University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 11 | November 14, 2023

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in November 2023

1. Largest DDoS attacks ever reported by Google, Cloudflare and AWS

cshub.com

The DDoS attack exceeded the previous record by over seven times, exploiting a zero-day vulnerability. The attack began during August and are continuing.

2. US SEC sues SolarWinds for concealing cyber risks before massive hacking

Reuters.com

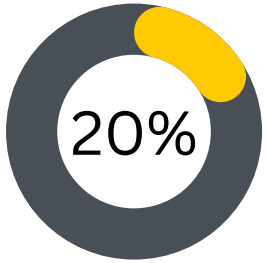
The U.S. Securities and Exchange Commission (SEC) has initiated legal action against SolarWinds Corp and its Chief Information Security Officer for allegedly misleading investors about the company's cybersecurity practices before a significant hack that targeted U.S. government agencies.

3. Data Encrypted in 75% of Ransomware Attacks on Healthcare Organizations

Infosecurity-Magazine.com

The ability of healthcare organizations to stop these attacks before data encryption fell to 24%, indicating a decline in security effectiveness against faster and more elusive cyber threats

DID YOU KNOW?

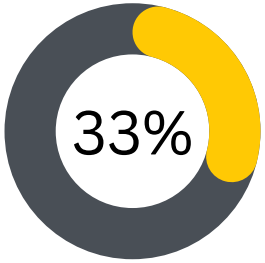


Only 20% of American consumers 'mostly' or 'completely' trust AI

Job loss, security and privacy concerns ranked the highest among consumers. Click to read more.

1 in 5 execs have shared work passwords outside the company

Despite 96% of executives claiming support for cybersecurity initiatives, many use weak password creation strategies, and nearly half have requested to bypass security measures. Click to read more.



Phishing emails impersonating HR are on the rise

Nearly one-third of users are likely to engage with these fraudulent emails, which may include topics like dress code changes, training notifications, and vacation updates. Click to read more.

November Security Article

Critical Infrastructure Security and Resilience Month

As we embrace the crisp and cozy days of November, it's more than just the post-Halloween candy sales and falling leaves that occupy our thoughts. It's also a time for reflection on the security awareness events that transpired in October. From delving into the ever-evolving trends in fraud, phishing, and social engineering, to contemplating the ethical implications of artificial intelligence, and securing the future of research, specifically focusing on the cybersecurity challenges faced by UCF as an R1 institution, October was a month filled with invaluable insights. As we move forward into November, let us continue to build upon the knowledge gained and stay vigilant in our commitment to strengthening the cybersecurity landscape.

1. Assess Your Risk:

Identify your most critical functions and assets, understand dependencies, and consider potential threats to determine vulnerabilities.

2. Make a Plan and Exercise It:

Create a resilience plan with defined recovery timelines and test it through exercises to ensure effective functionality during disruptions.

3. Continuously Improve and Adapt:

Cultivate a culture of continuous improvement, learning from experiences and evolving plans to stay prepared for changing conditions and threats.

As we embrace the opportunities presented by November's Critical Infrastructure Security and Resilience Month, let us carry forward the lessons from our October security awareness events. By assessing our risks, making well-structured plans, and continuously evolving our strategies, we not only strengthen our own resilience but also contribute to the security, vitality and the broader critical infrastructure. Together, we forge a path to a safer and more secure future.

In Other (Security) News...

Israeli Entities Under Attack By MuddyWater's Advanced Tactics

The campaign, uses spear-phishing emails and a multi-stage infection vector, including deceptive files and a new file-sharing service, to execute conduct reconnaissance.
Click to read more.

Microsoft pledges to bolster security as part of 'Secure Future' initiative

The initiative will focus on AI-based cyber defenses, improvements in software engineering, and the application of international norms to protect civilians from cyber threats.
Click to read more.

The People Hacker: AI a Game-Changer in Social Engineering Attacks

Artificial intelligence (AI) is significantly enhancing the effectiveness of social engineering attacks, making it challenging to differentiate between genuine interactions and those that are AI-generated.
Click to read more.

Security Alerts

AI ChatBot plugin for WordPress is vulnerable to Arbitrary File Deletion

Click to read more.

DHCP Server Service Denial of Service Vulnerability

Click to read more.