November 12th, 2019

Try our November quiz – The Humans of Security

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

This week's stories:

- **Twenty-eight million Canadians hit by data breaches – report**
- **Police warn of new 'SIM swapping' scam that could empty your bank accounts**
- **Google's secret cache of medical data includes names and full details of millions – whistleblower**
- **WhatsApp hack led to targeting of 100 journalists and dissidents**
- **Apple resumes human reviews of Siri audio with iPhone update**
- **Play store apps to be scanned for malware**
- **Is enough being done to combat cybercrimes?**
- **Understanding the Ripple Effect: Large Enterprise Data Breaches Threaten Everyone**

Twenty-eight million Canadians hit by data breaches – report

https://www.insurancebusinessmag.com/ca/news/cyber/twentyeight-million-canadians-hit-by-data-breaches--report-191332.aspx

The Office of the Privacy Commissioner of Canada (OPC) has published the results of its assessment of the various data breach incidents that have occurred over the past year, noting that tens of millions of individuals' private data have been compromised.

Based on data the OPC gathered from reports by private sector firms, the commissioner revealed in its assessment that over the past 12 months, about 28 million Canadians were affected by a data breach incident. In total, there were 680 breach reports for the year ending October 31, 2019.

Click link above to read more

Police warn of new 'SIM swapping' scam that could empty your bank accounts

https://toronto.ctvnews.ca/police-warn-of-new-sim-swapping-scam-that-could-empty-your-bank-accounts-1.4678110

TORONTO -- Ontario residents are being warned of a new scam called "SIM swapping" that allows fraudsters to steal your personal information and even empty your bank accounts.

The Ontario Provincial Police (OPP) said through the scam, fraudsters have the potential to access your social media accounts, calendar, contacts and money. Police said scammers can even apply for credit in your name or impersonate you to defraud your entire contact list.

Click link above to read more

Google's secret cache of medical data includes names and full details of millions – whistleblower

https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information

A whistleblower who works in Project Nightingale, the secret transfer of the personal medical data of up to 50 million Americans from one of the largest healthcare providers in the US to Google, has expressed anger to the Guardian that patients are being kept in the dark about the massive deal.

The anonymous whistleblower has posted a video on the social media platform Daily Motion that contains a document dump of hundreds of images of confidential files relating to Project Nightingale. The secret scheme, first reported by the Wall Street Journal, involves the transfer to Google of healthcare data held by Ascension, the second-largest healthcare provider in the US. The data is being transferred with full personal details including name and medical history and can be accessed by Google staff. Unlike other similar efforts it has not been made anonymous though a process of removing personal information known as de-identification.

Click link above to read more

WhatsApp hack led to targeting of 100 journalists and dissidents

https://www.ft.com/content/67a5b442-f971-11e9-a354-36acbbb0d9b6

At least 100 journalists, human rights activists and political dissidents had their smartphones attacked by spyware that exploited a vulnerability in WhatsApp, according to the Facebook-owned messaging service.

The victims of the attack, which was first revealed by the Financial Times in May, were contacted by WhatsApp on Tuesday.

Their phones were targeted through WhatsApp's call function by customers of the Israel-based NSO Group, which makes Pegasus, a spyware program. Once installed, Pegasus is designed to take over all of a phone's functions.

WhatsApp told the FT it is filing a lawsuit in a US court that attributes the hack of its service to NSO. "This is the first time that an encrypted messaging provider is taking legal action against a private entity that has carried out this type of attack," WhatsApp said.

Click link above to read more

Apple resumes human reviews of Siri audio with iPhone update

https://www.ctvnews.ca/sci-tech/apple-resumes-human-reviews-of-siri-audio-with-iphone-update-1.4660772

Apple is resuming the use of humans to review Siri commands and dictation with the latest iPhone software update.

In August, Apple suspended the practice and apologized for the way it used people, rather than just machines, to review the audio.

While common in the tech industry, the practice undermined Apple's attempts to position itself as a trusted steward of privacy. CEO Tim Cook repeatedly has declared the company's belief that "privacy is a fundamental human right," a phrase that cropped up again in Apple's apology.

Click link above to read more

Play store apps to be scanned for malware

https://www.bbc.com/news/technology-50375579

Google is beefing up the way it checks if any of the apps uploaded to its Play store are malicious.

All new apps will be scanned by malware-spotting tools from three cyber-security companies as well as Google's own in-house system.

Google said it needed help because the number of apps being uploaded was too large for it to handle alone.

Nasty Play apps can hit lots of people. Malicious code found in June was in apps downloaded 400 million times.

Click link above to read more

Is enough being done to combat cybercrimes?

https://www.aljazeera.com/programmes/insidestory/2019/10/combat-cybercrimes-191029190702030.html

Cyberattacks are now one of the biggest concerns for governments and companies across the world. In the past year alone, there has been an 11 percent increase in security breaches by hackers.

These growing figures show just how big a threat cybercrime has become.

With security experts fighting the hackers, the cybercrime economy is growing so quickly, it is now making profits of $1.5 trillion each year A recent Microsoft survey suggests executives now consider cyberattacks to be the top threat to their businesses.

Click link above to read more

Understanding the Ripple Effect: Large Enterprise Data Breaches Threaten Everyone

https://threatpost.com/ripple-effect-large-enterprise-data-breaches/150041/

Big businesses are constantly under attack, and that affects everyone from customers and business partners to parties with national security interests.

When successful, the initial compromise is only a means to an end — the real goal is to mount follow-on attacks like spearphishing, extortion attempts and account takeover (ATO). And much to the chagrin of security experts, those attacks on household-name companies are growing. Last year saw more than 6,500 data breaches, exposing a staggering 5 billion compromised records, according to Risk Based Security.

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