends and findings from PhishProof's Global Reporting Statistics and provides a snapshot comparison of two anonymous companies.

DOWNLOAD NOW

2019 Holiday Scams

Tis' the season for giving. And taking. As more Christmas shopping is done online, scammers are coming up with clever ways to con you out of your hard-earned dollar. The days of worrying about the fraudulent cashier's check in the mail are long gone. With Black Friday and Cyber Monday on the horizon, scammers are deploying the latest tricks of their trade to catch you in the midst of a post-Thanksgiving food coma. Experts warn that now is the time to be most vigilant while taking advantage of those annual holiday deals.

What holiday scams should I watch out for this year?
It isn't just Boomers getting scammed out of their hard-earned dollars. According to the Federal Trade Commission, millennials are more likely to report being victims of financial scams. In fact, reports of fraud are [25% more likely](#) to come millennials than persons over 40. In the past two years alone, millennials have lost almost half-a-billion dollars to online scams. While you're in the midst of online shopping this year, it's important to protect your identity and your financial

information. Scammers will use your willingness to go to the ends of the earth to buy that special gift for a loved one against you.

Secret Sister

Secret Sister is a social media scam that has been going around for the last couple of years. Facebook users recruit "sisters" with the promise that they could receive up to 36 gifts. The catch is, they have to buy a $10 gift for a stranger on the internet. Users provide your name, address and email. Then recruit friends to join. If you think it sounds like a pyramid scheme you're right. Users don't know who they're buying gifts for or whether those internet strangers will even return the favor. In addition, giving personal information such as your home address could open you up to cybersecurity breaches.

Elaborate fake websites

Whenever you receive an email saying that your account has been compromised and requires immediate attention such as a password, BE. SKEPTICAL. Often, these emails will contain links to elaborate web pages that closely mimic major websites such as Apple, Amazon, Google, Banks or even social media sites. These websites are typically part of phishing scams. Phishing scams lure users to these fake websites that capture login information, account numbers, credit cards and more.

Call spoofing/ Robocalls

Robocalls are often scammers looking to find working numbers. If you answer the phone, they may ask to push a button to stop calls or reply yes. They will use these responses to make unauthorized charges on accounts.

However, during the holiday season, you may get calls from spoofed numbers asking you to donate to the local police or fire department. More often than not, these are scammers. It's recommended that you verify the name of the caller and the organization they are calling from. In addition, if you feel compelled to donate, send a check instead of giving your credit or debit card number.

"Car warranty" scams (mail or phone)

If you get a phone call or a letter in the mail saying that your extended car warranty is about to expire. Use caution. Car warranty scams attempt to trick consumers into buying useless vehicle service contracts. Often, these service contracts cost anywhere from $1,300 to nearly $2,900. A salesperson will convince a victim that the warranty provides bumper to bumper coverage, including engine troubles. However, any attempt to make use of the warranty is stonewalled and refunds for the purchase of the warranty are virtually impossible. Despite government efforts to crack down on car warranty scams, it remains alive and well.

Cheap products

Scammers will pretend to be legitimate online sellers, with either a fake website or fake ad for a genuine retailer. The sites will offer luxury, name brand items such as clothing, jewelry or electronics at very low prices. Sometimes, you will receive the item you paid for, but as a very cheap knock off or you will receive nothing at all. While many people believe Amazon to be safe to make purchases, there are third party vendors on the site that sell homemade or cheap products. It's important to scrutinize everything.

Many of us believe that we can't be duped. However, making this errant assumption is what online thieves depend on. By following common-sense tips, you can prevent your personal data from being compromised online.

This article was written by The Carlson Law Firm and can be found in its entirety here.

How to Motivate Employees to Take Training

Security awareness training helps educate organizations and prepare its people to defend against today's most threatening cyberattacks. However, most people tend to forget the majority of infrequent or insufficient training. With that the case, how can security and risk management pros ensure their security awareness program sticks?

According to John Trest, Chief Learning Officer at Inspired eLearning, motivation, retention, and support are the crucial components of every successful security awareness training program. This blog will focus on part one of creating a comprehensive security awareness program: Motivation.

Employees don't want to take mandatory training courses. In order to keep adults interested and learning you must motivate them internally and externally, making them feel compelled to engage with the material.

The first key to doing this is to ensure your trainings have a high level of production quality. Inspired eLearning's training leverages cinematic videos, game-based simulations, virtual reality, and content with real-life scenarios that engage the learner and motivate them to pay attention.

Another key to motivating adults is to make sure they see value in the training material. They need to know what they can take away from it that furthers their interests or helps them. In the case of cybersecurity, they need to know how the learning will help protect them, their job, and their families.

In addition to value, adults need to relate training material back to what they know or have experienced. It's important that they see imagery relevant to their day-to-day lives. If it's not relevant to them, it can come across as a waste of their time.
Recognition is another important piece of motivation. Encourage learners to pay attention and participate in the training. Simply giving learners recognition for completing training early, modeling good cyber hygiene, or not falling for phishing simulations can make a big difference in adoption.

Inspired eLearning's award-winning security awareness education programs adapt to each learning style ensuring that your employees are engaged, learning, and retaining cyber-security best practices.

Our courses are created by a team of instructional designers that have more than 60 years of combined elearning experience, and our experts use the ADDIE model paired with cinematic creation styles to create courses that appeal to adult learning processes, making our security awareness programs the most engaging and effective in the industry.

Read the full version of this blog here

2020 Threats on the Horizon

While we cannot predict the future, we can see threats that are trending into 2020. Phishing, mobile malware, and IoT will be mainstays for the foreseeable future. We will also see some new twists on some old exploits. Read on to learn more.

Phishing is Here to Stay
In 2020 we will see a rise in SMS scams (SMiShing) and manipulation of messaging on social media and gaming platforms. Attackers will try to influence political views, incite dissonance, or trick users into giving up personal information, login credentials, or money. Tips to keep top of mind: Always verify the sender, practice a no trust policy, and do not befriend online folks whom you do not know personally.

Threats without Borders
We already witnessed weaponized social media attempts by the Russian government using AI-driven bots to bombard Facebook and Twitter with political propaganda trying to sway our US voters back in 2016. We can expect to see even more overseas political adversary groups creating and spreading false stories to undermine support for their opponents in the US 2020 elections. These borderless attacks will also extend to the 2020 Olympics. BoozAllenHamilton's top intel analysts predict that nation-states will be poised to interfere in the 2020 Olympics. So, watch out for the cyber gymnastics that will be no doubt be scattered throughout your social media feeds.

Bottom line: Check your sources and don't believe everything you read on social media platforms.

Craftier Mobile Malware on the Rise
Cyber criminals are churning out mobile banking malware as their top selling app on the dark web. These banking malware strains can steal payment data, credentials and funds from victims' bank accounts, and make fraudulent purchases with victims' credit card information. Fake apps or malicious links with this malware pre-embedded will proliferate every cyber landscape. Be wary of clicking on links that show up in text messages social media feeds, advertisement popups, email, and gaming platforms. Download apps from trusted sources only. Check the app reviews for anything suspicious like "too many ads," "runs the battery down," and "always freezes up my app or device."

Convenience vs Risk: The IoT dilemma
It can be very easy for cyber criminals to gain access to our networks through weak IoT devices. With one attack, they can burn your house down by gaining control of your smart oven. With the same attack multiplied throughout your whole neighborhood of smart appliances, they can cause a mass fire or shut down the power grid by overloading the systems. That's just one scenario. In 2020, we will see IoT attacks escalating in the industrial sector and affecting the masses.

For the consumer: Take advantage of technological conveniences but weigh the risks first. If possible, segregate your IoT network from your everyday use Wi-Fi network so that your computer and mobile devices are not sharing the same network as your smart home gadgets.

Passwords Galore
"By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion" (Symantec). While we wait for Single-Sign-On (SSO) and token-based authentication to gain traction, it will be wise to invest in a good secure password manager tool—one that encrypts your data. Popular ones today are LastPass, Dashlane, and 1Password.
We can't stress enough: DON'T REUSE Passwords!!! That means, once you've changed the password, forget it forever. People will recycle their passwords and resurrect ones from years back. Attackers have caught on to your bad habits, and they are retrying passwords that were cracked from a couple years ago.

The full version of this blog can be found here.

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:

info@inspiredelearning.com I 800.631.2078
4630 N Loop 1604 W, Suite 401
San Antonio, TX 78249 USA

Privacy Notice