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

August 27th, 2019

Try our August quiz – Security While Traveling

This week's stories:

- **Canada's shift on strong encryption is 'irresponsible' says privacy group** 🇨🇦
- **What Canada is, and isn't, doing to prevent foreign interference** 🇨🇦
- **Cisco Patches Many Serious Vulnerabilities in Unified Computing Products**
- **Instagram Phishing Emails Use Fake Login Warning Baits**
- **Portland Public Schools Recovers $2.9 Million Lost in BEC Scam**
- **PokerTracker.com Hacked to Inject Payment Card Stealing Script**
- **Medical device cybersecurity will be rubbish for 20 more years**
- **Study says fintech startups vulnerable to web or mobile app attacks**
- **Data Security: Data hacked by Mastercard Bonus Program**
- **Microsoft: Using multi-factor authentication blocks 99.9% of account hacks**

Canada's shift on strong encryption is 'irresponsible' says privacy group 🇨🇦

https://www.itworldcanada.com/article/canadas-shift-on-strong-encryption-is-irresponsible-says-privacy-group/421054

A Canadian privacy watchdog this week said the federal government is wrong to change its policy by now urging technology companies to weaken encryption protection in products and services.

The move will put people and their data in danger, Citizen Lab said in a report issued Wednesday.

Click link above to read more

What Canada is, and isn't, doing to prevent foreign interference 🇨🇦

https://www.nationalmagazine.ca/en-ca/articles/law/in-depth/2019/what-canada-is-and-isn-t-doing-to-prevent-foreign

#TrudeauMustGo, or so the hashtag said, as it trended on Twitter some weeks ago. Was this a surge in public discontent? A poor omen for the Prime Minister? None of the above – the "trend" found its fuel in assorted "fake" accounts, masquerading as members of the public. It snowballed as legitimate accounts joined in.

The Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) have already found foreign actors attempting to influence Canada's upcoming federal election. As the Government of Canada's Canadian Centre for Cyber Security has predicted, foreign cyber interference ahead of and during the campaign is "very likely."

Click link above to read more

Cisco Patches Many Serious Vulnerabilities in Unified Computing Products

https://www.securityweek.com/cisco-patches-many-serious-vulnerabilities-unified-computing-products

Cisco informed customers on Wednesday that it has released patches for 17 critical and high-severity vulnerabilities affecting some of its Unified Computing products.

A majority of these vulnerabilities impact the Integrated Management Controller (IMC), which provides embedded server management capabilities for Cisco Unified Computing System (UCS) servers. Five of the security holes also impact UCS Director and UCS Director Express for Big Data, and one issue only affects UCS Director and UCS Director Express for Big Data.

Click link above to read more

Instagram Phishing Emails Use Fake Login Warning Baits

https://www.bleepingcomputer.com/news/security/instagram-phishing-emails-use-fake-login-warning-baits/

Instagram users are currently targeted by a new phishing campaign that uses login attempt warnings coupled with what looks like two-factor authentication (2FA) codes to make the scam more believable.

Crooks use phishing to trick potential victims into handing over sensitive information via fraudulent websites they control with the help of a wide range of social engineering techniques, as well as messages designed to look like they're sent by someone they know or a legitimate organization.

Click link above to read more

Portland Public Schools Recovers $2.9 Million Lost in BEC Scam

https://www.bleepingcomputer.com/news/security/portland-public-schools-recovers-29-million-lost-in-bec-scam/

Oregon urban school district Portland Public Schools is on track to recover roughly $2.9 million wired by district employees to a BEC scammer, after discovering the fraudulent transactions before the money left the fraudster's accounts.

Portland Public Schools is a PK-12 urban school district in Portland, Oregon, with over 49,000 students enrolled in 81 schools, and one of the largest ones in the Pacific Northwest.

BEC (also known as EAC, short for Email Account Compromise) fraud schemes are scams through which fraudsters attempt to trick one or more employees of a targeted organization into wiring them money.

Click link above to read more

PokerTracker.com Hacked to Inject Payment Card Stealing Script

https://www.bleepingcomputer.com/news/security/pokertrackercom-hacked-to-inject-payment-card-stealing-script/

A curious case of web-based card skimming activity revealed that the Poker Tracker website had been compromised and loaded a Magecart script - code that steals payment information from customers.

Online poker enthusiasts use the Poker Tracker software suite to improve their winning chances by making decisions based on statistics compiled from the opponents' gameplay.

Click link above to read more

Medical device cybersecurity will be rubbish for 20 more years

https://www.zdnet.com/article/medical-device-cybersecurity-will-be-rubbish-for-20-more-years/

"Everything with a power point is probably connected, or will be shortly," says Christopher Neal, chief information security officer (CISO) of Ramsay Health Care.

"Increasingly that connectivity is critical to patient care," he told the Gartner Security and Risk Management Summit in Sydney on Monday.

Even if those connected devices aren't transmitting patient medical data, increasingly they're conveying information about their own health.

Click link above to read more

Study says fintech startups vulnerable to web or mobile app attacks

https://www.itworldcanada.com/article/fintech-startups-vulnerable-to-web-or-mobile-app-attacks-vendor-study/421134

Financial technology startups like to boast that they are more nimble than their counterparts in the traditional banking world.

But if a test of their websites and mobile apps by a cybersecurity vendor is accurate, the startups aren’t necessarily better at protecting their applications.

The study released this week by ImmuniWeb is a follow-up to an identical one released last month that tested the websites and mobile apps of the world’s biggest financial institutions against the free version of the vendor’s tools.

Click link above to read more

Data Security: Data hacked by Mastercard Bonus Program

https://www.tellerreport.com/tech/2019-08-19---data-security--data-hacked-by-mastercard-bonus-program-.rkZPuvd4S.html

An online forum has published the data of thousands of users of a Mastercard bonus program. Including name, e-mail address and partly card numbers.

Due to a data leak, data from users of the Mastercard bonus program "Priceless Specials" from Germany have at times appeared in an online forum. A spreadsheet file includes, among other things, customer names and e-mail addresses. Next to it were the first two and the last four numbers of the Mastercard card numbers and in some cases the address and phone number of the credit card users.

Click link above to read more

Microsoft: Using multi-factor authentication blocks 99.9% of account hacks

https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/

Microsoft says that users who enable multi-factor authentication (MFA) for their accounts will end up blocking 99.9% of automated attacks.

The recommendation stands not only for Microsoft accounts but also for any other profile, on any other website or online service.

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.

Security News Digest
Information Security Branch

British Columbia OCIO | Office of the Chief Information Officer