University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 9 | September 10, 2024

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News September S202t4

1. CISA Releases Election Security Focused Checklists for Both Cybersecurity and Physical Security

CISA.gov

The Cybersecurity and Infrastructure Security Agency (CISA) has introduced two checklists designed to help election officials assess and strengthen both physical and cybersecurity measures ahead of Election Day, addressing common vulnerabilities and short-term resilience options.

2. Hackers Leak 2.7 Billion Data Records With SSNs

BleepingComputer.com

. The breach exposes sensitive details like social security numbers, names and addresses, raising concerns about identity theft and privacy risks.

3. Critical infrastructure Cyberattacks 'A Geopolitical Weapon' Says New Report

StateScoop.com

A recent report identifies cyberattacks on critical infrastructure as a rising geopolitical tool, highlighting the risks to national security and the increasing complexity of these threats.

DID YOU KNOW?

DDoS Attacks Double With Governments Most Targeted

DDoS attacks have surged, doubling in frequency with government entities as primary targets, indicating escalating cyber threats against public infrastructure. Click to read more.

Active Ransomware Groups Surge by 56% in 2024

A report reveals a 56% rise in active ransomware groups in early 2024, underscoring growing threats and challenges in the cybersecurity landscape. Click to read more.

There was a 56% increase in ransomware groups in H1 2024

The first half of 2024 saw a significant 56% increase in ransomware groups, with heightened activity from emerging and smaller groups. Click to read more.

September Security Article

National Insider Threat Awareness Month: Stay Vigilant as We Move Forward This School Year

With the new academic year in full swing, it's the perfect time to refocus on cybersecurity as part of National Insider Threat Awareness Month. Whether you're a student, faculty member, or staff, everyone plays a role in safeguarding our institution from insider threats—intentional or accidental. Here's how you can help:

Stay Vigilant - Just as you're keeping up with assignments, stay alert to unusual activity around you—whether it's in physical spaces or digital systems. A small oversight can lead to big security issues, so be proactive in spotting anything out of the ordinary.

Secure Your Access - Much like keeping your dorm room locked, safeguard your digital access. Use strong, unique passwords and enable multi-factor authentication (MFA) to prevent unauthorized access to university systems. Never share your login details with others.

Report Quickly - If you notice any suspicious behavior, such as unusual requests for access or misplaced sensitive information, report it immediately. Quick action can prevent potential security breaches.

Mind Your Workspace - Whether you're studying in the library or working remotely, keep sensitive documents secure, both digitally and physically. Always log off or lock your device when stepping away.

Stay Informed - Cyber threats are always evolving. Stay updated by attending university cybersecurity trainings, and keep an eye on communications about new security policies.

Watch for Phishing - Phishing attempts are like surprise tests. Be cautious of emails or messages asking for personal or financial information. Verify the sender before clicking any links or attachments.

Practice Good Habits - Just like developing good study habits, adopting cybersecurity best practices—such as regular system updates and proper data handling—helps protect against insider threats.

Together, we can make this academic year not just productive, but also safe and secure. Stay aware, stay informed, and help keep our university community protected.

In Other (Security) News...

A new malware named "Voldemort" may be a cyber espionage campaign

The malware, possibly linked to a cyber espionage effort, uses unconventional methods like Google Sheets for command and control, complicating detection for affected sectors, including insurance and aerospace.

Click to read more.

YubiKeys are vulnerable to cloning attacks thanks to newly discovered side channel

A side-channel vulnerability exposes YubiKeys to potential cloning attacks, raising concerns over hardware-based security.

Click to read more.

White House launches cybersecurity hiring sprint to help fill 500,000 job openings

This initiative seeks to address a shortage of 500,000 cybersecurity roles to strengthen national resilience.

Click to read more.

Security Alerts

Google Chrome Vulnerability Before Version 128.0.6613.84 Allows Remote Attackers to Exploit Heap Corruption with Malicious HTML

Click to read more.

Microsoft Windows SmartScreen Vulnerability Lets Attackers Bypass Security with Malicious Files

Click to read more.