University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 10 ⚡ October 8, 2024

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News October 2024

1. **CISA Kicks Off 21st Anniversary of Cybersecurity Awareness Month**
   CISA.gov
   Celebrating over two decades, CISA's annual Cybersecurity Awareness Month emphasizes the “Secure Our World” theme, sharing resources and events throughout October to boost public online safety efforts.

2. **First Credible Ransomware Variant Detected For Macs**
   CyberNews.com
   Researchers have identified a ransomware variant specifically targeting macOS, marking a significant shift in cyber threats aimed at Apple users. This variant underscores the growing need for macOS-focused security measures as hackers increasingly target traditionally secure platforms.

3. **How To Spot A Business Email Compromise Scam**
   Wired.com
   Business email compromise (BEC) scams, which manipulate employees to gain unauthorized access or extract payments, are a rising threat. This guide offers key indicators of BEC scams, helping users detect suspicious emails and minimize business risks from these attacks.

DID YOU KNOW?

67% Of Orgs Say Employees Lack Basic Security Awareness

A majority of organizations report that employees lack essential cybersecurity skills, signaling a critical gap in workplace readiness.
Click to read more.

Eight Million Users Install 200+ Malicious Apps From Google Play

Over 200 malicious apps have been installed by millions on Google Play, exposing users to significant security threats.
Click to read more.

Only 24% Of Organizations Are 'Very Confident' In Their AI Policies

TFewer than a quarter of organizations feel secure in their AI policy frameworks, reflecting uncertainty in managing AI risks effectively.
Click to read more.

October Security Article

October is Cybersecurity Awareness Month: Stay Safe Online with These Essential Tips

October marks Cybersecurity Awareness Month—a perfect time to brush up on digital safety habits that keep our personal and work lives secure. This year, the focus is on empowering individuals and organizations to stay protected online with simple, effective cybersecurity practices. Let's look at four essential steps everyone can take to strengthen their digital defenses.

1. Create Strong, Unique Passwords - Passwords are the first line of defense against cyber threats. Using strong, unique passwords for each of your accounts can help prevent unauthorized access. and are typically at least 12 characters long, including a mix of upper and lower-case letters, numbers, and special symbols. A password manager can be helpful for keeping track of them securely, eliminating the need to memorize multiple complex passwords. Try using UCF's passwordless authentication on applications that offer it

2. Turn on Multi-Factor Authentication (MFA) - Multi-Factor Authentication (MFA) adds an extra layer of protection by requiring a second form of verification in addition to your password—like a code sent to your phone. Even if someone obtains or guesses your password, MFA can help prevent them from accessing your account. Enable MFA on any platform that offers it, particularly for email, financial, and social media accounts.

3. Recognize and Report Phishing - Phishing attacks often appear as messages that look trustworthy but attempt to trick you into giving away personal information or clicking on malicious links. To spot phishing emails, look out for suspicious email addresses, grammatical errors, or urgent requests for sensitive information. If you receive an email or message that seems off, don't click any links or download attachments. Instead, report it to your IT department or use your email platform's built-in reporting feature.

4. Keep Your Software Updated - Software updates are released to fix vulnerabilities, improve security, and add new features. By regularly updating your devices and applications, you're protecting yourself from known threats that could otherwise be exploited by attackers. Set up automatic updates whenever possible so you won't miss critical patches.

5. Stay Cyber Smart - Small steps add up to big security improvements. This month, consider assessing your own online habits and reinforcing these cybersecurity practices. By staying informed and vigilant, you're playing an active role in keeping both your personal information and workplace safe. Cybersecurity is everyone's responsibility—let's make our online world a safer place.

In Other (Security) News...

Flaw Crashes Apple Devices With A Single Click, Tesla Also Vulnerable

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.

DDOS Attacks Surge To Unprecedented Levels, Bombarding Servers With 4.2Tbps

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

Click to read more.

Organizations Can Substantially Lower Vulnerabilities With Secure-By-Design Practices, Report Finds

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

Click to read more.

Security Alerts

A Logged-in Attacker With Site Owner Permissions Can Use This Weakness To Add And Run Any Code Within Sharepoint Server

Click to read more.

This Macos Vulnerability Could Allow Attackers To Access Users' Protected Data, And There May Already Be Signs Of It Being Actively Exploited.

Click to read more.