University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 1 ⚡ January 9, 2024

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

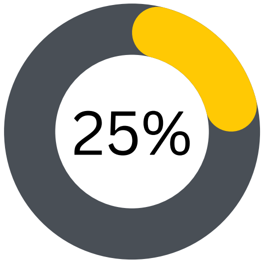
Top 3: Security News in January 2024

1. **Comcast Says Data of 36 Million Accounts Was Compromised in Breach**
WSJ.com
Accounts were compromised after hackers gained access to Comcast's systems through a vulnerability in Citrix cloud computing software.

2. **Google Settles $5 Billion Privacy Lawsuit Over Tracking Users in 'Incognito Mode'**
TheHackerNews.com
Google settled a lawsuit accusing it of misleading users about private internet browsing in "incognito" mode.

3. **Cybercriminals using fewer than 1% of thousands of potential exploits**
CyberNews.com
Over 26,000 vulnerabilities were reported in 2023, with cybercriminals exploiting less than 1% and nearly half were unknown to defenders, according to a Qualys report.

DID YOU KNOW?



Using Stronger Passwords Among Top 2024 Digital Resolutions

Almost a quarter of people mentioned cybersecurity among their New Year's digital resolutions for 2024.
Click to read more.

An innocent-looking Instagram trend could be a gift to hackers

People spent the last few days of 2023 encouraging their followers to get to know them better.
Click to read more.

New data reveals the states at highest risk of cybercrime

Analyzing FBI Internet Crime Reports from 2018-2022, the U.S. states most vulnerable to cyberattacks have been revealed.
Click to read more.

January Security Article

Mobile Cybersecurity Trends in 2024

In the ever-evolving digital landscape of the University of Central Florida (UCF), securing mobile devices against cyber threats remains a top priority. As smartphones and tablets become integral to academic and administrative activities, UCF faces a pressing need to fortify its mobile cybersecurity measures. Here are key areas of focus for enhancing mobile security in 2024.

- Continuous Authentication: Ongoing user verification through multifactor authentication and behavior analysis.
- Hacking Detection: Real-time monitoring and machine learning to detect sophisticated hacking attempts.
- Mobile Banking Security: Encryption, biometrics, and transaction monitoring for fortified app security.
- Zero Trust Approach: Strict access controls and continuous verification to prevent unauthorized access.
- Wireless Data Security: Ensuring encrypted wireless data exchange channels.
- AI-Powered Security: Utilizing AI for anomaly detection and swift threat response.

As we navigate the digital frontiers of 2024, safeguarding the university's mobile ecosystem stands as an imperative. This proactive approach is not just a shield; it's an assertion of UCF's commitment to an uninterrupted, secure academic pursuit. By fostering a cybersecurity-aware culture among students and faculty, we can confidently navigate the mobile cybersecurity landscape in 2024 and beyond, ensuring a secure academic environment.

In Other (Security) News...

Top ten biggest security incidents of 2023

Threat actors have thrived in this year's environment of ongoing cyberwars and economic and geopolitical uncertainty, committing all their tools and ingenuity. Let's look at the ten high-profile cybersecurity incidents that scarred 2023 the most, chosen by ESET researchers.
Click to read more.

Top 10 Cybersecurity Predictions for 2024 and Beyond

Despite cybersecurity's unpredictability and constant evolution, a diverse panel of experts offered their top ten predictions on future cybersecurity trends, aiming to equip defenders with foresight and preparedness.
Click to read more.

Cyber-Attacks Drain $1.84bn from Web3 in 2023

In 2023, cyber-attacks on Web3 resulted in $1.84 billion in losses across 751 incidents, with a significant decline from 2022 and private key compromises causing the most damage, according to Certik's report.
Click to read more.

Security Alerts

Log4j Vulnerability Enables Arbitrary Code Execution

Click to read more.

OpenSSH, Key Networking Tool, Vulnerable to Exploit

Click to read more.