August 6, 2024

Theme of the month: Multi-factor Authentication (MFA) Fatigue Attacks (look for the ✪)
Challenge yourself with our MFA Fatigue Attacks Quiz!
What you can do to improve your MFA security:

All Users	Technical Users	Business Owners
If you receive an unsolicited message letting you know that there has been an attempt to access your account, be suspicious of this. Do not follow any links in the message and reset your account's password.	Consider implementing MFA measures that can boost security and make the authentication process easier for users, which include: time-based one-time passwords (TOTPs), biometric authentication, and context-aware authentication.	Consider various factors when planning for an MFA solution for your organization. To prevent MFA fatigue, have your IT team provide a plan that simplifies MFA where applicable while applying complex MFA requirements for critical assets.

Check out our MFA Quiz to learn more about MFA security.

This past week's stories:

Privacy commissioner launches investigation into Ticketmaster data breach

Thousands of cybersecurity professionals needed in Canada, report shows

U.S. releases high-profile Russian hackers in diplomatic prisoner exchange

Personal, health information stolen from pharma giant Cencora

Meta settles for $1.4 billion with Texas over illegal biometric data collection

Phishing campaign exploited Proofpoint email protections for spoofing

Scammers now impersonating crypto exchanges to get access to your accounts, FBI warns

CrowdStrike sued by shareholders over global outage

Thousands of Ubiquiti cameras and routers vulnerable, despite patches available

CrowdStrike outage renews supply chain concerns, federal officials say

---

Privacy commissioner launches investigation into Ticketmaster data breach

Canada's privacy commissioner has launched an investigation into a cybersecurity breach at Ticketmaster after an attack by a hacker group compromised the personal information of millions of customers around the world.

https://www.cbc.ca/news/politics/privacy-commissioner-probe-data-breach-1.7280917

Click above link to read more.

Back to top

Thousands of cybersecurity professionals needed in Canada, report shows

About 157,000 Canadian cybersecurity professionals are needed to fill skill gaps, says a new report after a recent survey found security breaches have been felt by nearly 90 per cent of Canadian organizations due to a lack of such skills.

https://www.vancouverisawesome.com/highlights/thousands-of-cybersecurity-professionals-needed-in-canada-report-shows-9258943

Click above link to read more.

Back to top

U.S. releases high-profile Russian hackers in diplomatic prisoner exchange

In a historic prisoner exchange between Belarus, Germany, Norway, Russia, Slovenia, and the U.S., two Russian nationals serving time for cybercrime activities have been freed and repatriated to their country.

https://thehackernews.com/2024/08/us-releases-high-profile-russian.html

Click above link to read more.

Back to top

Personal, health information stolen from pharma giant Cencora

Pharma giant Cencora this week confirmed that personally identifiable information (PII) and protected health information (PHI) was stolen in a February 2024 cyberattack.

https://www.securityweek.com/personal-health-information-stolen-from-pharma-giant-cencora/

Click above link to read more.

Back to top

Meta settles for $1.4 billion with Texas over illegal biometric data collection

Meta, the parent company of Facebook, Instagram, and WhatsApp, agreed to a record $1.4 billion settlement with the U.S. state of Texas over allegations that it illegally collected biometric data of millions of users without their permission, marking one of the largest penalties levied by regulators against the tech giant.

https://thehackernews.com/2024/07/meta-settles-for-14-billion-with-texas.html

Click above link to read more.

Back to top

Phishing campaign exploited Proofpoint email protections for spoofing

Threat actors have exploited an issue in Proofpoint's email protection service to spoof well-known brands as part of a broad phishing campaign, according to a report from Guardio Labs.

https://www.securityweek.com/phishing-campaign-exploited-proofpoint-email-protections-for-spoofing/

Click above link to read more.

Back to top

Scammers now impersonating crypto exchanges to get access to your accounts, FBI warns

Scammers are increasingly impersonating cryptocurrency exchanges, feigning concern about clients' funds. They urge victims to "safeguard" accounts from attackers by providing credentials or access, The Federal Bureau of Investigation (FBI) warns.

https://cybernews.com/security/scammers-impersonating-crypto-exchanges-fbi-warns/

Click above link to read more.

Back to top

CrowdStrike sued by shareholders over global outage

CrowdStrike is being sued by its shareholders after a faulty software update by the cybersecurity firm crashed more than eight million computers and caused chaos around the world.

https://www.bbc.com/news/articles/cy08ljxndr4o

Click above link to read more.

Back to top

Thousands of Ubiquiti cameras and routers vulnerable, despite patches available

More than 20,000 internet-exposed Ubiquiti devices are open to attackers, revealing sensitive data about the owners, Check Point Research warns.

https://cybernews.com/security/thousands-ubiquiti-cameras-and-routers-vulnerable/

Click above link to read more.

Back to top

CrowdStrike outage renews supply chain concerns, federal officials say

The White House and the U.S. Government Accountability Office are raising questions about the resilience of the software supply chain and memory safety vulnerabilities.

https://www.cybersecuritydive.com/news/crowdstrike-outage-supply-chain/723198/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca