University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 5 May 9, 2023

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in May 2023

1. The DOJ Detected the SolarWinds Hack 6 months Earlier than First Disclosed
Wired.com

The breach, publicly announced in December 2020, involved Russian hackers compromising the software maker SolarWinds and inserting a backdoor into software served to about 18,000 of its customers.

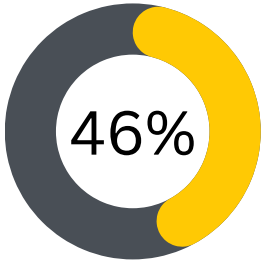
2. Malware-Free Cyberattacks on the Rise
DarkReading.com

According to CrowdStrike CEO George Kurtz and president Michael Sentonas, 71% of enterprise cyberattacks in calendar year 2022 were done without malware.

3. Google's New Two-Factor Authentication Isn't End-to-End Encrypted, Tests Show
Gizmodo.com

An examination by security researchers finds an alarming flaw in the search giant's new feature, which syncs your Authenticator app across devices.

DID YOU KNOW?

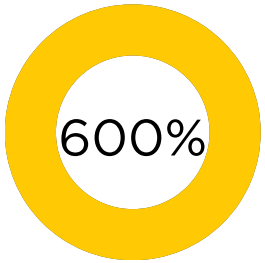


46 percent of organizations faced synthetic identity fraud in 2022

New artificial intelligence (AI) technologies have raised a number of security concerns, Click to read more.

65% of cyberattacks targetted at the U.S., report shows

A new report reveals an increase in cyberattacks directed at financial institutions, food retailers and healthcare providers, with 60% of all attacks targeting these three key industries, Click to read more.



Report shows nearly 600 percent annual growth in vulnerable cloud attack surface

Click to read more.

Around Campus Update

Reducing Phishing Attacks

Phishing attacks are a constant threat, and we need to ensure that everyone in our organization understands how to recognize and avoid them.

The UCF Information Security Office is always looking for effective ways to increase security awareness among the UCF Community. That's why we utilize the KnowBe4 platform, a provider of security awareness training and phishing simulation services.

KnowBe4's phishing simulation platform allows us to create realistic phishing campaigns that mimic real-world attacks. By sending these simulated phishing emails to our faculty, staff and students, we can track who falls for the scam and who reports it. The results help us identify areas where additional security training is needed, so we can target our efforts more effectively.

While it may seem counterintuitive to conduct phishing campaigns against our own employees, the reality is that these simulations are an extremely effective way to increase security awareness and identify vulnerabilities that could be exploited by real attackers. By utilizing a platform like KnowBe4, we have been able to establish a culture of security awareness at UCF, where employees are more vigilant and less likely to fall for phishing scams.

Over the past 12 months through education initiatives, we have been able to reduce our phish-prone score from 7.7 percent to just over 4 percent, sending over 12,000 simulated emails each month to faculty and staff. While 4 percent of 12,000 is still a large number, we are consistently below the industry average of 6.5% percent.

Overall, the use of phishing simulations has helped us to better protect ourselves against phishing attacks and other forms of cyber-attacks. It's just one of many tools and resources available to us, but it has proven to be a particularly powerful one that has had a positive impact at UCF.

In Other (Security) News...

Microsoft Edge is Leaking User Browsing Data to Bing

It's probably a good idea to disable Edge's follow creator feature until this privacy issue is fixed, Click to read more.

Trigona Ransomware Targets Microsoft SQL Servers

Threat actors are hacking into poorly secured and public-facing Microsoft SQL servers to deploy Trigona ransomware, Click to read more.

Google Gets Court Order to Take Down CryptBot That Infected Over 670,000 Computers

Google said it obtained a temporary court order in the U.S. to disrupt the distribution of a Windows-based information-stealing malware called CryptBot and "decelerate" its growth, Click to read more.

Security Alerts

Apache Log4j2 Deserialization of Untrusted Data Vulnerability

Click to read more.

Oracle WebLogic Server Unspecified Vulnerability

Click to read more.