November 19th, 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:

- **32 arrested at Indian call centre that targeted Canadians**
- **Ontario's Grey County realizes disaster recovery is not a business continuity plan**
- **More collaboration needed to improve national cyber resilience, says Bank of Canada exec**
- **Here's Why The Google Fitbit Deal Matters–And What You Should Do**
- **Macy's Customer Payment Info Stolen in Magecart Data Breach**
- **Senator Raises Concerns Over Insider Breach at Twitter**
- **Two Charged Over Crypto Theft via SIM Swapping, Death Threats**
- **Compromised Website Led to Australia Parliament Hack**
- **New Threat Actor Impersonates Govt Agencies to Deliver Malware**

---

32 arrested at Indian call centre that targeted Canadians

https://www.ctvnews.ca/world/32-arrested-at-indian-call-centre-that-targeted-canadians-1.4690651?taid=5dd311161dd1a30001b96439&utm_campaign=trueAnthem%3A+Trending+Content&utm_medium=trueAnthem&utm_source=twitter

TORONTO – Indian authorities say they have shut down a call centre where dozens of people tried to dupe Canadians into handing over money through a phone scam involving social insurance numbers.

Sameer Sharma, a deputy police commissioner in New Delhi, said in a statement that the "swanky international scam call centre targeting Canadian citizens" first came to the attention of police on Friday.

Click link above to read more

Ontario's Grey County realizes disaster recovery is not a business continuity plan

https://www.itworldcanada.com/article/ontario-county-realizes-disaster-recovery-is-not-a-business-continuity-plan/424004

Like many municipalities, Ontario's Grey County had a disaster recovery plan. Or thought it did.

Actually, admits Jody MacEachern, the county's manager of information technology, it was "a really old document that was developed, stapled sat on a shelf. Everything in that document was out of date."

And, he added, if IT couldn't recover data needed from a backup it wasn't going to be restored.

Click link above to read more

More collaboration needed to improve national cyber resilience, says Bank of Canada exec

https://www.itworldcanada.com/article/more-collaboration-needed-to-improve-national-cyber-resilience-says-bank-of-canada-exec/423916

More candid threat sharing between companies and governments is needed to help protect critical infrastructure and residents from cyber-attacks, said experts, including a senior official of the Bank of Canada, at a meeting on Tuesday with the Information Technology Association of Canada (ITAC).

Click link above to read more

Here's Why The Google Fitbit Deal Matters–And What You Should Do

https://www.forbes.com/sites/kateoflahertyuk/2019/11/17/heres-why-the-google-fitbit-deal-mattersand-what-you-should-do/#67af755f2abc

Google is in the process of buying Fitbit for $2.1 billion, and the move is making many people feel very uncomfortable. On November 17, CNBC reported that some Fitbit users had started looking for an alternative as soon as they heard about Google's plans to acquire the firm.

Citing concerns about privacy, many were considering the Apple Watch as a safer option than their Fitbit. This is despite the fact that Google explicitly stated in its announcement that it would not sell people's personal or health information.

Click link above to read more

Macy's Customer Payment Info Stolen in Magecart Data Breach

https://www.bleepingcomputer.com/news/security/macys-customer-payment-info-stolen-in-magecart-data-breach/

Macy's has announced that they have suffered a data breach due to their web site being hacked with malicious scripts that steal customer's payment information.

This type of compromise is called MageCart attack and consists of hackers compromising a web site so that they can inject malicious JavaScript scripts into various sections of the web site. These scripts then steal payment information that is submitted by a customer.

Click link above to read more

Senator Raises Concerns Over Insider Breach at Twitter

https://www.databreachtoday.com/senator-raises-concerns-over-insider-breach-at-twitter-a-13413

U.S. Sen. Bob Menendez, D-N.J., is raising national security, user privacy and other concerns about the recent insider breach at Twitter and what role Saudi Arabia is playing in manipulating American tech firms to crackdown on dissidents.

In separate letters to Twitter CEO Jack Dorsey and the U.S. State Department, Menendez, who is the ranking Democrat on the Senate Foreign Relations Committee, raises questions about failures to prevent infiltration attempts by two former Twitter employees who spied on critics of the Saudi government and the country's royal family.

Click link above to read more

Two Charged Over Crypto Theft via SIM Swapping, Death Threats

https://www.bleepingcomputer.com/news/security/two-charged-over-crypto-theft-via-sim-swapping-death-threats/

Two men from Massachusetts were arrested and charged by the Boston U.S. District Court with stealing high-value social media accounts and hundreds of thousands worth of cryptocurrency from at least ten victims by using SIM swapping, death threats, and hacking.

Eric Meiggs and Declan Harrington, the two defendants, were charged with one count of conspiracy, eight counts of wire fraud, one count of computer fraud and abuse, and one count of aggravated identity theft in an 11-count indictment unsealed today.

Click link above to read more

Compromised Website Led to Australia Parliament Hack

https://www.databreachtoday.com/compromised-website-led-to-australia-parliament-hack-a-13412

The Australian Parliament's computer network was compromised in January after politicians browsed a legitimate website that was compromised.

Sen. Scott Ryan, president of the Senate, revealed the style of attack, which hadn't been discussed before, on Thursday during a hearing of the Finance and Public Administration Legislation Committee. A transcript of the hearing is posted on Parliament's website.

Click link above to read more

New Threat Actor Impersonates Govt Agencies to Deliver Malware

https://www.bleepingcomputer.com/news/security/new-threat-actor-impersonates-govt-agencies-to-deliver-malware/

A new threat actor is using email to impersonate government agencies in the United States, Germany, and Italy to deliver ransomware, backdoors, and banking Trojans through malicious attachments.

Since the end of October, Proofpoint researchers detected a new threat actor who has been impersonating the United States Postal Service, the German Federal Ministry of Finance, and the Italian Revenue Agency in malicious spam campaigns that deliver a variety of malware.

Click link above to read more

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