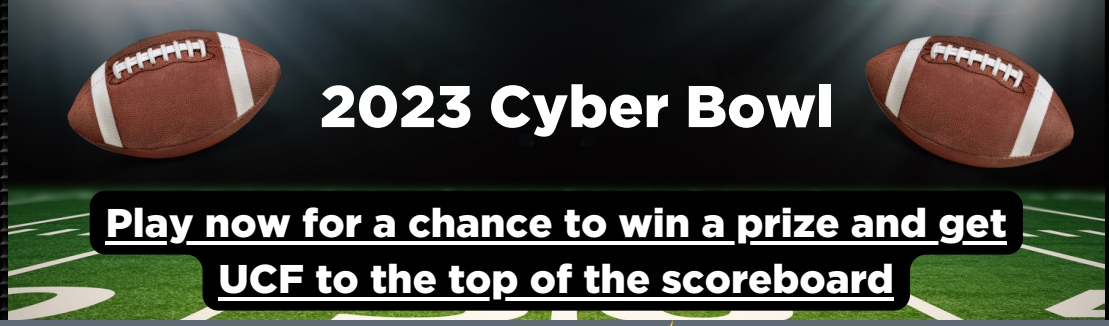
University of Central Florida

INFOSEC

Security Awareness Newsletter



Issue 10 | October 10, 2023

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in October 2023

1. MGM Resorts Hit: Cyberattack Inflicts $100 Million Blow

NBCnews.com

The company said it deliberately shut down a number of services "to mitigate risk to customer information" after the hack last month.

2. NSA Unveils AI Security Center: Fortifying National Defense

InfoSecurity-Magazine.com

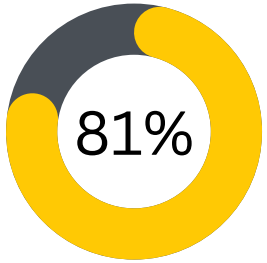
The National Security Agency (NSA) has unveiled the AI Security Center, a new entity dedicated to overseeing the development and integration of artificial intelligence (AI) capabilities within US national security systems.

3. FDA Tightens Cybersecurity for Medical Devices, Empowering Vigilance

CyberScoop.com

New regulations that went into effect on Sunday aim to make it more difficult to hack into medical devices by requiring vendors to beef up the security features of things like pacemakers and insulin pumps before they make it onto the market.

DID YOU KNOW?

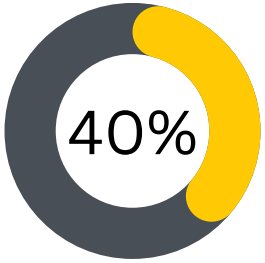


of leaders make API security top priority

Confidence in respondents' ability to tackle such incidents has shot up from 67% to 94% saying they are confident that their current application testing tools are capable of testing APIs for vulnerabilities in 2023, Click to read more.

72% increase in ransomware double-extortion attacks

Malware and network security trends were analyzed in a recent report by WatchGuard highlighting the increase in ransomware double-extortion attacks, double-extortion attacks, Click to read more.



of U.S. security leaders cite malware as threat focus

Companies are capturing far more data, creating new privacy implications for customers and operational risk for their internal workflows, Click to read more.

October Security Article

Empowering IT and InfoSec Teams During Cybersecurity Awareness Month

As we step into October, it's not just about falling leaves and pumpkin spice lattes. It's also the month we collectively sharpen our digital swords because October is Cybersecurity Awareness Month. For all of us in IT and InfoSec, this is our time to shine by showcasing and applying our knowledge of cybersecurity best practices.

1. Passwords are Your Digital Shields: Let's start with the basics, passwords. Think of them as the moat around your castle. This month, commit to fortifying them. Use passphrases, update them regularly and never share them with others.

2. Phishing, the Sneaky Enemy: Phishing is the ninja of the cyber world. It's stealthy, and it could get you when you least expect it. Be skeptical of unexpected emails or messages. If something seems off, report it to SIRT.

3. Keep Your Software Castle Walls Tall: Outdated software is like a breached wall in your fortress. Keep your systems updated; it's not just a suggestion, it's your duty. Set up those automatic updates, so you don't have to worry about the latest vulnerabilities.

4. USB Drives, The Trojan Horses: USB drives may seem innocent, but they can carry hidden dangers. Don't plug in random USB drives. If you find one lying around, resist the temptation to see what's on it. It could be a cyber Trojan horse.

5. Report, Report, Report: See something suspicious? Hear an unusual request? Don't be a lone warrior; report it. You might just save your digital kingdom from an impending attack.

6. Educate Your Fellow Knights: Knowledge is power. Share your cybersecurity wisdom with your colleagues. Conduct a mini-training session, share tips in the breakroom and be the cybersecurity knight the office needs.

This Cybersecurity Awareness Month, let's not be the weak links. Let's be the digital guardians our organization deserves. Update, educate and elevate our collective cybersecurity defenses. We've got this!

In Other (Security) News...

RICO Lawsuit: H&R Block, Google, Meta Accused in Data Privacy Case

A trial lawyer filed suit against H&R Block on Wednesday, alleging the firm collaborated with Meta and Google to embed "spyware" on its website to make money from scraped tax return data., Click to read more.

Signal Boosts Security: Quantum-Resistant Encryption in E2EE

Signal has announced that it upgraded its end-to-end communication protocol to use quantum-resistant encryption keys to protect users from future attacks, Click to read more.

Microsoft AI Blunder: Terabytes of Sensitive Data Exposed

Microsoft AI researchers accidentally exposed tens of terabytes of sensitive data, including private keys and passwords, while publishing a storage bucket of open-source training data on GitHub, Click to read more.

Security Alerts

Critical Privilege Escalation Flaw in Windows CNG Service

Click to read more.

Apple iOS and iPadOS at Risk: Kernel Privilege Escalation

Click to read more.