University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 4 April 9, 2024

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in April 2024

1. **Dataset of 73 Million AT&T Customers Linked to Dark Web Data Breach**
   InfoSecurity-Magazine.com
   AT&T has acknowledged the authenticity of a dataset containing the details of 73 million current and former customers after a hacker advertised it on a dark web marketplace around March 17.

2. **iPhone Users Targeted with MFA Bombing Attacks – Don't Tap 'Allow!'**
   BitDefender.com
   A sophisticated phishing campaign targeting iPhone users has emerged in recent months, signaling what appears to be a weakness in Apple's password-reset mechanism – one that may need addressing.

3. **YouTube Being Used to Distribute Malware**
   CyberNews.com
   Malware, including Vidar, StealC, and Lumma Stealer, has been distributed on YouTube in the form of video game cracks, the firm revealed after the investigation. Malicious links were disguised as video descriptions and led to the download of information stealers, it said.

DID YOU KNOW?

17 Billion Personal Records Exposed in Data Breaches in 2023

Reported data breach incidents rose by 34.5% in 2023, with over 17 billion personal records compromised throughout the year, according to Flashpoint's 2024 Global Threat Intelligence Report.
Click to read more.

92% of IT Leaders Report Cyberattacks are More Frequent Than Last Year

A report by Keeper Security contains a survey of more than 800 global IT professionals and security executives, revealing key trends in the cybersecurity landscape.
Click to read more.

New, Sophisticated Phishing-As-A-Service Platform Discovered

Researchers from Netcraft have revealed that they discovered a new phishing-as-a-service platform, which has been named darcula.
Click to read more.

April Security Article

Don't be the Fool: Protect Yourself from Cyber Tricks Year-round!

Even though April Fools' Day has passed, the jokes don't end when it comes to cyber threats. While it's fun to engage in harmless pranks, being caught off guard by phishing attacks, outdated software vulnerabilities, weak passwords, data loss, or unsecured public WiFi networks is no laughing matter. That's why we're here to keep you one step ahead in the cybersecurity game.

1. Phishing Attacks - Hook, Line, and Sinker: Phishing scams are like the ultimate pranksters of the cyber world, tricking you into revealing sensitive information. Always double-check sender addresses, avoid clicking on suspicious links or attachments, and be wary of urgent requests for personal or financial data.
2. Keep Your Software Updated - Patch Up Those Holes: Just like a magic trick, cybercriminals can exploit the gaps in outdated software. Stay on top of updates for your operating system, antivirus, and applications to patch up vulnerabilities before cyber tricksters can take advantage of them.
3. Strong & Unique Passwords - The Secret to Security: Don't let your passwords be the punchline of a cyber attack. Create strong, unique passwords for each account and consider using a password manager to keep track of them securely. Remember, "password123" is about as funny as a whoopee cushion at a business meeting.
4. Backup Your Data - Don't Let Data Loss be the Punchline: Imagine the prank of losing all your data unexpectedly. It's not a joke! Regularly back up your important files to external hard drives or cloud storage services. That way, even if cyber tricksters strike, you can restore your data and avoid the punchline of data loss.
5. Public WiFi Networks - Watch Out for Cyber Pickpockets: Public WiFi networks can be as precarious as a prankster's handshake. Exercise caution when connecting to them, avoid sensitive transactions, and consider using a VPN for an extra layer of security. Remember, not every WiFi network is your friend!

So, while April Fools' Day is behind us, the importance of staying vigilant against cyber threats remains ever-present. Don't be the fool who falls victim to cyber trickery. Stay informed, stay secure, and keep those cyber pranksters at bay.

In Other (Security) News...

Cybercriminals Selling New Tool Weaponizing Raspberry Pi

Threat actors have come up with a new solution called Geobox that transforms the mini-computer Raspberry Pi into a Swiss-army knife type of hacking device for fraudsters and other criminals.

Click to read more.

NIST Awards $3.6 Million for Community-Based Cybersecurity Workforce Development

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has awarded cooperative agreements totaling nearly $3.6 million aimed at building the workforce needed to safeguard enterprises from cybersecurity risks.

Click to read more.

Government Board Pins China Hack on Microsoft's 'inadequate' Cybersecurity Strategies

A high-profile government advisory board released a scathing report Tuesday evening concluding that a Chinese espionage campaign targeting Microsoft last summer was "preventable and should never have occurred."

Click to read more.

Security Alerts

Bug in the iPhone's Core System Could Let a Hacker Get Around the Phone's Security Measures

Click to read more.

A Flaw in Windows Hyper-V Could Lead to a Shutdown or Disruption of Service

Click to read more.