Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

February 5th, 2019

February is Cyberbullying Month

Watch out for the 20th Annual Privacy and Security Conference from Feb.6th to 8th.

This week's stories:

- **Chief electoral officer worries parties are weak link in cybersecurity chain**
- **Industrial Internet Consortium, OpenFog group officially merge**
- **Google Launches Password Checkup Extension to Alert Users of Data Breaches**
- **Huddle House Fast Food Chain Suffers Data Breach in POS System**
- **Houzz Break-In: Data Breach Announced**
- **New Scam Holds YouTube Channels for Ransom**
- **Hackers targeted universities with phishing attacks**
- **Officer jailed for using police database to access personal details of dozens of Tinder dates**
- **Student Loan Company Fought Off 1 Million Cyberattacks in a Year**
- **Hackers hit Airbus, steal personal details of employees**

Chief electoral officer worries parties are weak link in cybersecurity chain

https://www.cbc.ca/news/politics/electoral-officer-parties-cybersecurity-1.5006055

anada's chief electoral officer is "pretty confident" that Elections Canada has good safeguards to prevent cyberattacks from robbing Canadians of their right to vote in this year's federal election.

But Stephane Perrault is worried that political parties aren't so well equipped.

"They don't have access to the resources we have access to," Perrault said in an interview Monday, noting that "securing [computer] systems is quite expensive... Even the larger parties have nowhere near our resources and you've got much smaller parties with very little resources."

Click link above to read more

Industrial Internet Consortium, OpenFog group officially merge

https://www.itworldcanada.com/article/industrial-internet-consortium-openfog-group-officially-merge/414781

Two industry associations aimed at accelerating the Internet of Things are officially pooling their resources.

The Industrial Internet Consortium, formed to create standards for trustworthy IIoT systems and devices, is folding in members of the OpenFog Consortium, which is pushing a new architecture embracing the Internet of things and 5G communications with distributed computing.

Click link above to read more

Google Launches Password Checkup Extension to Alert Users of Data Breaches

https://www.bleepingcomputer.com/news/security/google-launches-password-checkup-extension-to-alert-users-of-data-breaches/

Google announced the release of the Password Checkup Chrome extension designed to keep an eye on current data breaches and announce its users if their accounts have been impacted by recent security breaches.

While Google already resets passwords of user accounts who might have been affected by third-party breaches as part of an effort to limit the potential security impact on its users' accounts, this feature is limited only to Google accounts.

Click link above to read more

Huddle House Fast Food Chain Suffers Data Breach in POS System

https://www.bleepingcomputer.com/news/security/huddle-house-fast-food-chain-suffers-data-breach-in-pos-system/

Fast food restaurant chain Huddle House has disclosed that they were affected by a data breach in the point of sale system at some locations that allowed attackers to steal payment information.

According to a security notification released on February 1st, point of sale systems at various Huddle House locations were infected with malware that allowed attackers to steal credit card information that used to purchase food at the restaurant.

Click link above to read more

Houzz Break-In: Data Breach Announced

https://www.bleepingcomputer.com/news/security/houzz-break-in-data-breach-announced/

The home improvement site Houzz announced a data breach this week involving third-parties gaining access to a file that contains publicly visible user data as well as private account information.

In an email sent to affected users, Houzz stated that an unauthorized third-party gained access to a file containing both publicly available information as well as internal account information such as user IDs, email address, one-way encrypted passwords, IP addresses, city and zip codes derived from IP addresses, and Facebook information.

Click link above to read more

New Scam Holds YouTube Channels for Ransom

https://www.bleepingcomputer.com/news/security/new-scam-holds-youtube-channels-for-ransom/

Scammers are abusing the YouTube policy violation system by filing fake copyright infringements against content creators until their channel is close to being suspended. These scammers then hold the channel ransom by telling YouTubers to send them a payment or they will file another copyright infringement to have the channel suspended.

YouTube has a policy infringement system where users can report a video that they feel breaks policies such as sexual content or nudity, hateful content, violent or graphic content, or copyright infringement. When a video receives a policy violation report, it will be reviewed if it's deemed to be a violation, YouTube will issue a strike against the video owner's account and remove the video.

Click link above to read more

Hackers targeted universities with phishing attacks

https://www.databreaches.net/hackers-targeted-universities-with-phishing-attacks/

Two men who were citizens of Nigeria, living in Malaysia, and conducting their crimes from behind computers likely assumed they were safe from the reach of American law enforcement when they hacked into university computer systems to steal paychecks and tax returns.

But through strong partnerships with the Georgia Institute of Technology (Georgia Tech), the Department of Justice, and Malaysian authorities, the FBI was able to identify, arrest, and extradite Olayinka Olaniyi and Damilola Soloman Ibiwoye to face charges of conspiracy to commit wire fraud, computer fraud, and aggravated identity theft.

Click link above to read more

Officer jailed for using police database to access personal details of dozens of Tinder dates

https://www.databreaches.net/au-officer-jailed-for-using-police-database-to-access-personal-details-of-dozens-of-tinder-dates/

A former long-serving police officer has been jailed for six months for illegally accessing the personal details of almost 100 women to determine if they were “suitable” dates.

Adrian Trevor Moore was a 28-year veteran of WA Police and was nominated as police officer of the year in 2011.

The former senior constable pleaded guilty to 180 charges of using a secure police database to access the information of 92 women he had met, or interacted with, on dating websites including Tinder and Plenty of Fish.

Click link above to read more

Student Loan Company Fought Off 1 Million Cyberattacks in a Year

https://hotforsecurity.bitdefender.com/blog/student-loan-company-fought-off-1-million-cyberattacks-in-a-year-20806.html

The financial services industry registered three times more security incidents than any other industry in 2018. According to data released under Freedom of Information legislation, UK government organization The Student Loans Company (SLC) experienced close to a million cyberattacks in the 2017 – 2018 fiscal year. The information was made public upon written request from the Parliament Street think tank.

While most attacks were categorized as malware (323), Denial-of-Service, and malicious emails or calls (235), they all failed, except for a cryptojacking attack. Manipulating a third-party plugin, hackers injected Monero mining software into the company’s network. This was attributed to third-party incidents.

Click link above to read more

Hackers hit Airbus, steal personal details of employees

https://hotforsecurity.bitdefender.com/blog/hackers-hit-airbus-steal-personal-details-of-employees-20798.html

Aircraft manufacturer Airbus is investigating a security breach that has seen hackers steal personal information from its systems.

In a statement published on its website, Airbus admitted that systems used by its commercial aircraft business had been accessed by an unauthorised party, and personal data related to European employees had been stolen.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors 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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.