University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 9 September 12, 2023

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in September 2023

1. **Chinese Hackers Breach Japan's Cyber Agency, Prompting Cybersecurity Boost**
   [ft.com]

   Japan's cyber security agency suffers months-long breach.

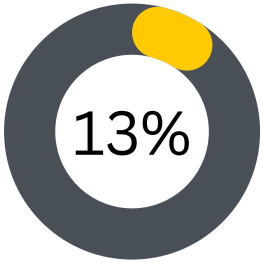
2. **Univ. of Michigan Halts Internet After Cyberattack: Classes Unaffected**
   [TheRecord.media]

   The university on Sunday "made the intentional decision to sever our ties to the internet" after "careful evaluation of a significant security concern."

3. **US Govt Email Services Hacked via Barracuda Zero-Day**
   [BleepingComputer.com]

   Suspected Chinese hackers disproportionately targeted and breached government and government-linked organizations worldwide in recent attacks targeting a Barracuda Email Security Gateway (ESG) zero-day, with a focus on entities across the Americas.

DID YOU KNOW?

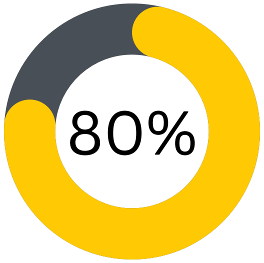


of remote employees admit to falling for phishing attacks while working at home

Twenty-one percent of employees said that they would continue working business as usual in the event they fell victim to a phishing attack while working remotely on a Friday, Click to read more.

58% of malicious emails feature spoofed content

According to a VIPRE Security Group report, 85% of phishing emails utilized malicious links in the content of the email, and spam emails increased by 30% from Q1 to Q2 2023, Click to read more.



of organizations anticipate rising ransomware expenditure

According to the Enterprise Strategy Group (ESG) report, 65% of organizations confirmed that ransomware is one of the top three threats to their viability, Click to read more.

September Security Article

Elevate Security: National Insider Threat Awareness Month 2023

As IT and infosec professionals, your role in safeguarding our organization against insider threats is paramount. September marks National Insider Threat Awareness Month, urging each one of you to be proactive defenders of our digital ecosystem.

- Stay Vigilant: Keep an eagle eye on unusual activities, unauthorized accesses, or data breaches within our systems. Your attentiveness can nip threats in the bud.
- Secure Your Access: Maintain robust passwords, implement MFA, and regularly update your credentials. Your authentication practices are gatekeepers against potential breaches.
- Report Swiftly: If something seems amiss, don't hesitate. Report any suspicious activity or anomaly to SIRT promptly. Your swift reporting can neutralize threats in real time. Phone: 407-823-5117 | Email: sirt@ucf.edu
- Mind Your Workspace: Keep physical documents and access devices out of prying eyes. Your diligence in maintaining a clean workspace can prevent accidental leaks.
- Stay Informed: Stay updated on the latest security protocols and emerging threat trends. Your knowledge arms you to stay ahead of evolving risks.
- Bolster Education: Participate actively in security training sessions. Your proactive involvement enhances your ability to respond effectively to emerging threats.
- Phishing Beware: Be cautious of unsolicited emails and links. Verify the authenticity of senders before engaging. Your email savvy thwarts potential breaches.

As we observe National Insider Threat Awareness Month, remember that your contributions as individuals cumulate into a fortified defense for us all. Each proactive step you take cements our digital stronghold and upholds our commitment to UCF's security excellence.

In Other (Security) News...

Cybercriminals Threaten Ransom Over GDPR Fines: 'Digital Peace Tax' Scheme

Researchers are tracking a new cybercrime group that uses a never-seen-before extortion tactic, Click to read more.

UK Cyber Agency Warns Against Chatbot Prompt Injection Threats

The National Cyber Security Centre (NCSC) has said there are growing cybersecurity risks of individuals manipulating the prompts through "prompt injection" attacks, Click to read more.

Cisco VPNs Breached: Brute Force Attacks by Akira Ransomware Group

Hackers are targeting Cisco Adaptive Security Appliance (ASA) SSL VPNs in credential stuffing and brute-force attacks that take advantage of lapses in security defenses, such as not enforcing multi-factor authentication (MFA), Click to read more.

Security Alerts

WinRAR < 6.23 allows code execution via malicious ZIP archives.

Click to read more.

Adobe ColdFusion allows arbitrary code execution without user interaction.

Click to read more.