Top 3: Security News in February 2024

1. GTA 5 Used to Lure Torrent Users with Malicious File
   CyberNews.com
   All files were used by bad actors to distribute malware such as Trojans, Remote Access Tools (RATs), malicious web extensions, coin miners, keyloggers, and more.

2. Cyberattacks on Clorox, Johnson Controls Cost Companies $76M Combined
   SCMagazine.com
   Cybersecurity incidents in 2023 cost Clorox and Johnson Controls nearly $76 million combined, according to reports filed with the Securities and Exchange Commission (SEC). The incidents underscore the painful reality that such attacks cost real money.

3. Malware-as-a-Service Now the Top Threat to Organizations
   InfoSecurity-Magazine.com
   MaaS infections were the biggest threat to organizations in the second half of 2023, according to a new Darktrace report.

DID YOU KNOW?

Tax Return Scammers Flood Google with Fake Ads
Scammers are using malicious ads that appear across the top of search engine results to try and con people into parting with their money or data. Click to read more.

79% of Organizations Faced a Ransomware Attack in H2 2023
The cyber threat landscape is expected to get even worse in 2024, according to the report, with 96% of respondents saying the threat of cyberattacks to their industry will increase this year. Click to read more.

Hackers Exploit Job Boards, Stealing Millions of Resumes and Personal Data
ResumeLooters has stolen 510,259 data files from job search websites. Click to read more.
February Security Article

Navigating Love and Cybersecurity Awareness in February

As we embrace the uniqueness of February, including the extra day this leap year, let’s take a moment to enhance our cybersecurity awareness, especially in matters of the heart. This month’s theme, “Love Safely in the Digital Age,” addresses common romance cybersecurity threats:

1. Common Romance Cybersecurity Threats:
   a. Phishing: Verify the legitimacy of unsolicited emails or messages to protect yourself from potential threats.
   b. Vishing (Voice Phishing): Confirm the identity of callers before sharing personal information over the phone.
   c. Smishing (SMS Phishing): Exercise caution with unexpected text messages, especially when it comes to clicking on links.

2. Catfishing:
   a. Be vigilant on social media and dating platforms, taking steps to verify identities and promptly reporting suspicious behavior.

3. Dating App Security:
   a. Enhance security by using strong, unique passwords for dating apps.
   b. Safeguard your personal information until trust is established.
   c. Stay up-to-date with app updates to benefit from the latest security features.

4. Stay Informed, Stay Secure:
   a. Foster conversations about online security within our community.
   b. Share these valuable tips with friends and loved ones, contributing to a safer digital environment for all.

As we navigate through February’s unique landscape, let’s prioritize safe and secure online connections. Love responsibly and stay secure!