November 5th, 2019

October is "Cybersecurity awareness" Month

Try our November quiz – The Humans of Security

Don't miss Security Day! - "The Humans of Security", Nov 20, 2019

This week's stories:

- **Privacy experts slam National Bank asking customers for their password at other banks**
- **Canadian, U.S. man admit trying to blackmail Uber, LinkedIn after data thefts**
- **CIRA strikes deals with Finland, Poland and New Zealand**
- **Desjardins revises data theft impact numbers, says 4.2 million affected**
- **Nunavut government rebuilding network after ransomware attack**
- **Researchers unearth malware that siphoned SMS texts out of telco's network**
- **This aggressive IoT malware is forcing Wi-Fi routers to join its botnet army**
- **Breaches at NetworkSolutions, Register.com, and Web.com**
- **Paradise ransomware: Now victims can get their files back for free with this decryption tool**
- **Facebook agrees to pay fine over Cambridge Analytica scandal**

Privacy experts slam National Bank asking customers for their password at other banks

https://www.cbc.ca/news/canada/nova-scotia/national-bank-canada-customer-banking-privacy-1.5334059

It's the mantra virtually everyone has heard from privacy experts, their banks and anti-fraud investigators: Never give anyone your banking passwords or access to your online accounts.

Paul Kaminsky has heard it many times, too, and that's why the Edmonton resident couldn't believe it when he was asked to provide his account number and password from another bank as he tried to open a new online account with National Bank of Canada.

Click link above to read more

Canadian, U.S. man admit trying to blackmail Uber, LinkedIn after data thefts

https://www.itworldcanada.com/article/canadian-u-s-man-admit-trying-to-blackmail-uber-linkedin-after-data-thefts/423454

Two men are facing prison this week for pleading guilty to blackmailing Uber and trying to extort LinkedIn after stealing millions of customer records and holding them ransom.

Vasile Mereacre of Toronto and Brandon Charles Glover, of Winter Springs, Fla., admitted that during a four-month period starting in October 2016, they partnered to use stolen log-in credentials to gain access to confidential corporate databases being stored on Amazon Web Services.

Click link above to read more

CIRA strikes deals with Finland, Poland and New Zealand

https://www.itworldcanada.com/article/cira-strikes-deals-with-finland-poland-and-new-zealand/423511

The Canadian Internet Registration Authority is broadening its security product partnerships to providers in Finland, New Zealand and Poland.

CIRA said Thursday it has signed deals with Traficom (Finland), InternetNZ (New Zealand) and NASK (Poland) to use or resell its global registry and cybersecurity solutions for protecting domain name system (DNS) infrastructure.

Click link above to read more

Desjardins revises data theft impact numbers, says 4.2 million affected

https://www.ctvnews.ca/canada/desjardins-revises-data-theft-impact-numbers-says-4-2-million-affected-1.4666066

MONTREAL -- The Desjardins Group data theft is much more widespread than first thought and actually hit 4.2 million members, the banking co-operative's chief executive said Friday.

Guy Cormier told a news conference the revised number -- which represents the entirety of the Levis, Que.-based organization's membership -- were victims.

Desjardins Group initially reported in June that 2.9 million customers had been impacted by the theft -- 2.7 million individuals and 173,000 businesses in Ontario and Quebec.

Click link above to read more

Nunavut government rebuilding network after ransomware attack

https://www.cbc.ca/news/canada/north/nunavut-government-ransomware-attack-1.5347208

The government of Nunavut is rebuilding its communications network after a ransomware attack encrypted its files.

All Word documents and PDF files the virus had access to are encrypted and unreadable by the government, according to Martin Joy, Nunavut's director of information, communications and technology.

Click link above to read more

Researchers unearth malware that siphoned SMS texts out of telco’s network

https://arstechnica.com/information-technology/2019/10/researchers-unearth-malware-that-siphoned-sms-texts-out-of-telcos-network/

Nation-sponsored hackers have a new tool to drain telecom providers of huge amounts of SMS messages at scale, researchers said.

Dubbed "Messagetap" by researchers from the Mandiant division of security firm FireEye, the recently discovered malware infects Linux servers that route SMS messages through a telecom’s network. Once in place, Messagetap monitors the network for messages containing either a preset list of phone or IMSI numbers or a preset list of keywords.

Messages that meet the criteria are then XOR encoded and saved for harvesting later. FireEye said it found the malware infecting an undisclosed telecom provider. The company researchers said the malware is loaded by an installation script but didn't otherwise explain how infections take place.

Click link above to read more

This aggressive IoT malware is forcing Wi-Fi routers to join its botnet army

https://www.zdnet.com/article/this-aggressive-iot-malware-is-forcing-wi-fi-routers-to-join-its-botnet-army/

Tens of thousands of Wi-Fi routers are potentially vulnerable to an updated form of malware that takes advantage of known vulnerabilities to rope these devices into a botnet for the purposes of selling distributed denial of service (DDoS) attack capabilities to cyber criminals.

Click link above to read more

Breaches at NetworkSolutions, Register.com, and Web.com

https://krebsonsecurity.com/2019/10/breaches-at-networksolutions-register-com-and-web-com/

"On October 16, 2019, Web.com determined that a third-party gained unauthorized access to a limited number of its computer systems in late August 2019, and as a result, account information may have been accessed," Web.com said in a written statement. "No credit card data was compromised as a result of this incident."

Jacksonville, Fla.-based Web.com said the information exposed includes "contact details such as name, address, phone numbers, email address and information about the services that we offer to a given account holder."

Click link above to read more

Paradise ransomware: Now victims can get their files back for free with this decryption tool

https://www.zdnet.com/article/paradise-ransomware-now-victims-can-get-their-files-back-for-free-with-this-decryption-tool/

Victims of Paradise ransomware can now retrieve their files without giving into the demands of cyber criminals thanks to a newly released decryption tool. Researchers at cybersecurity company Emsisoft have released a free decryption tool for Paradise – a ransomware sold 'as-a-service' on the dark web which has been locking the networks of victims and holding them for ransom since September 2017.

Click link above to read more

Facebook agrees to pay fine over Cambridge Analytica scandal

https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal

Facebook has agreed to pay a £500,000 fine, the highest possible, to the Information Commissioner's Office over the Cambridge Analytica scandal, ending more than a year of litigation between the regulator and social network.

Click link above to read more

---

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:

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