Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

October 8th, 2018

October is "Cybersecurity awareness" Month
Test yourself with the Cybersecurity Awareness Month Quiz: Cybersecurity by the Numbers

This week's stories:

- Canadian companies are overconfident when it comes to cyberattacks, study finds
- More than a dozen federal departments flunked a credit card security test
- Canadian Centre for Cyber Security opens, to be focus for federal safety efforts
- Google+ Shutting Down After Bug Leaks Info of 500k Accounts
- Facebook hit with Canadian class-action lawsuit after massive security breach
- Canadian restaurant chain suffers country-wide outage after malware outbreak
- Heathrow Airport Fined £120,000 for Lost USB Storage Drive
- Dutch and British Governments Slam Russia for Cyberattacks
- Tesco Bank Hit With £16 Million Fine Over Debit Card Fraud
- California to Ban Weak Passwords

Canadian companies are overconfident when it comes to cyberattacks, study finds

https://www.msn.com/en-ca/news/canada/canadian-companies-are-overconfident-when-it-comes-to-cyberattacks-study-finds/ar-BBNXiYV

Canadian companies tend to be overconfident or unprepared to protect sensitive information from data breaches — mostly because they have an incomplete or inadequate picture about the evolving challenges they face, according to cybersecurity experts.

A study conducted by Ovum for FICO — a California-based data analytics company that operates a global fraud detection system for banks, credit card companies and others — found 84 per cent of Canadian executives surveyed felt their organization was "better than average" or a "top performer."

Click link above to read more

More than a dozen federal departments flunked a credit card security test

https://www.cbc.ca/news/politics/security-data-shared-services-it-1.4848688

The Canada Revenue Agency, the RCMP, Statistics Canada and more than a dozen other federal departments and agencies have failed an international test of the security of their credit card payment systems.

Altogether, half of the 34 federal institutions authorized by the banking system to accept credit-card payments from citizens and others have flunked the test — risking fines and even the revocation of their ability to accept credit and debit payments.

Those 17 departments and agencies continue to process payments on Visa, MasterCard, Amex, the Tokyo-based JCB and China UnionPay cards, and federal officials say there have been no known breaches to date.

Click link above to read more

Canadian Centre for Cyber Security opens, to be focus for federal safety efforts

https://www.itworldcanada.com/article/canadian-centre-for-cyber-security-opens-to-be-focus-for-federal-safety-efforts/409452

The country's new consolidated cyber security hub opens today, promising better government co-operation with the private sector on threat analysis and security issues as well as more efficient help to all federal departments.

Perhaps fittingly, the Canadian Cyber Security Centre, announced in the federal budget seven months ago, begins with the start of the annual international Cyber Security Awareness Month.

Among the centre's mandates is to provide Canadian citizens and businesses with a one-stop place to turn to for cyber security information, both online and in person. It will also be a place where the private sector can come for advice and to test products they want to sell to Ottawa as well as commercially.

Click link above to read more

Google+ Shutting Down After Bug Leaks Info of 500k Accounts

https://www.bleepingcomputer.com/news/security/google-shutting-down-after-bug-leaks-info-of-500k-accounts/

Google has announced that they are closing the consumer functionality of Google+ due lack of adoption and an API bug that leaked the personal information of up to 500,000 Google+ accounts.

While no evidence was found that indicates this bug was ever misused, it was determined that the complexity of protecting and operating a social network like Google+ was not a worthwhile endeavor when so few users actually used the service for any length of time.

Click link above to read more

Facebook hit with Canadian class-action lawsuit after massive security breach

https://business.financialpost.com/technology/personal-tech/facebook-hit-with-class-action-lawsuit-after-massive-security-breach

A class-action lawsuit has been proposed in Canada against Facebook following a security breach that put the accounts of tens of millions of users at risk.

The social media company announced last week that about 50 million user accounts worldwide had been accessed by hackers, with another 40 million left vulnerable during the attack.

Click link above to read more

Canadian restaurant chain suffers country-wide outage after malware outbreak

https://www.zdnet.com/article/restaurant-chain-suffers-canada-wide-outage-after-malware-outbreak/

A Canadian restaurant chain that operates over 20 restaurant brands has suffered a country-wide outage of its IT systems over the weekend in an incident it described as a "malware outbreak."

The company is Recipe Unlimited --formerly Cara Operations-- which operates restaurant brands in North American, but mostly in Canada.

The mysterious malware outbreak happened last Friday, September 28. Not all restaurants were affected, but only those operating under brands such as Swiss Chalet, Harvey's, Milestones, Kelseys, Montana's, Bier Markt, East Side Mario's, The Landing Group of Restaurants, and Prime Pubs, according to a press release the company shared with ZDNet.

Click link above to read more

Heathrow Airport Fined £120,000 for Lost USB Storage Drive

https://www.databreachtoday.com/heathrow-airport-fined-120000-for-lost-usb-storage-drive-a-11588

The U.K.'s largest airport has been slammed by the country's privacy watchdog for a series of missteps that led to a USB memory drive containing highly sensitive information being lost on a London city street, where it was found by a passerby.

On Monday, the Information Commissioner's Office announced that it was fining Heathrow Airport Limited £120,000 ($155,000) under the Data Protection Act 1998, which was in effect at the time of the breach.

Click link above to read more

Dutch and British Governments Slam Russia for Cyberattacks

https://www.databreachtoday.com/dutch-british-governments-slam-russia-for-cyberattacks-a-11584

The British and Dutch governments have issued a strong rebuke to the Russian government over an ongoing series of hack attacks that they say were launched by the Russian Main Intelligence Directorate, aka the GRU.

The military intelligence agency has been tied to attacks that researchers have previously attributed to a group called APT28 or Fancy Bear.

The U.K.'s National Cyber Security Center, which is attached to the country's GCHQ intelligence agency, says the GRU's hacking operations are associated with - and known as - APT 28 and Fancy Bear. The group is also known as: BlackEnergy Actors, Cyber Berkut, CyberCaliphate, Pawnstorm, Sandworm, Sednit, Sofacy, Strontium, Tsar Team and Voodoo Bear.

Click link above to read more

Tesco Bank Hit With £16 Million Fine Over Debit Card Fraud

https://www.databreachtoday.com/tesco-bank-hit-16-million-fine-over-debit-card-fraud-a-11577

Scotland-based Tesco Bank has been hit with a £16.4 million ($21.3 million) fine by the U.K.'s Financial Conduct Authority for failing to proactively deal with "foreseeable risks" that led to hackers executing a successful online attack campaign.

The attacks, in November 2016, lasted for 48 hours and led to hackers stealing £2.26 million ($2.93 million), says the Financial Conduct Authority, the U.K.'s financial regulatory body that operates independently of the U.K. government.

Click link above to read more

California to Ban Weak Passwords

https://www.securityweek.com/california-ban-weak-passwords

The state of California recently passed a bill that requires the manufacturers of connected devices to use unique hardcoded passwords for each device manufactured.

The bill, meant to combat the widespread use of weak passwords in connected devices such as Internet of Things (IoT) products, also demands that manufacturers implement a security feature in their devices to require users to select new means of authentication upon first use.

The use of weak passwords in connected devices is a well-known security issue that has fueled a broad range of cyber-attacks, including the emergence of numerous, large IoT botnets.

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