University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 7 July 16, 2024

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in July 2024

1. Cybersecurity regulations face 'uphill battle' after Chevron ruling

CyberScoop.com

The Biden administration has looked to regulation to strengthen cybersecurity rules, but a Supreme Court ruling threatens that effort.

2. US bans Kaspersky for posing 'significant risk'

CyberNews.com

The US is banning the sale of antivirus software made by Russian cyber-security firm Kaspersky because of its ties with Russia's regime.

3. OpenAI breach in 2023 raises national security concerns

SCMagazine.com

A hacker believed to be a private individual gained access to OpenAI's internal messaging systems early last year and stole details about the design of ChatGPT has raised fears that the nation's adversaries could do the same.

DID YOU KNOW?

10 Billion Passwords Leaked on Hacking Forum

The researchers discovered the leak of 9.94 million plaintext passwords, described as the largest password compilation of all time, which was posted on a popular hacking forum by a user named 'ObamaCare' on July 4. Click to read more.

Half of Employees Fear Punishment for Reporting Security Mistakes

The report also highlighted significant concerns among cybersecurity professionals about the impact of security awareness training on changing employee behaviors. Click to read more.

Australian Man Charged for Fake Wi-Fi Scam on Domestic Flights

The individual is said to have staged what's called an evil twin Wi-Fi attack across various location. Click to read more.

July Security Article

Stay Cyber-Safe: Ransomware Awareness Month

As summer heats up and we reflect on July 4, it's crucial to stay vigilant against ransomware. July is Ransomware Awareness Month, a time to educate ourselves on online dangers and protection methods.

Understanding Ransomware Attacks

Ransomware blocks access to data until a ransom is paid. It affects individuals and corporations through:

- Malspam: Emails with infected attachments or links.
- Malvertising: Malicious online ads.
- Spear Phishing: Personalized attacks with malicious links or attachments.
- Social Engineering: Manipulating individuals to gain system access.

Types of Ransomware

- Scareware: Displays fake warnings to scare victims into paying.
- Screen Lockers: Locks users out of their computers with a payment demand.
- Encrypting Ransomware: Encrypts files, requiring payment for a decryption key.

Summer Cyber Safety Tips

- Be Skeptical: Avoid opening attachments or links from unknown sources.
- Keep Software Updated: Regular updates protect against vulnerabilities.
- Back Up Data: Regular backups ensure data recovery without paying a ransom.
- Educate Yourself and Others: Stay informed and share knowledge on cybersecurity threats.

As we continue to enjoy the summer and the memories of Independence Day, let's also commit to safeguarding our digital independence. Stay safe, stay vigilant, and have a wonderful July!

In Other (Security) News...

Apple rolls out quantum-resistant cryptography for iMessage

On Wednesday, Apple said it is integrating cryptographic protocols in iMessage that are resistant to attack from quantum computers of the future.
Click to read more.

Hackers hit Poland Euro 2024 match broadcast in second attack

Initial checks suggested the hackers launched a distributed denial of service (DDoS) attack - which overwhelms servers with huge amounts of traffic - blocking fans from watching the transmission of the Group D clash, the broadcaster TVP said. Click to read more.

YouTube Creates Privacy Tools To Protect Users From AI Content

YouTube creators and users can now request to erase artificial intelligence-generated content meant to look or sound like them. The new policy is not listed under YouTube's Community Guidelines but instead under its privacy policy, suggesting that simulating someone with AI technology is a violation of user privacy.
Click to read more.

Security Alerts

A flaw in Citrix ADC and Citrix Gateway can let attackers run any code without logging in

Click to read more.

Older Drupal versions have a security flaw allowing attackers to remotely execute any code due to default module configuration issues.

Click to read more.