2024 IOT Cybersecurity Awareness Training Calendar

Modules are launched the first Tuesday of the month (State Holiday's may impact this) and are due 21 days from assignment date. This schedule is tentative. Emerging threats or the release of a module better able to build resiliency in the workforce may result in a change.

Indiana Office of Technology
Powering a State that Works

Launch Date	Title	Module Description
Quarter 1		
Wednesday January 3rd	**2024 Social Engineering Red Flags (13 minutes)**	Social engineering is one of the main ways cybercriminals get people to take actions that go against their or their organization's best interests. To stay safe online and protect yourself and your organization, it is vital that you don't fall for these tricks. In this module, you will learn how to spot the red flags or signs of danger associated with common social engineering methods as well as choose the safest course of action when facing a cyberthreat.
Tuesday February 6th	**Cybersecurity Onboarding 2024 (15 minutes)**	Cybercriminals are indiscriminate in their pursuit of targets, and with this training, you'll gain insights into the tools and tactics they use, learn to recognize the warning signs of cyberattacks and understand the best actions to take when faced with such situations and learn how to strengthen your defense against potential threats and ensure a safer digital environment for you and your organization. You'll also get to see the inner workings of a cyberattack with a demonstration from legendary security consultant Kevin Mitnick. **After the February launch this assignment will be ongoing to pull in New Hires as a training requirement.**
Tuesday March 12th	**The Inside Man: Season 1 Ep 01 - The New Guy (Social Engineering) (8 minutes)**	The Khromacom IT team frantically attempts to deal with a cyber-attack when, seemingly out of nowhere, an unexpected job applicant steps in to save the day. Mark Shepard stops the attack, impressing IT Manager Ed, who offers him a temporary contract to join the security department. But who was the source of the attack ... and does this mean they can access all of the company's systems? It turns out Mark may not be exactly what he seems … This video module teaches users about tailgating and enforces the importance of physical security.
Quarter 2		
Tuesday April 2nd	**Criminal Minds: Business Email Compromise (5 minutes)**	Through phishing scams cybercriminals can gain access to an email system. They then monitor emails and can intercept an invoice requiring payment - this can cost an organization or individuals. Find out more about email compromise and how to protect yourself and your organization. Criminals apply the same tactics to organizations - also known as business email compromise or BEC.
Wednesday May 8th	**QR Codes: Safe Scanning (4 minutes)**	QR codes continue to be more common in our daily lives as quick, convenient ways of accessing websites without typing in long web addresses. They also offer a way to complete contact-free transactions without handing over cards or cash. However, their widespread applications and ease of use give cybercriminals another method of carrying out their attacks. This module discusses the threats associated with scanning QR codes, along with security tips to help you scan them safely.
Tuesday June 4th	**The Inside Man: Season 1 Ep 02 - Social Hour (Social Media) (7 minutes)**	Mark begins his new job at Khromacom, receiving his badge and meeting his new co-workers. Ed assigns Mark the task of finding out how the media got wind of the merger talks the company is involved in, but Mark already knows the source of the stories. Someone's been a little loose lipped with their social media updates...This module warns of the dangers when sensitive information is shared on social media. This module warns of the dangers when sensitive information is shared on social media.

2024 IOT Cybersecurity Awareness Training Calendar

Modules are launched the first Tuesday of the month (State Holiday's may impact this) and are due 21 days from assignment date. This schedule is tentative. Emerging threats or the release of a module better able to build resiliency in the workforce may result in a change.

Indiana Office of Technology
Powering a State that Works

Launch Date	Title	Module Description
Quarter 3		
Tuesday July 2nd	**Generative AI: Intelligent and Dangerous? (12 minutes)**	Software that can write about any subject independently, solve math problems or write program code — this is possible because of generative artificial intelligence (AI). DALL-E, Bard or ChatGPT are all prominent examples. Generative AI gives us countless opportunities. Unfortunately, this applies to cybercriminals too. The training module "Generative AI: Intelligent and Dangerous?" explains the basics, shows how cybercriminals are using the technology for their own goals, and how employees can protect themselves against new threats. The training consists of three short videos, in which Dr. Swantje Westpfahl, cybersecurity expert and director of the Institute for Security and Safety at Mannheim University of Applied Sciences, answers the most important questions. Additional interactive slides and knowledge checks use graphics and checklists to summarize key concepts and tips. Learners will take a short quiz at the end.
Tuesday August 6th	**Mobile Phishing (5 minutes)**	While phishing attacks have traditionally been associated with emails, the rise in mobile devices has changed that forever. This short course explores that idea, focusing on how cybercriminals target phones and tablets and what every individual needs to do to protect devices, data, and people.
Wednesday September 4th	**The Inside Man: Season 1 Ep 03 - On Our Side (Phishing Attacks) (7 minutes)**	Mark's search for information about the merger brings him to the finance department where Erica stops him in his tracks. Mark decides to try a different tactic, targeting her with a phishing email. But when AJ, who has aspirations of joining the security department himself, sees what he's up to, Mark must pretend it was a phishing test for the whole office. Will anyone spot the red flags? Teach your users how to protect your network by identifying social engineering red flags and avoiding clicking on links and downloading suspicious attachments in emails.
Quarter 4		
Tuesday October 1st	**A Guide to Avoiding Password Reuse (6 minutes)**	The reuse of weak passwords is estimated to cause 19% of data breaches. This is why it is so important that people don't reuse passwords. In this module, you will learn why reusing passwords is dangerous and how to change reused passwords to stronger, more complex ones.
Wednesday November 6th	**Criminal Minds: Spear Phishing (5 minutes)**	Social media is where cybercriminals get information to craft their scams. The more details they can get, the more tailored and believable it is. This is called spear phishing. Avoid oversharing, and never use your work credentials for personal purposes. If your account access is compromised, it is an easy way for cybercriminals to get inside your organization.
Tuesday December 3rd	**The Inside Man: Season 1 Ep 04 - Surprise (Document Disposal) (6 minutes)**	After his phishing email fails to reveal all the information the mysterious "handler" is looking for, Mark turns from the digital realm to the physical, and enlists the help of an expert dumpster diver to see what surprises the company's trash holds. Meanwhile, Mark's colleagues throw him a surprise party--an experience completely new to Mark... In this module you will learn how to securely dispose of documents containing sensitive data.