University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 3 | March 12, 2024

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in March 2024

1. Cyberattack Paralyzes the Largest U.S. Health Care Payment System

NYTimes.com

The hacking shut down the nation's biggest health care payment system, causing financial chaos that affected a broad spectrum ranging from large hospitals to single-doctor practices.

2. Lockbit Cybercrime Gang Disrupted by Britain, US and EU

USNews.com

The operation was run by Britain's National Crime Agency, the U.S. Federal Bureau of Investigation, Europol and a coalition of international police agencies, according to a post on the gang's extortion website.

3. Apple Rolls Out Quantum-Resistant Cryptography for iMessage

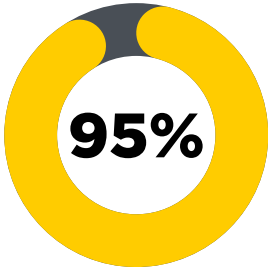
CyberScoop.com

The tech giant hopes to make its messaging platform secure against highly capable quantum computers of the future.

DID YOU KNOW?

Ransomware Extortion is Evolving

The ransomware extortion landscape is evolving with threat actors adopting new methods to blackmail and threaten their victims. Click to read more.



95% of Websites Run on Outdated Software with Known Vulnerabilities

it seems that the common-sense practice of keeping software up to date is not that common, according to a new study conducted by a group of researchers. Click to read more.

Ads for Zero-Day Exploit Sales Surge 70% Annually

Security researchers have warned that threat actors are increasingly turning to zero-day exploits to increase the success rate of advanced targeted attacks. Click to read more.

March Security Article

Guarding Against Social Engineering Threats During National Fraud Awareness Month

As March unfolds, we embrace National Fraud Awareness Month—a timely opportunity to fortify our defenses against the ever-evolving landscape of cyber threats. This month, our focus zeroes in on Social Engineering, a pervasive and sophisticated tactic employed by cybercriminals to exploit human psychology and gain unauthorized access to sensitive information. We must equip ourselves with knowledge and vigilance to stay one step ahead of these deceptive practices:

1. Phishing: Phishing emails remain a primary weapon in a cybercriminal's arsenal. Be wary of unsolicited emails, especially those urging you to click on suspicious links or divulge personal information. Always verify the sender's legitimacy before taking any action.
2. Smishing: With the rise of mobile technology, cybercriminals have adapted their tactics. Be cautious of unexpected text messages containing links or requests for sensitive information. Always confirm the legitimacy of the sender before responding.
3. Whaling: Whaling attacks target high-profile individuals within an organization, such as executives or key decision-makers. Stay alert for personalized and convincing messages that may attempt to manipulate you into divulging sensitive information or initiating unauthorized transactions.
4. Baiting: Cybercriminals may leave infected USB drives, CDs, or other media in public spaces, relying on curiosity to prompt individuals to plug them into their devices. Avoid using unfamiliar storage devices and report any found items.
5. Tailgating/Piggybacking: Physical security is just as crucial as digital security. Be mindful of unauthorized individuals attempting to gain entry by following closely behind someone with legitimate access. Always question unfamiliar faces in secure areas.

Let's commit to fortifying our defenses, empowering ourselves with knowledge, and fostering a community that stands resilient against the deceptive tactics of cybercriminals. Stay vigilant, stay secure!

In Other (Security) News...

U.S. State Government Network Breached via Former Employee's Account

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has revealed that an unnamed state government organization's network environment was compromised via an administrator account belonging to a former employee.
Click to read more.

Is Now the Right Time for a Ransomware Payment Ban?

Experts have long debated a nationwide ban on paying cyber extortionists. But any ban must be paired with measures to help targets improve defenses, cybersecurity experts say.
Click to read more.

How GenAI and Custom GPTs Could Impact Government in 2024

New generative AI tools are poised to make an even bigger impact in state and local government in the year ahead. Jurisdictions need to understand their potential uses and how they will impact resident services.
Click to read more.

Security Alerts

Out-of-Bounds Memory Access and Arbitrary Code Execution Risk on Apple Devices

Click to read more.

Google Warns: Critical Vulnerability Poses Local Privilege Escalation Risk

Click to read more.