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

August 7th, 2018

August is "Wi-Fi" Month

This week's stories:

- Canada watching for cyber threats to 2019 election, says government
- BlackBerry announces new ransomware recovery tool
- Facebook: We're not 'actively' seeking consumers' banking data
- 11,000 Wikileaks Twitter DMs Have Just Been Published For Anyone To Read
- Lying Sextortion Scammers Score $250,000 After Sending Victims Their Own Hacked Passwords
- For Less Than $10, Anyone Can Bypass Apple's Big iPhone Security Feature
- Atlanta's Reported Ransomware Bill: Up to $17 Million
- Australia's Biggest Breach Offender: Healthcare Sector
- Dixons Carphone: 10 Million Records Exposed in 2017 Breach
- Iowa Health Group Data Breach Hits 1.4 Million Patients
- Pentagon Restricts Use of Fitness Trackers, Other Devices

Canada watching for cyber threats to 2019 election, says government

https://www.itworldcanada.com/article/canada-watching-for-cyber-threats-to-2019-election-says-government/407729

Canada is "working hard to ensure that the 2019 elections are protected and defended against cyber threats and foreign interference," says a spokesperson for federal Democratic Institutions.

"We continue to closely monitor and address foreign and cyber threats, including those that may affect the 2019 election," Nicky Cayer,
press secretary to minister Karina Gould, said Thursday in a statement to ITWorldCanada.com.

It came shortly after senior U.S. law enforcement and intelligence officials told White House reporters that, at the direction of President Trump, countering election interference a top priority.

Click link above to read more

BlackBerry announces new ransomware recovery tool

https://www.itworldcanada.com/article/blackberry-announces-new-ransomware-recovery-tool/407774

BlackBerry is attempting to make it easier for a businesses to protect itself against ransomware attacks by introducing a new recovery feature for its Workspaces platform, it announced on Monday.

Making the announcement at the Black Hat conference in Las Vegas, Blackberry, in a press release, called the feature a precise recovery tool able to minimize the disruption a business may face when attacked by ransomware.

Click link above to read more

Facebook: We're not 'actively' seeking consumers' banking data

https://money.cnn.com/2018/08/06/technology/facebook-banks-data/index.html

On Monday, the Wall Street Journal reported that Facebook has asked several major banks to provide information like account balances and credit card activity. According to the report, Facebook asked firms like JPMorgan Chase, Wells Fargo, Citigroup and U.S. Bancorp to discuss possible offerings it could provide for users on its Messenger chat platform.

Facebook declined to comment on whether it has been in talks with those companies but clarified it does work with banks to offer various services on Messenger.

"A recent Wall Street Journal story implies incorrectly that we are actively asking financial services companies for financial transaction data -- this is not true," a Facebook spokesperson told CNNMoney. "Like many online companies with commerce businesses, we partner with banks and credit card companies to offer services like customer chat or account management."

Click link above to read more

11,000 Wikileaks Twitter DMs Have Just Been Published For Anyone To Read

https://www.forbes.com/sites/thomasbrewster/2018/07/30/11000-wikileaks-twitter-messages-released-to-the-public/#38078bec30a0

Ever wondered what's going on behind closed doors at Julian Assange's pro-transparency outfit Wikileaks? Thanks to journalist Emma Best, you can now rifle through 11,000 direct, private messages sent to and from Wikileaks' Twitter account.

Best released the messages Monday, saying they came from the "Wikileaks + 10 chat," a private group for the organization's more active supporters. She claimed many of the messages contained offensive material. "At various points in the chat, there are examples of homophobia, transphobia, ableism, sexism, racism, antisemitism and other objectionable content and language." Wikileaks hadn't responded to a request for comment at the time of publication.

Click link above to read more

Lying Sextortion Scammers Score $250,000 After Sending Victims Their Own Hacked Passwords

https://www.forbes.com/sites/thomasbrewster/2018/07/31/sextortion-scam-with-hacked-passwords-scores-250000-dollars-for-cybercriminals/#3b5b8e13df16

Online scammers have been innovating of late. In the last month, one group of ne’er-do-wells has sent out spam emails telling recipients they’ve been caught watching porn through their webcam, and if they don’t pay, all their dirty laundry will be aired in public. That’s not new. But putting a novel twist on that scam, the crooks are sending through passwords they claim to have stolen as proof they have been spying on the victim. So far, more than 150 people have coughed up $250,000 in Bitcoin for fear of their private Web browsing habits being exposed.

And yet the claims that the hackers have stolen passwords and obtained access to webcams appear to be lies. The perpetrators of this particular deception have simply collected passwords from previous data breach leaks. Nevertheless, they're duping enough people, making more than 30 Bitcoin in a matter of weeks, according to a cybersecurity expert who has been tracking the attacks. And, the researcher said, the cybercriminals have now made three times as much as the individuals behind WannaCry, the ransomware that spread rapidly around the world in 2017, causing disruption at hospitals and other businesses.

Click link above to read more

For Less Than $10, Anyone Can Bypass Apple's Big iPhone Security Feature

https://www.forbes.com/sites/thomasbrewster/2018/08/02/for-less-than-10-anyone-can-bypass-apples-big-iphone-security-feature/#4abdd1ff42d3

Apple is causing real headaches for police trying to hack their way into iPhones with each iOS update. But according to one ex-cop, all it takes is a little ingenuity, some patience and less than $10 to bypass one of Apple's most significant barriers to entry and break open locked iPhones.

That was made apparent in a webcast with former West Virginia State Police forensics specialist Chris Vance on Thursday. Speaking on behalf of his current employer, government supplier Magnet Forensics, Vance talked about the problems police faced with Apple's USB Restricted Mode. The feature, introduced in the latest iOS release (11.4.1), kills any data connection between an iPhone and a computer once a device has been locked for an hour. If there's no data connection, there's no way an iPhone can be hooked up to a PC and have all the information inside transferred.

Click link above to read more

Atlanta's Reported Ransomware Bill: Up to $17 Million

https://www.databreachtoday.com/atlantas-reported-ransomware-bill-up-to-17-million-a-11281

The cost of the city of Atlanta's mitigation and subsequent IT overhaul following a massive SamSam ransomware infection earlier this year could reach $17 million.

The March 22 ransomware outbreak left 8,000 city employees unable to use their PCs for several days and led to longer outages for residents who wanted to pay for parking tickets or report potholes online as the city's IT team continued to grapple with the incident.

The Atlanta Journal-Constitution and Atlanta's WSB-TV Channel 2 Action News last week reported that they obtained a seven-page document, marked "confidential and privileged," that describes the most recent costs incurred by the city as it has continued to respond to the ransomware outbreak.

The city's assessment says Atlanta has about $6 million in contract commitments as a result of the ransomware attack, and it faces up to $11 million more in additional costs, the news outlets report.

Of the $6 million in commitments, about $1.1 million has been budgeted for "new desktops, laptops, smartphones and tablets," while the rest is for "security services and software upgrades," they report.

Click link above to read more

Australia's Biggest Breach Offender: Healthcare Sector

https://www.databreachtoday.com/australias-biggest-breach-offender-healthcare-sector-a-11267

With Australia's data breach reporting law now in full effect, figures published for the second quarter of this year reveal that the country's healthcare sector is the worst breach offender. The finding is sure to intensify the already intense scrutiny facing the country's controversial e-health records project.

The country's data breach regulator, the Office of the Australian Information Commissioner, released the data breach statistics that it collected, covering breach reports that it received from April through June. It is the first full reporting period since Australia's mandatory breach notification law came into effect on Feb. 22.

Click link above to read more

Dixons Carphone: 10 Million Records Exposed in 2017 Breach

https://www.databreachtoday.com/dixons-carphone-10-million-records-exposed-in-2017-breach-a-11265

Struggling European electronics giant Dixons Carphone says its investigation into a July 2017 data breach has found that the incident was worse than it initially believed, affecting 10 million customers - 10 times the number it previously reported.

"Our investigation, which is now nearing completion, has identified that approximately 10 million records containing personal data may have been accessed in 2017," the publicly traded company says in a Tuesday statement. "While there is now evidence that some of this data may have left our systems, these records do not contain payment card or bank account details and there is no evidence that any fraud has resulted."

Click link above to read more

Iowa Health Group Data Breach Hits 1.4 Million Patients

https://www.databreachtoday.com/iowa-health-group-data-breach-hits-14-million-patients-a-11264

A large Midwestern health network says a successful phishing campaign exposed a raft of personal and medical data stored in its email systems. But it says that the information exposure appears to have been an unintentional byproduct of an attempt to divert corporate payments via what's known as business email compromise or CEO fraud.

UnityPoint Health, which runs more than 50 clinics in Iowa with 290 physicians and other providers, says it began notifying breach victims by mail on Monday. The Des Moines Register reports that 1.4 million patients are being notified.

Click link above to read more

Pentagon Restricts Use of Fitness Trackers, Other Devices

https://www.securityweek.com/pentagon-restricts-use-fitness-trackers-other-devices

WASHINGTON (AP) — Military troops and other defense personnel at sensitive bases or certain high-risk warzone areas won't be allowed to use fitness-tracker or cellphone applications that can reveal their location, according to a new Pentagon order.

The memo, obtained by The Associated Press, stops short of banning the fitness trackers or other electronic devices, which are often linked to cellphone applications or smart watches and can provide the users' GPS and exercise details to social media. It says the applications on personal or government-issued devices present a "significant risk" to military personnel, so those capabilities must be turned off in certain operational areas.

Under the new order, military leaders will be able to determine whether troops under their command can use the GPS function on their devices, based on the security threat in that area or on that base.

Click link above to read more

****

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.

Information Security Branch
www.gov.bc.ca/informationsecurity

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer