University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 8 | August 13, 2024

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in August 2024

1. CrowdStrike—How Microsoft Will Protect 8.5 Million Windows Machines

Forbes.com

As part of this, Microsoft has explained how kernel level access for products such as CrowdStrike is important and outlined how it will protect millions of Windows machines in the future.

2. How Infostealers Pillaged the World's Passwords

Wired.com

Infostealer malware is swiping millions of passwords, cookies, and search histories. It's a gold mine for hackers—and a disaster for anyone who becomes a target.

3. Facebook Ads Lead to Fake Websites Stealing Credit Card Information

TheHackerNews.com

Facebook users are the target of a scam e-commerce network that uses hundreds of fake websites to steal personal and financial data using brand impersonation and malvertising tricks.

DID YOU KNOW?

CVEs Surge 30% in 2024, Only 0.91% Weaponized

In the first half of 2024, the number of reported Common Vulnerabilities and Exposures (CVEs) has increased by 30% compared to last year, totaling 22,254.
Click to read more.

Email attacks rose by 293% compared to the first half of 2023

A report by Acronis found email attack instances were 293% greater in the first half of 2024 when compared to the first half of 2023.
Click to read more.

Gaming Industry Faces 94% Surge in DDoS Attacks

According to Akamai, the figures highlight the growing cybersecurity challenges in a sector with 2.58 billion players and a market valuation of $184.4b. Click to read more.

August Security Article

Olympic Cyber-Savvy: Your August 2024 Data Privacy Playbook

As you dive into the Olympic excitement, remember to safeguard your personal info. Use strong, unique passwords and enable two-factor authentication (2FA) to keep your accounts secure. Think twice before sharing personal details on social media and ensure your privacy settings are tight. Focus on the games, not on data breaches!

Be a Privacy Pro: Mastering Your Settings
Olympic fever is high, and so is online activity. Now's the perfect time to review your privacy settings on social media, sports apps, and streaming services. Know who can see your posts, what data is being collected, and how it's used. Stay in control while cheering for your favorite athletes!

Gold Medal Security: Safeguarding Your Transactions
Buying Olympic gear or streaming subscriptions? Make sure your online transactions are secure. Always use trusted websites, look for the padlock symbol, and ensure the URL starts with "https://". Avoid public Wi-Fi for transactions and use a credit card for extra protection. Shop smart, cheer hard!

Don't Get Played: Phishing and Scam Prevention
Cybercriminals are also enjoying the Olympic rush, looking for ways to scam you. Be wary of phishing emails and scam messages posing as official Olympic communications. Check the sender's email address, avoid suspicious links and never share personal info unless you're sure it's legit. Stay sharp and don't let scammers ruin the fun!

Encrypt and Go: Using VPNs and Encryption Tools
Streaming live events or accessing sensitive info? Encrypt your data and use a VPN to stay secure. A VPN masks your IP address, making it tougher for hackers to track you. Encryption tools ensure your data is unreadable to unauthorized parties. Watch the games with peace of mind!

Cookie Crunch Time: Managing Cookies and Trackers
Websites love cookies, but they can compromise your privacy. As you follow Olympic content, regularly clear your browser's cookies and use extensions to block trackers. Adjust your browser's privacy settings to limit data collection. Enjoy the games without the trackers!

In Other (Security) News...

Researchers find new way to steal tokens using cross-site scripting and OAuth
Although cross-site scripting (XSS) attacks might have fallen out of prominence in recent years, researchers have demonstrated a new method that enables bad actors to steal user session tokens.
Click to read more.

Cyberattacks may follow CrowdStrike outage, warns MS-ISAC
After working long hours over the weekend to help their organizations recover from last week's CrowdStrike outage, many state and local government IT officials this week told StateScoop that the worst of the disruptions appear to be over. Click to read more.

Chrome now asking for ZIP archive passwords to help detect malicious files
Cybercriminals are increasingly using encrypted and password-protected files to deliver infostealers and other malware while slipping through security defenses.
Click to read more.

Security Alerts

A security flaw in Ivanti ICS versions 9.x and 22.x, lets a hacker bypass checks and access restricted parts of the system remotely.
Click to read more.

A logic error in Android's code could let someone gain higher access on the device without needing extra permissions. Click to read more.

Changes in the Information Security Office:
Research Cyber Risk Management

As federal regulations evolve to strengthen cybersecurity protections for sensitive data, UCF has integrated the information security professionals responsible for safeguarding this information into the Information Security Office.

In May, the Office of Cyber Risk Management (Office of Research) and personnel operating Knight Shield (at the Institute for Simulation & Training) joined the Information Security Office and formed Research Cyber Risk Management (RCRM). Tammie McClellan is leading RCRM as Deputy CISO. Tammie served as interim director for the Office of Cyber Risk Management since November 2021. Before that, she worked as a researcher, principal investigator, and IT program director at UCF's Institute for Simulation & Training.

Research Cyber Risk Management is responsible for establishing cyber risk strategies and implementing an effective cybersecurity compliance program for research. RCRM is involved with any research agreement that encompasses data protection requirements. A primary focus for RCRM is safeguarding sensitive federal unclassified information, known as Controlled Unclassified Information (CUI).

RCRM has two primary areas of focus:

- **Cyber Risk Management and Compliance**
  This includes conducting ancillary reviews for sponsored agreements, sponsor communications, project tracking, developing security plans, facilitating onboarding into Knight Shield, lab walk-throughs and assessments, training, and performing various monitoring activities.

- **Operating Knight Shield**
  Knight Shield is a separate computing environment and framework for faculty and staff who handle CUI. Knight Shield is securely configured to meet NIST SP 800-171 and federal regulations for CUI.

Please congratulate and welcome ISO's newest members: Tammie McClellan, Ed Moses, Angela Moten, Henry Glaspie, Mark Darty, Leith Tussing, Patrick Skelly, Christopher Upchurch, and Steven Valdez. For assistance, reach out to any team member or contact: ResearchCyberRisk@ucf.edu.

Knight Shield Moving to GCC-High

We have exciting news! A new Knight Shield environment has been established to support Controlled Unclassified Information (CUI) at UCF. Knight Shield now has its own domain (knightshield.ucf.edu) and will soon be disconnected from the IST-School of Modeling, Simulation & Training to support future growth. Faculty and staff with an active Knight Shield user account, workstation, virtual desktop, and any file shares will move to "Knight Shield 2.0" in October.

Informational sessions for affected personnel will be held every Thursday during September to review the migration schedule and the essential steps users will need to perform.

What's New in Knight Shield 2.0:

- ***Backed by Microsoft's Azure Government Community Cloud High Tenant (GCC-High):*** This platform offers tools that meet the highest compliance standards for CUI (e.g., ITAR).

- ***Microsoft 365 Integration:*** Knight Shield 2.0 will provide Microsoft 365 apps, including OneDrive, Teams, and Email (e.g., a Knight Shield email account), to help you communicate and collaborate more effectively with your sponsors and partners. Support for physical Knight Shield workstations will continue.

- ***Built for CMMC Certification:*** Knight Shield 2.0 has been developed from the ground up to position Knight Shield for CMMC certification. New procedures, forms, and tools will be implemented to help prepare UCF for certification!