Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

October 5, 2021

Challenge yourself with our Cyber Security Awareness Month quiz!

Join Cyber Security Awareness Month!

Register for Security Day!

This week's stories:

🍁 **Seven in 10 Canadian organizations facing ransomware attack paid demands: survey**

🍁 **Interac acquires rights to SecureKey digital identification services in Canada**

🍁 **Half of Canadian employees not concerned about cyber crime, but vigilance is key to preventing attacks**

Facebook Releases New Tool That Finds Security and Privacy Bugs in Android Apps

Baby's Death Alleged to Be Linked to Ransomware

Ransomware attack disrupts hundreds of bookstores across France, Belgium and the Netherlands

Neiman Marcus says 4.6 million affected by data breach

Researcher refuses Telegram's bounty award, discloses auto-delete bug

Ransomware is leading hospital boards to pour more money into cybersecurity

Cybercriminals bypass 2FA and OTP with robocalling and Telegram bot

Why today's cybercriminals are more dangerous

Coinbase warns users of 'large-scale' phishing threat

Ukrainian police arrest hacker who caused $150 million damage to global firms

---

Seven in 10 Canadian organizations facing ransomware attack paid demands: survey

Cybersecurity experts say a new poll that suggests nearly 70 per cent of Canadian organizations facing a ransomware attack last year paid the demands is evidence that such payments should be made illegal.

Of the businesses surveyed, 17 per cent said they faced such attacks, according to the Canadian Internet Registration Authority's (CIRA) annual cybersecurity survey.

https://www.coastreporter.net/the-mix/seven-in-10-canadian-organizations-facing-ransomware-attack-paid-demands-survey-4482972

Click above link to read more.

Back to top

Interac acquires rights to SecureKey digital identification services in Canada

Interac Corp. says it has signed a deal to acquire the exclusive rights to SecureKey Technologies Inc.'s digital identification services in Canada.

Financial terms of the agreement were not immediately available.

Interac says SecureKey will help in its building of a national network that will allow people to securely share and verify their identity information digitally.

https://www.cp24.com/news/interac-acquires-rights-to-securekey-digital-identification-services-in-canada-1.5607074

Click above link to read more.

Back to top

Half of Canadian employees not concerned about cyber crime, but vigilance is key to preventing attacks

Cyber crime is rampant today, and 2022 is predicted to be the worst year ever. Yet, half of employed Canadians (51%) say they are not concerned their place of employment will experience a cyber attack or security breach. And almost four in 10 say they don't receive cybersecurity training at work. For Cybersecurity Awareness Month, ISA Cybersecurity is providing advice on how to follow cyber-smart work practices. That includes encouraging business owners to educate employees that cyber attacks are a real threat, and they must play a part in preventing them.

"Creating a cyber-aware culture in the workplace is a must in 2021," says Kevin Dawson, President & CEO of ISA Cybersecurity. "Employees are the front line of defense against cyber crime, and as an employer it's up to you to make cyber awareness a priority. Continuous training and adherence to best practices will make employees less likely to click on a phony link or open an infected attachment. These are simple but powerful ways to prevent a cyber attack."

https://www.newswire.ca/news-releases/half-of-canadian-employees-not-concerned-about-cyber-crime-but-vigilance-is-key-to-preventing-attacks-872577965.html

Click above link to read more.

Back to top

Facebook Releases New Tool That Finds Security and Privacy Bugs in Android Apps

Facebook on Wednesday announced it's open-sourcing Mariana Trench, an Android-focused static analysis platform the company uses to detect and prevent security and privacy bugs in applications created for the mobile operating system at scale.

"[Mariana Trench] is designed to be able to scan large mobile codebases and flag potential issues on pull requests before they make it into production," the Menlo Park-based social tech behemoth said.

https://thehackernews.com/2021/09/facebook-releases-new-tool-that-finds.html

Click above link to read more.

Back to top

Baby's Death Alleged to Be Linked to Ransomware

Access to heart monitors disabled by the attack allegedly kept staff from spotting blood & oxygen deprivation that led to the baby's death.

A U.S. hospital paralyzed by ransomware in 2019 will be defending itself in court in November over the death of a newborn, allegedly caused by the cyberattack.

As the Wall Street Journal reported on Thursday, the baby's mother, Teiranni Kidd, gave birth to her daughter, Nicko Silar, on July 16, 2019, without knowing that the hospital was entering its eighth day of clawing its way back from the attack.

https://threatpost.com/babys-death-linked-ransomware/175232/

Click above link to read more.

Back to top

Ransomware attack disrupts hundreds of bookstores across France, Belgium and the Netherlands

Hundreds of bookstores across France, Belgium, and the Netherlands have had their operations disrupted this week after a ransomware attack crippled the IT systems of TiteLive, a French company that operates a SaaS platform for book sales and inventory management.

The incident, which took place earlier this week, has impacted bookstore chains such as Libris, Aquarius, Malperthuis, Donner, Atheneum Boekhandels, and others, according to reports from news outlets in France, Belgium, and the Netherlands.

https://therecord.media/ransomware-attack-disrupts-hundreds-of-bookstores-across-france-belgium-and-the-netherlands/

Click above link to read more.

Back to top

Neiman Marcus says 4.6 million affected by data breach

Dallas-based Neiman Marcus Group says it is notifying 4.6 million of its online customers who are affected by a data breach that occurred in May 2020.

The compromised data includes usernames, passwords, and security questions and answers linked with online accounts. Neiman Marcus has triggered a password reset for accounts that have not changed their passwords since the breach.

https://www.bankinfosecurity.com/neiman-marcus-says-46m-affected-by-data-breach-a-17658

Click above link to read more.

Back to top

Researcher refuses Telegram's bounty award, discloses auto-delete bug

Telegram patched another image self-destruction bug in its app earlier this year. This flaw was a different issue from the one reported in 2019. But the researcher who reported the bug isn't pleased with Telegram's months-long turnaround time—and an offered $1,159 (€1,000) bounty award in exchange for his silence.

Like other messaging apps, Telegram allows senders to set communications to "self-destruct," such that messages and any media attachments are automatically deleted from the device after a set period of time. Such a feature offers extended privacy to both the senders and the recipients intending to communicate discreetly.

https://arstechnica.com/information-technology/2021/10/researcher-refuses-telegrams-bounty-award-discloses-auto-delete-bug/

Click above link to read more.

Back to top

Ransomware is leading hospital boards to pour more money into cybersecurity

Ransomware has been plaguing healthcare provider organizations for some time now. The onset of the COVID-19, in fact, brought even more attacks.

Steve Smerz is chief information security officer at Halo Health, vendor of a clinical collaboration platform that includes secure messaging, video, voice, alarms and alerts designed to enable clinicians to connect easily.

He says he's seeing a drive for hospital and health system boards to increase resources to cybersecurity teams as ransomware continues to nail healthcare organizations in the second half of 2021.

https://www.healthcareitnews.com/news/ransomware-leading-hospital-boards-pour-more-money-cybersecurity

Click above link to read more.

Back to top

Cybercriminals bypass 2FA and OTP with robocalling and Telegram bot

Two-factor authentication (2FA) has been widely adopted by online services over the past several years and turning it on is probably the best thing users can do for their online account security. Faced with this additional hurdle that prevents them from exploiting stolen passwords, cybercriminals have had to adapt, too, and come up with innovative ways to extract one-time use authentication codes from users.

According to a new report from cybercrime intelligence firm Intel 471, the latest development in 2FA bypassing involves the use of robocalls with interactive messages that are meant to trick users into handing over their one-time passwords (OTPs) in real-time as attackers are trying to access their accounts. All of this is automated and controlled by using Telegram-based bots, much like teams in organizations use Slack bots to automate workflows.

https://www.csoonline.com/article/3634603/cybercriminals-bypass-2fa-and-otp-with-robocalling-and-telegram-bots.html

Click above link to read more.

Back to top

Why today’s cybersecurity threats are more dangerous

Over the past two years, the rise of big-ticket ransomware attacks and revelations of harmful software supply chain infections have elevated cybersecurity to the top of the government's agenda. At the same time, corporate America and even the general public have awakened to the new array of digital dangers posed by nation-state actors and criminal organizations.

It's little surprise then that two threads running through this year's Aspen Cyber Summit were the intricate nature of the cybersecurity threats we now face and how they may differ from the challenges we faced in the past. "We've got this growing complexity and growing interdependence," Window Snyder, CEO of Thistle Technologies, said. "So, the opportunities [for threat actors] are growing faster than we're able to mitigate them.”

https://www.csoonline.com/article/3635097/why-today-s-cybersecurity-threats-are-more-dangerous.html

Click above link to read more.

Back to top

Coinbase warns users of 'large-scale' phishing threat

Just in time for Cybersecurity Awareness Month, Coinbase has disclosed a "large-scale" phishing attack that impacted users earlier this year.

In a Sept. 27 blog post, Coinbase announced that the "broad" attack occurred between April and early May of 2021. At least 6,000 Coinbase customers were affected by the attack.

https://www.cnet.com/personal-finance/coinbase-warns-users-of-large-scale-phishing-threat/

Click above link to read more.

Back to top

Ukrainian police arrest hacker who caused $150 million damage to global firms

Ukrainian police said on Monday they had arrested a 25-year-old man who hacked more than 100 foreign companies and caused damage worth more than $150 million.

The hacker, who was not identified, used phishing attacks and hijacked software that allows computers to be accessed remotely, a police statement said. The victims included "world-famous energy and tourism companies", it added.

https://www.reuters.com/technology/ukrainian-police-arrest-hacker-who-caused-150-million-damage-global-firms-2021-10-04/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer