Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer

April 30th, 2019

Try our April quiz - Spotting a Fake

This week's stories:

Evaluate suppliers for cyber risk, Canadian manufacturers told 🇨🇦

Canada Says Facebook Violated Privacy Laws 🇨🇦

How Avengers: Endgame can teach us about quantum computing's threat to encryption

Breaches, ID Theft & Malware: Schools At Risk From Vulnerabilities

Docker Hub Database Hack Exposes Sensitive Data of 190K Users

Cybercrime's Total Earnings Skyrocketed to $2.7 Billion Says the FBI

A cyber-attack in Japan could now bring the US into war

Millions using 123456 as password, security study finds

Apple defends removing parental control apps

Facebook now says its password leak affected 'millions' of Instagram users

---

Evaluate suppliers for cyber risk, Canadian manufacturers told 🇨🇦

https://www.itworldcanada.com/article/evaluate-suppliers-for-cyber-risk-canadian-manufacturers-told/417362

Few Canadian manufacturers make every part of their products. Instead, they rely on a large number of suppliers. But criminals and nation states also see those third-party suppliers as a big opportunity to slip into the computer systems of manufacturers, and from there get into the bigger companies manufacturers sell to.

Click link above to read more

Canada says Facebook broke privacy laws in Cambridge Analytica scandal🇨🇦

https://www.engadget.com/2019/04/25/canada-facebook-privacy-laws-cambridge-analytica/

Facebook is facing yet more legal trouble over the Cambridge Analytica scandal after Canada's privacy commissioner said it violated federal and provincial privacy laws. Daniel Therrien plans to take the company to federal court in the hopes of forcing Facebook to change its privacy policies.

Click link above to read more

How Avengers: Endgame can teach us about quantum computing's threat to encryption

https://www.itworldcanada.com/article/how-avengers-endgame-can-teach-us-about-quantum-computings-threat-to-encryption/417338

At some point in the future, someone with bad intentions is going to figure out how to use technology to transport back in time and steal all of your secrets.

Well, that's almost true. When quantum computing is solved, it will be capable of cracking algorithms used for encryption today. As a result, CIOs have to start thinking about how to encrypt their data against this future threat today. Otherwise, a well-planned attack might steal that encrypted data today, stowing it away to decrypt in the future to attain the desired information.

Click link above to read more

Breaches, ID Theft & Malware: Schools At Risk From Vulnerabilities

https://www.bleepingcomputer.com/news/security/breaches-id-theft-and-malware-schools-at-risk-from-vulnerabilities/

Recently, Scott County Schools, in Kentucky, fell victim to a $3.7 million fraud phishing scam. According to Superintendent Dr. Kevin Hub, a vendor informed the district that an invoice sent to the district had not been paid. In looking into the matter, the district found that someone else had been paid instead, via a fraudulent email disguised as the vendor. "This is a process that we use currently in Scott County Schools. It's a way that we pay our vendors. And it was in this specific case, a single case, that we can verify, and this fraudulent email and fraudulent documentation is what caused this crime to happen."

Click link above to read more.

Docker Hub Database Hack Exposes Sensitive Data of 190K Users

https://www.bleepingcomputer.com/news/security/docker-hub-database-hack-exposes-sensitive-data-of-190k-users/

An unauthorized person gained access to a Docker Hub database that exposed sensitive information for approximately 190,000 users. This information included some usernames and hashed passwords, as well as tokens for GitHub and Bitbucket repositories.

According to a security notice sent late Friday night, Docker became aware of unauthorized access to a Docker Hub database on April 25th, 2019.

Click link above to read more

Cybercrime's Total Earnings Skyrocketed to $2.7 Billion Says the FBI

https://www.bleepingcomputer.com/news/security/cybercrimes-total-earnings-skyrocketed-to-27-billion-says-the-fbi/

FBI's Internet Crime Complaint Center (IC3) published its 2018 Internet Crime Report which shows that cybercrime was behind $2,7 billion in total losses during 2018 as shown by 351,936 complaints received during the last year.

Since its inception in May 2000, IC3 says that it has received 4,415,870 complaints, with an average of around 300,000 complaints each year and roughly 900 per day. These resulted in a total loss of $7.45 billion over the last five years, between 2014 and 2018.

Click link above to read more

A cyber-attack in Japan could now bring the US into war

https://qz.com/1600574/a-cyber-attack-in-japan-could-now-bring-the-us-into-war/

In a briefing yesterday in Washington, DC, US secretary of state Mike Pompeo declared that “a cyberattack could, in certain circumstances, constitute an armed attack under Article 5 of the US-Japan Security Treaty.” The security agreement, ratified after World War II, guarantees the United States’ defense in the event of an attack on Japan.

Click link above to read more

Millions using 123456 as password, security study finds

https://www.bbc.com/news/technology-47974583

Millions of people are using easy-to-guess passwords on sensitive accounts, suggests a study.

The analysis by the UK's National Cyber Security Centre (NCSC) found 123456 was the most widely-used password on breached accounts.

The study helped to uncover the gaps in cyber-knowledge that could leave people in danger of being exploited.

Click link above to read more

Apple defends removing parental control apps

https://www.bbc.com/news/technology-48092151

Apple has defended its decision to remove a number of parental control apps from the App Store, citing security concerns.

Several app-makers complained to the New York Times that Apple had taken their products off sale when it launched its own similar tools.

Click link above to read more

Facebook now says its password leak affected ‘millions’ of Instagram users

https://techcrunch.com/2019/04/18/instagram-password-leak-millions/

Facebook has confirmed its password-related security incident last month now affects “millions” of Instagram users, not “tens of thousands” as first thought.

The social media giant confirmed the new information in its updated blog post, first published on March 21.

“We discovered additional logs of Instagram passwords being stored in a readable format,” the company said. “We now estimate that this issue impacted millions of Instagram users. We will be notifying these users as we did the others.”

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

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer