Security Digest
Information Security Branch

BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer

October 23rd, 2018

October is "**Cybersecurity awareness**" Month
Test yourself with the Cybersecurity Awareness Month Quiz: **Cybersecurity by the Numbers**

This week's stories:

- **Businesses spent $14B on cybersecurity in 2017, more than 20% hit by cyberattack**
- **CIRA Canadian Cybersecurity Survey identifies disconnect between awareness and actions**
- **What Are The Biggest Cyber-Security Trends Of 2018?**
- **Twitter shuts down hundreds of suspected bots which shared pro-Saudi views on Jamal Khashoggi**
- **Say cheese: U.S. airports plan to scan your face at security, bag check and boarding**
- **Apple launches tool that allows users to control data collected**
- **Four identity management trends to prepare for**
- **Fraudster Targets Cryptocurrency Wallets with a Variety of Info Stealers**
- **Abandoned Tweet Counter Hijacked With Malicious Script**
- **Vending Machine App Hacked for Unlimited Credit**
- **FDA Calls for 'Cybersecurity Bill of Materials' for Devices**

Businesses spent $14B on cybersecurity in 2017, more than 20% hit by cyberattack

https://www.canadiansecuritymag.com/news/data-security/businesses-spent-$14b-on-cybersecurity-in-2017-more-than-20-hit-by-cyberattack

More than one in five Canadian companies say they were hit by a cyberattack last year, with businesses spending $14 billion on cybersecurity as they confront greater risks in the digital world, according to a new Statistics Canada survey.

The most common suspected motive was an attempt to steal money or demand a ransom payment, according to the survey. Theft of personal or financial information was less typical — less than one-quarter of the cyberattacks — though it was the most cited reason for investing in cybersecurity, StatCan said.

Click link above to read more

CIRA Canadian Cybersecurity Survey identifies disconnect between awareness and actions

https://www.canadiansecuritymag.com/news/data-security/cira-canadian-cybersecurity-survey-identifies-disconnect-between-awareness-and-actions

On Oct. 15, the Canadian Internet Registration Authority (CIRA) released its 2018 CIRA Cybersecurity Survey, which provides an overview of the Canadian cybersecurity landscape.

The organization responsible for the .CA web domain surveyed 500 individuals with responsibility over IT security decisions at small and medium-sized businesses across Canada to learn more about how they are coping with the increase in cyber threats — the sample included both business owners and employees who manage information technology.

Key findings

- 40 per cent of respondents experienced a cyberattack in the last 12 months. One in ten experienced 20 or more attacks.
- Among larger businesses with 250-499 employees, the number that experienced an attack increases to 66 per cent.
- 67 per cent of respondents outsource at least part of their cybersecurity footprint to external vendors.
- While 59 per cent of respondents said they stored personal information from customers, 38 per cent said they were unfamiliar with PIPEDA.
- One-third of respondents indicated that the most significant impact of a cyberattack is the time and resources required to respond to the incident.
- 88 per cent of respondents were concerned with the prospect of future cyberattacks, which resulted in 28 per cent suggesting they would add cybersecurity staff in the next year.
- Although 78 per cent were confident in their level of cyber threat preparedness, 37 per cent didn't have anti-malware protection installed and 71 per cent did not have a formal patching policy – exposing these organizations to massive security holes.
- Only 54 per cent of small businesses provide cybersecurity training for their employees even though the most common form of malware seen by respondents, phishing attacks (42 per cent), directly exploit employees as a point of weakness.

Click link above to read more

What Are The Biggest Cyber-Security Trends Of 2018?

https://www.forbes.com/sites/quora/2018/10/17/what-are-the-biggest-cyber-security-trends-of-2018/#3bea47097d34

What are the biggest cybersecurity trends in 2018? originally appeared on Quora: the place to gain and share knowledge, empowering people to learn from others and better understand the world.

I'll answer this with the lens of what's current on my mind as I look to keep Dropbox and Dropbox user data secure.

Click link above to read more

Twitter shuts down hundreds of suspected bots which shared pro-Saudi views on Jamal Khashoggi

https://globalnews.ca/news/4571810/twitter-khashoggi-saudi-bot-accounts/

A network of hundreds of Twitter accounts was shut down after tweeting pro-Saudi sentiments regarding the disappearance of journalist Jamal Khashoggi.

The accounts are suspected of being bots, NBC News reported, because they were tweeting and re-tweeting pro-Saudi government tweets at the same time and in the same order.

Click link above to read more

Say cheese: U.S. airports plan to scan your face at security, bag check and boarding

https://globalnews.ca/news/4567183/facial-recognition-technology-u-s-airports/

If you're travelling by plane in the United States any time soon, you may come across facial recognition technology to check in, drop off a bag, go through security and board your flight.

U.S. Customs and Border Protection (CPB) has been using the technology to screen non-U.S. residents on international flights for a few years. But now the Transport Security Administration (TSA) is partnering with the CPB and rolling out facial recognition on domestic flights, too.

Click link above to read more

Apple launches tool that allows users to control data collected

https://globalnews.ca/news/4564818/apple-privacy-data-control-tool/

Apple Inc on Wednesday rolled out an online tool to users in the United States and several other countries to download, change or delete all the data that the iPhone maker has collected on them.

Click link above to read more

Four identity management trends to prepare for

https://www.itworldcanada.com/article/sector-2018-four-identity-management-trends-to-prepare-for/410536

Cyber security conferences usually have many predictable sessions, along the lines of 'Here's how this foolish company let itself be hacked ….'

However, one speaker at this month's annual SecTor conference in Toronto beamed a ray of optimism.

"I genuinely think that in 10 years we will not see the level of attacks we see today," predicted Sarah Squire, a senior technical architect with Ping Identity, who is also on board of the OpenID Foundation and a co-founder of IDPro, an association for identity professionals.

Click link above to read more

Fraudster Targets Cryptocurrency Wallets with a Variety of Info Stealers

https://www.bleepingcomputer.com/news/security/fraudster-targets-cryptocurrency-wallets-with-a-variety-of-info-stealers/

An online scammer targeting thousands of victims interested in cryptocurrencies runs a large and diverse business that includes phishing and fraud operations.

The crook tempts users with offers to make digital coins the easy way, to trick them into installing information-stealing malware and backdoors that provide access to sensitive data.

Click link above to read more

Abandoned Tweet Counter Hijacked With Malicious Script

https://www.bleepingcomputer.com/news/security/abandoned-tweet-counter-hijacked-with-malicious-script/

When a site owner utilizes a third-party script in their site, it is necessary to monitor whether that script has been abandoned or not. Otherwise, you may find bad actors come along and replace the script with a malicious one that is then displayed to your visitors.

This is exactly what happened with a Tweet counter called New Share Counts that was abandoned/discontinued in July 2018. When the service was discontinued, the developer posted a message on their newsharecounts.com domain stating that the service was dead and gave recommendations for other services to use.

Click link above to read more

Vending Machine App Hacked for Unlimited Credit

https://www.bleepingcomputer.com/news/security/vending-machine-app-hacked-for-unlimited-credit/

A hacker enticed by the payment method used by the vending machines located on a university campus found a way to get free credit after looking at the inner workings of the machine's accompanying mobile app.

The vending machines are from Argenta, a popular provider of coffee services in Italy, now acquired by the Selecta Group B.V.. The machines are used all over the country for automated sales of all sorts of products, from refreshing drinks to cigarettes.

Click link above to read more

FDA Calls for 'Cybersecurity Bill of Materials' for Devices

https://www.databreachtoday.com/fda-calls-for-cybersecurity-bill-materials-for-devices-a-11628

Before marketing their medical devices, manufacturers should prepare a "cybersecurity bill of materials" that lists components that could be susceptible to vulnerabilities, according to a draft of updated Food and Drug Administration premarket guidance.

In addition to releasing the proposed guidance this week, the FDA announced a formalized agreement with the Department of Homeland Security to implement a new framework for greater collaboration between the two agencies for addressing cybersecurity in medical devices.

Click link above to read more