Inspired eLearning September Newsletter

Welcome to the new and improved Inspired eLearning Monthly Newsletter! In addition to providing you updates regarding the cybersecurity industry, we will now also provide compliance industry updates and new resources from Inspired eLearning's resource center.

Please feel free to respond to this email address with feedback or questions regarding this updated format.

Thank you!
Inspired eLearning Marketing Team

SECURITY AWARENESS BEST PRACTICES PPT

With security threats evolving every day, it's important to not only train your employees on thwarting cyber attacks but also to convey the importance of security awareness training. This 35-slide PowerPoint presentation provides an overview of security awareness training best practices.

DOWNLOAD NOW

HARASSMENT PREVENTION POSTERS

It's important for employees to have reminders of what conduct is and is not appropriate in the workplace. Build a respectful workplace with this poster series covering harassment prevention techniques in the workplace. Download all five harassment prevention posters today!

DOWNLOAD NOW

Cybercriminals Impersonate CEO's Voice to Steal $243,000

Cybercriminals are always looking for new ways to trick their victims. Recently, attackers used AI and voice recording to steal $243,000 from a UK based organization.

The incident occurred when the CEO of the UK based energy company received a phone call from who he thought was his boss, the chief executive officer of his organization's German parent company. The individual on the phone requested that the CEO send $243,000 to a Hungarian supplier in an "urgent" request.

According to Threatpost, the victim, deceived into thinking that the voice was that of his boss – particularly because it had a similar slight German accent and voice pattern – made the transfer. However, when the scammers continued to call back, making additional requests, the CEO grew suspicious and contacted the authorities.

While this incident is still under investigation, the Wall Street Journal cites officials saying this impersonation attack is the first in which fraudsters "clearly" leveraged AI to mimic someone's voice. It's believed this technology could make it easier for scammers to manipulate enterprise victims, complicating matters for defenders who don't yet have the technology to detect them.

October 9th Deadline Approaches for New York Employers

All employers in the state of New York must provide harassment prevention training for all employees by October 9th, 2019. This deadline comes after a nine-month extension from an original deadline of January 1st.

In addition to providing mandatory training by October 9th, employees must continue to provide harassment prevention training to all employees each year. All companies that bid on contracts with the New York State government must submit an affirmation that they have a sexual harassment policy and have provided sexual harassment training to all employees, even those not located in New York State. California, Connecticut, Delaware, Illinois, and Maine are other states that have recently passed legislation requiring harassment prevention training. Specifically, the New York State law:

- Applies to all employers, regardless of their size, who employ anyone in the state of New York.
- Applies to all contractors who bid on New York State contracts.
- Applies to all employees, not just supervisors. (California, Connecticut, Delaware, and Maine also require training for all employees.)
- Requires that the training is provided annually.

Find more information regarding harassment prevention courses by clicking here.

How Twitter's CEO Was Hacked

An anonymous hacker recently took over Twitter CEO, Jack Dorsey's account for 20 minutes and retweeted various threatening and anti-Semitic posts.

According to Wired, the hijacking of Dorsey's account started around 3:45 pm Eastern time, when the @jack account fired off nearly two dozen tweets and retweets. Several of the tweets were tagged #ChucklingSquad, the name of an apparent group of hackers who have been on an account-takeover spree this week. In addition to Dorsey, influencers such as Zane Hijazi of the podcast Zane and Heath and YouTuber Anthony Brown.

Some of the influencers affected have blamed so-called SIM swap attacks. In a SIM swap, a hacker either convinces or bribes a carrier employee to switch the number associated with a SIM card to another device, at which point they can intercept any two-factor authentication codes sent by text message. Twitter confirmed that it was a SIM issue in a tweet posted on August 30th.

For more information on social media safety best practices click 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