October 8th, 2019

October is "Cybersecurity awareness" Month

Try our October quiz – Fake or Not

This week's stories:

- **Investigation finds improper access to patient records at Red Deer hospital**
- **Canadian credit reporting agency compromised through third party**
- **FBI warns about attacks that bypass multi-factor authentication (MFA)**
- **The case for making political parties follow the same privacy rules as corporations**
- **Getting a new mobile number in China will involve a facial-recognition test**
- **A lack of physical security still leads to data breaches but is being ignored, says study from Shred-It and Ponemon Institute**
- **Muhstik Ransomware Victim Hacks Back, Releases Decryption Keys**
- **Check If You Are in the Sephora and StreetEasy Data Breaches**

Investigation finds improper access to patient records at Red Deer hospital

https://www.cbc.ca/news/canada/edmonton/red-deer-patient-records-breach-1.5309419

An internal investigation found inappropriate access to patient electronic health records at Red Deer Regional Hospital over a six-month period, Alberta Health Services said Friday in a news release.

A total of 2,158 patient records were accessed between December 2018 and May 2019. The breach was discovered during a routine audit in April, and an investigation followed.

The records were in the Alberta Public Laboratories clinical lab at the hospital, and most belonged to emergency patients.

Click link above to read more

Canadian credit reporting agency compromised through third party

https://www.itworldcanada.com/article/canadian-credit-reporting-agency-compromised-through-third-party/422576

A hacker was able to access financial information on 37,000 Canadians or businesses held by credit reporting agency TransUnion Canada for two weeks over the summer by going through one of the company's business customers.

The news site Bleeping Computer said Monday it had learned that TransUnion Canada began mailing notification letters to affected customers, saying someone stole the access code of equipment leasing firm CWB National Leasing, and with it entered a TransUnion business portal to do credit file lookups between June 28th and July 11th.

Click link above to read more

FBI warns about attacks that bypass multi-factor authentication (MFA)

https://www.zdnet.com/article/fbi-warns-about-attacks-that-bypass-multi-factor-authentication-mfa/

The US Federal Bureau of Investigation (FBI) has sent last month a security advisory to private industry partners about the rising threat of attacks against organizations and their employees that can bypass multi-factor authentication (MFA) solutions.

"The FBI has observed cyber actors circumventing multi-factor authentication through common social engineering and technical attacks," the FBI wrote in a Private Industry Notification (PIN) sent out on September 17.

Click link above to read more

The case for making political parties follow the same privacy rules as corporations

https://www.cbc.ca/news/technology/federal-elections-political-parties-apps-voter-data-privacy-rules-1.5306267

Though it's a topic the major parties don't seem too interested in discussing, the use of mobile apps as a key part of campaigning raises some important questions: What data is being collected? How is it being analyzed? And where is it being shared?

Given how voter data has been misused and manipulated in recent elections around the world, some experts wonder why there isn't more scrutiny of how Canada's political parties use the information they collect.

Click link above to read more

Getting a new mobile number in China will involve a facial-recognition test

https://qz.com/1720832/china-introduces-facial-recognition-step-to-get-new-mobile-number/

China is taking every measure it can to verify the identities of its over 850 million mobile internet users.

From Dec. 1, people applying for new mobile and data services will have to have their faces scanned by telecom providers, the Ministry of Industry and Information Technology said in a Sept. 27 statement (link in Chinese).

Click link above to read more

A lack of physical security still leads to data breaches but is being ignored, says study from Shred-It and Ponemon Institute

https://www.itworldcanada.com/article/a-lack-of-physical-security-still-leads-to-data-breaches-but-is-being-ignored-says-study-from-shred-it-and-ponemon-institute/422545

Do strong cybersecurity practises prevent all data breaches? Not according to a new study from Shred-it and the Ponemon Institute.

The recent major data breaches in Canada have led many to put a lot more focus into cybersecurity for their companies, but the study from Shred-It outlines how a lack of physical security can also lead to data breaches and many people seem to have forgotten about it.

Click link above to read more

Muhstik Ransomware Victim Hacks Back, Releases Decryption Keys

https://www.bleepingcomputer.com/news/security/muhstik-ransomware-victim-hacks-back-releases-decryption-keys/

A victim of the Muhstik Ransomware has hacked back against his attackers and released close to 3,000 decryption keys for victims along with a free decryptor to get their files back.

Since the end of September, an attacker has been hacking into publicly exposed QNAP NAS devices and encrypting the files on them. This ransomware has been named Muhstik based on the .muhstik extension appended to encrypted files.

The attacker would then demand 0.09 bitcoins, or approximately $700 USD, for a victim to get their files back.

Click link above to read more

Check If You Are in the Sephora and StreetEasy Data Breaches

https://www.bleepingcomputer.com/news/security/check-if-you-are-in-the-sephora-and-streeteasy-data-breaches/

Data breach lookup site Have I Been Pwned has added the stolen data from the StreetEasy and Sephora data breaches to their engine so that users can check if their information was exposed.

According to HIBP, StreetEasy was hit with a data breach in June 2016 that disclosed the information for close to 1 million users. This information included email addresses, names, passwords, and usernames,

Click link above to read more

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:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC V8X 4S8

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca