University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 8 | August 8, 2023

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in August 2023

1. Facebook Zero-Day Phishing Attack

BleepingComputer.com

Hackers exploited a zero-day vulnerability in Salesforce's email services and SMTP servers to launch a sophisticated phishing campaign targeting valuable Facebook accounts.

2. Hackers Exploiting Windows Search for Remote Access Trojans

TheHackerNews.com

A legitimate Windows search feature is being exploited by unknown malicious actors to download arbitrary payloads from remote servers and compromise targeted systems with remote access trojans such as AsyncRAT and Remcos RAT.

3. Israel's Top Oil Refinery Site Offline Following DDoS Attack

BleepingComputer.com

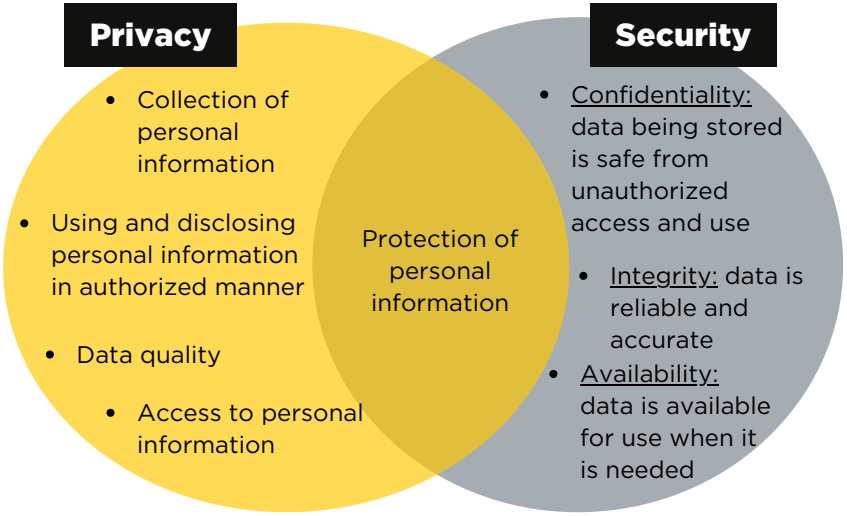
Website of Israel's largest oil refinery operator, BAZAN Group is inaccessible from most parts of the world as threat actors claim to have hacked the Group's cyber systems.

DID YOU KNOW?

You can have security without privacy, but you can't have privacy without security.

- "Privacy includes the laws and regulations requiring organizations to protect your data."
- "Security includes the technical methods to protect that data."

[National Cybersecurity Alliance]



August Security Article

Strengthening Password Security: A Vital Guide for IT and Infosec Professionals

In the realm of cybersecurity, password protection stands as our first line of defense against breaches. As members of the UCF community, your role in safeguarding our digital landscape is pivotal. Here's a concise yet actionable roadmap to bolster password security:

- Complexity Matters: Craft passwords with a minimum of eight characters for user accounts and 15 for accounts with access to sensitive information, blending cases, numbers and symbols. Avoid predictable choices like birthdays.
- Stay Unique: Never reuse passwords. Every account deserves its own strong passphrase to prevent a chain reaction of breaches.
- Passphrases, Your Allies: Consider using strings of unrelated words or a meaningful sentence (passphrases) as a secure and memorable option.
- Double Down with MFA: Activate multi-factor authentication (MFA) whenever possible for an added layer of security.
- Phishing Alert: Stay vigilant against phishing. Never share passwords via email or click on suspicious links.
- Secure Storage: Trust reputable password managers for encrypted, organized, and accessible credentials.
- Public Wi-Fi Caution: Avoid sensitive logins on public Wi-Fi networks to prevent password stealing and data exposure.
- Shared Computers, Shared Risks: Never save passwords on shared computers and always log out.
- Audit and Educate: Regularly review old accounts and spread these practices among colleagues.
- Report Anomalies: Swiftly notify SIRT of any suspicious activity for proactive breach prevention. Phone: 407-823-5117 | Email: sirt@ucf.edu

By following these steps, you fortify our collective cybersecurity efforts. Your commitment to robust password practices plays a pivotal role in our digital defense.

In Other (Security) News...

Canon Inkjet Printers Expose Wi-Fi Threat

In a security advisory published on Monday, Canon said it discovered a flaw in specific inkjet printer models where sensitive Wi-Fi connection settings are not adequately erased during the regular initialization process, Click to read more.

AI-Enhanced Phishing Driving Ransomware Surge

According to a new report published on August 2, 2023, by data protection provider Barracuda Networks, the number of reported attacks against municipalities, education and healthcare has doubled since last year and more than quadrupled since 2021, Click to read more.

Heart Monitoring Tech Provider Confirms Cyberattack

A tech provider for heart monitoring and medical electrocardiograms confirmed on Wednesday that it was responding to a cyberattack on its systems, Click to read more.

Security Alerts

Memory Safety Bugs Present in Firefox

Click to read more.

Apple Apps May be Able to Modify Sensitive Kernel State

Click to read more.