Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

August 6th, 2019

Try our August quiz – Security While Traveling

This week's stories:

- **Poll suggests Canadians feel they lack control over private data** 🇨🇦
- **Canadians must avoid desensitization to data breaches and lobby for stronger penalties, cybersecurity experts say** 🇨🇦
- **Google reveals fistful of flaws in Apple's iMessage app**
- **Cybersecurity experts weigh in on Capital One breach**
- **Cyber Security Today – How to discover if your email has been hacked**
- **North Carolina County Lost $1.7 Million in BEC Scam**
- **US Govt, NGOs Ask Cyber Community to Boost Ransomware Defenses**
- **FBI Warns of Romance Scams Turning Victims into Money Mules**
- **North Korea cyber-attacks reap almost $3b for weapons programs, UN report says**
- **Financial services and e-payment firms in Singapore must follow new cyber hygiene rules from next August: MAS**

Poll suggests Canadians feel they lack control over private data 🇨🇦

https://www.itworldcanada.com/article/poll-suggests-canadians-feel-they-lack-control-over-private-data/420539

A majority of Canadians know their rights when it comes to privacy, but polling data suggests an equal number of them also feel powerless when it comes to how private businesses use their private data.

The polling report, commissioned by the Privacy Commissioner Daniel Therrien and released earlier this year, says "Most Canadians feel they have little to no control over how their personal information is being used by companies (67 per cent) or by government (61 per cent)."

Click link above to read more

Canadians must avoid desensitization to data breaches and lobby for stronger penalties, cybersecurity experts say 🇨🇦

https://www.itworldcanada.com/article/canadians-must-avoid-desensitization-to-data-breaches-and-lobby-for-stronger-penalties-cybersecurity-experts-say/420471

Cybersecurity experts are worried that the increased frequency of data breaches is becoming normalized by the public, reducing the pressure on organizations that handle private data to do better.

“It’s clear that this happens to many major companies, even those who invest heavily in security. I don’t want to say that it’s inevitable, because it’s not, but there is an aspect of frequency to this, that is really startling,” said Ira Goldstein, the chief operating officer at Herjavec Group, in an interview with *IT World Canada.* “I think there’s kind of a societal and philosophical angle to that where people are becoming quite desensitized to it.”

Click link above to read more

Google reveals fistful of flaws in Apple's iMessage app

https://www.bbc.com/news/technology-49165946?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story

A team of bug-hunters at Google have shared details of five flaws in Apple's iMessage software that could make its devices vulnerable to attack.

In one case, the researchers said the vulnerability was so severe that the only way to rescue a targeted iPhone would be to delete all the data off it.

Another example, they said, could be used to copy files off a device without requiring the owner to do anything to aid the hack.

Apple released fixes last week.

Click link above to read more

Cybersecurity experts weigh in on Capital One breach

https://www.itworldcanada.com/article/cybersecurity-experts-weigh-in-on-capital-one-breach/420548

This week’s news of the breach at Capital One Financial Corp. rocked the world and has cybersecurity experts buzzing to analyze what went wrong and advise others how to prevent similar issues at their own organizations.

Private information given to Capital One through credit applications were exposed in a hack that the authorities believe was perpetrated by Paige Thompson, a suspect who was quickly apprehended once Capital One reported the breach to the FBI. Roughly 100 million Americans and 6 million Canadians were impacted.

Click link above to read more

Cyber Security Today – How to discover if your email has been hacked

https://www.itworldcanada.com/article/cyber-security-today-how-to-discover-if-your-email-has-been-hacked/420245

Here are some tips on how to be safer online. Reputable companies invest a lot of money in protecting their web sites and customer information. But sometimes mistakes are made that result in data breaches. Among the information that gets stolen are usernames, passwords and corresponding email addresses. How can you know if you’ve been a victim? Use a data breach monitoring site. They keep an eye on criminal web sites where there are lists of stolen email addresses and credentials. Two work in a similar way: You enter your email address, and the site tells you whether it’s listed on a criminal site. Those two are “Have I Been Pwned” — which is spelled P-W-N-E-D, and Identity Leak. The easiest way to get to them is by a browser search and then bookmark the sites. Both allow you to register your email address, so you’ll be sent a notice if they know your address has been compromised.

Click link above to read more

North Carolina County Lost $1.7 Million in BEC Scam

https://www.bleepingcomputer.com/news/security/north-carolina-county-lost-17-million-in-bec-scam/

After falling for a BEC scam, Cabarrus County in North Carolina lost $1,728,082.60 after sending $2.5 million to scammers pretending to be contractors building the county's new high school.

BEC, or Business Email Compromise, fraud schemes are scams where crooks deceive employees of privately-held companies and public organizations into wiring money to entities they trust but whose bank accounts were changed to ones controlled by the criminals.

Click link above to read more

US Govt, NGOs Ask Cyber Community to Boost Ransomware Defenses

https://www.bleepingcomputer.com/news/security/us-govt-ngos-ask-cyber-community-to-boost-ransomware-defenses/

A joint statement published by the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) urges government partners and the cyber community to reinforce their ransomware defenses.

"The recent ransomware attacks targeting systems across the country are the latest in a string of attacks affecting State and local government partners," says the press release.

Click link above to read more

FBI Warns of Romance Scams Turning Victims into Money Mules

https://www.bleepingcomputer.com/news/security/fbi-warns-of-romance-scams-turning-victims-into-money-mules/

Confidence and romance scams are not always the only side of the fraudster's business. Victims of this type of deceit are often used as mules that unwittingly move funds obtained from business email compromise (BEC) to various accounts controlled by the attacker.

Last year, the losses from romance and confidence scams added to over $362 million (70% more compared to the previous year), based on 18,000 complaints. However, not all victims report the deceit.

Click link above to read more

North Korea cyber-attacks reap almost $3b for weapons programs, UN report says

https://www.abc.net.au/news/2019-08-06/north-korea-accused-of-cyber-attacks-to-get-physical-weapons/11386182

North Korea has generated an estimated $US2 billion ($2.9 billion) for its weapons of mass destruction programs using "widespread and increasingly sophisticated" cyber-attacks to steal from banks and cryptocurrency exchanges, according to a confidential United Nations (UN) report.

Click link above to read more

Financial services and e-payment firms in Singapore must follow new cyber hygiene rules from next August: MAS

https://www.straitstimes.com/tech/financial-services-and-e-payment-firms-in-spore-must-follow-new-cyber-hygiene-rules-from-next

SINGAPORE - All financial services and e-payment firms in Singapore must follow a set of cyber hygiene rules from August next year, with Singapore's central bank stepping up efforts to strengthen the sector's defence against rising threats.

The Monetary Authority of Singapore (MAS) announced the mandatory rules on Tuesday (Aug 6), saying the sector will be more exposed to risks when it opens up to more technology players including e-wallet services and cryptocurrency firms.

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