September 14, 2021

Challenge yourself with our ABCs of Cyber Security quiz!

This week's stories:

- **Posthaste: Digital fraud is growing in Canada — at twice the world's pace**
- **Toronto police issue warning about cryptocurrency phishing scam**

Cyber arms dealer exploits new iPhone software vulnerability, affecting most versions, say researchers

UN confirms April 2021 data breach

Security fears & remote work drive continued 2FA adoption

New Android banking malware steals login credentials from shopping & banking apps

Why ransomware hackers love a holiday weekend

Nearly 50% of on-premise databases have vulnerabilities

Recent breaches underscore high healthcare security risk

HP OMEN Gaming Hub flaw affects millions of Windows computers

Hackers dump login credentials of Fortinet VPN users in plain-text

McDonald's email blast includes password to Monopoly game database

---

Posthaste: Digital fraud is growing in Canada — at twice the world's pace

A new study by TransUnion finds that digital fraud attempts in Canada are growing twice as fast as the percentage rise globally, and the focus of the attacks is shifting.

The rate of suspected digital fraud attempts rose 16.5% globally in the second quarter of 2021 compared to the same time period in 2020. In Canada that rate jumped 44.9%.

https://financialpost.com/executive/executive-summary/posthaste-digital-fraud-is-growing-in-canada-at-twice-the-worlds-pace

Click above link to read more.

Back to top

Toronto police issue warning about cryptocurrency phishing scam

Toronto police are warning the public about an ongoing phishing scam associated with cryptocurrency exchanges.

Police say the scam involves people searching for their account login page via online search engines.

According to investigators, when people with cryptocurrency stored on an online platform conduct a search to find the login page, they have encountered a sponsored advertisement that mirrors the actual exchange page.

https://toronto.ctvnews.ca/toronto-police-issue-warning-about-cryptocurrency-phishing-scam-1.5576992

Click above link to read more.

Back to top

Cyber arms dealer exploits new iPhone software vulnerability, affecting most versions, say researchers

A cyber surveillance company based in Israel developed a tool to break into Apple (AAPL.O) iPhones with a never-before-seen technique that has been in use since at least February, internet security watchdog group Citizen Lab said on Monday.

The discovery is important because of the critical nature of the vulnerability, which requires no user interaction and affects all versions of Apple's iOS, OSX, and watchOS, except for those updated on Monday.

https://www.reuters.com/technology/cyber-arms-dealer-exploits-new-apple-iphone-software-vulnerability-affects-most-2021-09-13/

Click above link to read more.

Back to top

UN confirms April 2021 data breach

The United Nations has confirmed its infrastructure was breached earlier this year. Additional attacks linked to the earlier breach have also been detected and are now under investigation.

Stéphane Dujarric, spokesman for the Secretary-General, released a statement following a Bloomberg report sharing details of the breach. "We can confirm that unknown attackers were able to breach parts of the United Nations infrastructure in April of 2021," he wrote, noting the attack had been detected before officials were notified by a security firm, named as Resecurity in the Bloomberg report, and that remediation was already being planned and implemented.

https://www.darkreading.com/attacks-breaches/un-confirms-april-2021-data-breach

Click above link to read more.

Back to top

Security fears & remote work drive continued 2FA adoption

A quarter of the population in the United States and the United Kingdom who had not encountered two-factor authentication (2FA) two years ago have now used the technology at least once in 2021, according to a biennial study conducted by Cisco System's Duo Labs.

The census-representative survey found more than three-quarters of the population (79%) used two-factor authentication in 2021, and 72% used the technology regularly. Companies have driven the gains, with 79% of employed workers regularly using 2FA technology and only 60% of unemployed people doing the same.

https://www.darkreading.com/authentication/security-fears-remote-work-drive-continued-2fa-adoption

Click above link to read more.

Back to top

New Android banking malware steals login credentials from shopping & banking apps

An Android Trojan has been recently discovered by security experts and, it could enable the threat actors to steals all the personally identifiable data from infected devices, which also include bank credentials, and open the door to perform fraud.

This trojan is a combination of banking apps, cryptocurrency wallets, and shopping apps and it is currently targetting the US and Spain.

https://cybersecuritynews.com/new-android-banking-malware-steals-login-credentials/

Click above link to read more.

Back to top

Why ransomware hackers love a holiday weekend

On the Friday heading into Memorial Day weekend this year, it was meat-processing giant JBS. On the Friday before the Fourth of July, it was IT-management software company Kaseya and, by extension, over a thousand businesses of varying size. It remains to be seen whether Labor Day will see a high-profile ransomware meltdown as well, but one thing is clear: hackers love holidays.

Really, ransomware hackers love regular weekends, too. But a long one? When everyone's off carousing with family and friends and studiously avoiding anything remotely office-related? That's the good stuff. And while the trend isn't new, a joint warning issued this week by the FBI and the Cybersecurity and Infrastructure Security Agency underscores how serious the threat has become.

https://arstechnica.com/information-technology/2021/09/why-ransomware-hackers-love-a-holiday-weekend/

Click above link to read more.

Back to top

Nearly 50% of on-premise databases have vulnerabilities

Almost half of all companies have internal databases with known vulnerabilities, with the average vulnerable database having 26 publicly disclosed flaws – more than half of which are critical or high-severity issues, according to data collected over the past five years by Internet security firm Imperva.

While vulnerable on-premise databases gain some protection from being inside the corporate firewall, companies that leave databases with known and unpatched flaws are exposing them to attackers who gain access to a company's network or are able to use public applications to deliver payloads to the back-end systems, the company states in a blog post. Many of the unpatched vulnerabilities are at least 3 years old, and more than half (56%) are considered serious.

https://www.darkreading.com/database-security/nearly-50-of-on-premise-databases-have-vulnerabilities

Click above link to read more.

Back to top

Recent breaches underscore high healthcare security risk

Cyberattacks continue to pummel healthcare organizations already stretched thin by lack of resources and the ongoing COVID-19 pandemic, as evidenced by two recently disclosed attacks targeting providers in California and Arizona.

Starting Aug. 24, 2021, California-based LifeLong Medical Care began informing individuals that their data was affected in a ransomware attack against Netgain, a third-party vendor that provides services to healthcare providers. LifeLong reported to the Department of Health and Human Services that 115,448 people were affected in the attack.

https://www.darkreading.com/attacks-breaches/recent-breaches-underscore-high-healthcare-security-risk

Click above link to read more.

Back to top

HP OMEN Gaming Hub flaw affects millions of Windows computers

Cybersecurity researchers on Tuesday disclosed details about a high-severity flaw in the HP OMEN driver software that impacts millions of gaming computers worldwide, leaving them open to an array of attacks.

Cybersecurity firm SentinelOne, which discovered and reported the shortcoming to HP on February 17, said it found no evidence of in-the-wild exploitation. The computer hardware company has since released a security update to its customers to address these vulnerabilities.

https://thehackernews.com/2021/09/hp-omen-gaming-hub-flaw-affects.html

Click above link to read more.

Back to top

Hackers dump login credentials of Fortinet VPN users in plain-text

Popular network security solutions provider, Fortinet, has confirmed that a cybercriminal gang managed to gain unauthorized access to VPN login IDs and passwords linked with 87,000 FortiGate SSL-VPN devices.

Hackread.com can confirm the gang has dumped a trove of around 500,000 login credentials belonging to Fortinet VPN users. This disclosure came after the hacker leaked a list of compromised credentials for free on a recently launched Russian-speaking Dark Web forum called RAMP and on the data leak website of Groove ransomware.

https://www.hackread.com/hackers-dump-fortinet-vpn-users-login-credentials/

Click above link to read more.

Back to top

McDonald's email blast includes password to Monopoly game database

McDonald's UK Monopoly VIP game kicked off at the end of August, and a recent round of emails sent to winners of the game's various prizes included more than a coupon for free fries. The franchise accidentally inserted passwords for a McDonald's server that hosted information tied to the UK Monopoly VIP game.

In the wrong hands, these credentials could have been abused to rip off players or cheat the game on a massive scale, according to experts. The gaff was spotted by researcher Troy Hunt, along with some tech-savvy winners who realized what they had.

McDonald's said it quickly changed the server passwords when it the error was brought to its attention.

https://threatpost.com/mcdonalds-email-blast-includes-password-to-monopoly-game-database/169346/

Click above link to read more.

Back to top

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

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

OCIOSecurity@gov.bc.ca