Security Digest
Information Security Branch
British Columbia
OCIO
Office of the Chief Information Officer

July 3rd, 2018

July is "Security while you travel" Month

This week's stories:

- Half a million Ontarians own cryptocurrency, says securities regulator, but many don't understand the risks 🇨🇦
- Act quickly to minimize damage from cyberattacks
- BlackBerry and Samsung team up on new IoT solutions 🇨🇦
- California passes strictest online privacy law in the country
- Tesla Wednesday sued an ex-employee accused of hacking its manufacturing operating system and stealing company data.
- Fake bookings hit Singapore's Ryde Technologies
- Baltimore's police department is a technological disaster
- Security Flaws Disclosed in LTE (4G) Mobile Telephony Standard
- Adidas Announces Data Breach
- National Security Concerns Over Hackers Commandeering Satellites
- Ticketmaster Announces Data Breach Affecting 5% of All Users

Half a million Ontarians own cryptocurrency, says securities regulator, but many don't understand the risks 🇨🇦

https://business.financialpost.com/technology/blockchain/half-a-million-ontarians-own-cryptocurrency-says-securities-regulator-but-many-dont-understand-the-risks

More than half a million Ontarians own cryptocurrencies, but many do not fully understand the risks associated with the emerging digital asset class, according to a new study from the Ontario Securities Commission.

Tyler Fleming, director of the Investor Office at the OSC said the regulator published the study, titled Taking Caution: Financial Consumers and the Cryptoasset Sector, as an initial snapshot of a sector still very much in its infancy.

“As a regulator, the reason we wanted to do this study is there are a number of investor protection concerns with this emerging cryptoasset sector — concerns around volatility, transparency, valuation, liquidity, et cetera,” Fleming said.

“We really wanted to get some baseline data.”

Click link above to read more

Act quickly to minimize damage from cyberattacks

https://business.financialpost.com/sponsored/business-sponsored/act-quickly-to-minimize-damage-from-cyberattacks

Advice for businesses that have been hacked or attacked by ransomware: hire professionals as soon as possible to negotiate with the attacker, pay the settlement and then restore the integrity of the company's data or network.

"In movies, police tell victims of crime that they shouldn't pay a ransom," says Joseph Khunaysir, chief technology officer with Canadian IT service provider Jolera Inc. "But law enforcement can't help you with a cyber attack and there's little you can do to help yourself. It's best to have a professional negotiate a settlement with the attacker as quickly as possible."

Database hacks and ransomware attacks have similar consequences: a disruption of business and a demand for cash, usually denominated in Bitcoin. However, the method of attack is very different.

Click link above to read more

BlackBerry and Samsung team up on new IoT solutions

https://www.itworldcanada.com/article/blackberry-and-samsung-team-up-on-new-iot-solutions/406693

Former mobile device giant BlackBerry Ltd. is extending its partnership with present mobile device giant Samsung Electronics Ltd. on a series of Enterprise of Things solutions.

According to a press release issued Wednesday, the companies' new "multi-year strategic relationship" will involve combining BlackBerry's security and endpoint management solutions to Samsung hardware including mobile phones, tablets, wearables, and desktops.

"One of the first outputs of this partnership will be that joint enterprise customers using cutting-edge Samsung devices, such as phones, tablets, wearables, and the Samsung DeX mobile desktop experience, will gain the ability – out-of-the-box – to manage all those devices on a single pane of glass via the BlackBerry Universal Endpoint Management (UEM) platform," the release said.

Click link above to read more

California passes strictest online privacy law in the country

http://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html

Gov. Jerry Brown signed the California Consumer Privacy Act of 2018 on Thursday, hours after its unanimous approval by the State Assembly and Senate.

The law, which takes effect in 2020, gives consumers sweeping control over their personal data. It grants them the right to know what information companies like Facebook and Google are collecting, why they are collecting it, and who they are sharing it with. Consumers will have the option of barring tech companies from selling their data, and children under 16 must opt into allowing them to even collect their information at all.
Assembly member Ed Chau and state Sen. Robert Hertzberg introduced the legislation on June 21. It drew the support of some privacy advocates including Common Sense Media.

Click link above to read more

Tesla Wednesday sued an ex-employee accused of hacking its manufacturing operating system and stealing company data.

http://money.cnn.com/2018/06/20/technology/tesla-sues-employee/index.html

But that ex-employee is fighting back, saying he's being targeted by Tesla for trying to bring problems at the company to light.
"I am being singled out for being a whistleblower. I didn't hack into system. The data I was collecting was so severe, I had to go to the media," said Martin Tripp, the defendant in Tesla's suit, told CNNMoney soon after the suit was filed.

Tesla filed the suit in federal court in Nevada Wednesday against Tripp, 40, of Sparks, Nevada, who had worked at its massive lithium battery Gigafactory since October 2017. Tesla (TSLA) asks for unspecified financial damages and to be able to search Tripp's computers and personal USB and electronic storage devices, email accounts, cloud-based storage accounts, and mobile phone call and messaging history.

Click link above to read more

Fake bookings hit Singapore's Ryde Technologies

https://www.bbc.com/news/technology-44655668

Hundreds of fake accounts making "phantom bookings" have recently plagued Singapore-based firm Ryde Technologies, the company has said.
In recent weeks, nearly 300 such accounts have made 2,000 bogus bookings, costing drivers $50,000 (£37,900). The start-up investigated the problem after drivers complained.

Uber, which offers a similar service, has in the past reported cases of fake bookings in other countries.

Ryde has filed a report with local police who are now investigating the matter, according to Reuters.

Click link above to read more

Baltimore's police department is a technological disaster

https://arstechnica.com/information-technology/2018/06/baltimore-police-study-mandated-by-feds-finds-massive-tech-fails/

As part of the consent decree reached in the Justice Department investigation that followed the death of Freddie Gray and the ensuing unrest, an assessment team from the National Police Foundation recently completed a study taking inventory of the Baltimore Police Department's technology infrastructure. The study meant to determine what work needs to be done in order for the department to meet the reporting and other requirements set by the decree. The study's findings—coming just months after Baltimore's 911 center was struck by a ransomware attack—paint a damning picture of how tech has been managed by the eighth-largest city police force in the country.

Over the past year, the Baltimore Police Department (BPD) has moved its IT department up and down within the organizational structure three time. The Information Technology Section has been put in charge of maintaining systems it had no hand in acquiring, because the director of ITS is not part of BPD's executive staff. Core technologies used by the department are no longer supported by software vendors, with some over 20 years old. And the Motorola radio system used for mobile communications by the force, including 911 dispatch, will no longer be supported after this year—and there are no plans in place to replace it.

Click link above to read more

Security Flaws Disclosed in LTE (4G) Mobile Telephony Standard

https://www.bleepingcomputer.com/news/security/security-flaws-disclosed-in-lte-4g-mobile-telephony-standard/

A team of academics has published research yesterday that describes three attacks against the mobile communication standard LTE (Long-Term Evolution), also known as 4G.

Two of the three attacks are passive, meaning an attacker can watch LTE traffic and determine various details about the target, while the third is an active attack that lets the attacker manipulate data sent to the user's LTE device.

According to researchers, the passive attacks allow an attacker to collect meta-information about the user's traffic (an identity mapping attack), while the second allows the attacker to determine what websites a user might be visiting through his LTE device (a website fingerprinting attack).

Click link above to read more

Adidas Announces Data Breach

https://www.bleepingcomputer.com/news/security/adidas-announces-data-breach/

Sportswear maker Adidas announced a data breach yesterday evening, which the company says it impacted shoppers who used its US website.

The company says it became aware of the breach on Tuesday, June 26, when it learned that an unauthorized party was claiming to have acquired the details of Adidas customers. "According to the preliminary investigation, the limited data includes contact information, usernames and encrypted passwords," an Adidas spokesperson said. "Adidas has no reason to believe that any credit card or fitness information of those consumers was impacted," he added.

The company said it's still investigating the breach with law enforcement and security firms. Although the sportswear company did not include a tally of affected customers, some news outlets like CBS, the Wall Street Journal, and Bloomberg reported citing inside sources that "a few millions" of Adidas customers might be impacted.

Click link above to read more

National Security Concerns Over Hackers Commandeering Satellites

https://www.bleepingcomputer.com/news/security/national-security-concerns-over-hackers-commandeering-satellites/

The number of satellites transmitting GPS locations, cellphone signals and other sensitive information has been rapidly increasing, which has resulted in the creation of favorable circumstances for hackers. Even with all the advances in satellite technology, much of the US military’s satellite technology remains vulnerable.

Earlier in the month, Bleeping Computer reported on a cyber-espionage group believed to be operating out of China who hacked companies who develop satellite communications and geospatial imaging. They also targeted defense contractors from the US and Southeast Asia:

"The company said that responsible for the attacks was an advanced persistent threat (APT, a term used to describe cyber-espionage groups) known under the codename of Thrip. The recent attacks were difficult to detect, the company said. Hackers used a technique known as "living off the land,"which consists of using local tools already available on the operating system to carry out malicious operations."

Click link above to read more

Ticketmaster Announces Data Breach Affecting 5% of All Users

https://www.bleepingcomputer.com/news/security/ticketmaster-announces-data-breach-affecting-5-percent-of-all-users/

Ticketing service Ticketmaster announced a data breach incident today that affected roughly 5% of its entire customer base, and has resulted in the theft of customer data, Ticketmaster login information, and payment details.

The breach didn't occur at Ticketmaster itself, but at Inbenta, a provider of AI-powered live chat widgets, which Ticketmaster was deploying on some of its localized sites across the world.

The ticketing service says that on Saturday, June 23, it detected that this live chat widget was being used to deliver malicious software to Ticketmaster users. The malicious software was logging and exfiltrating customer details.

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
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

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.

Information Security Branch
www.gov.bc.ca/informationsecurity
British Columbia
OCIO
Office of the Chief Information Officer