Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

December 12th, 2018

December is Mobile Month

This week's stories:

- Cybersecurity jobs expected to be in high demand in Canada, experts say
- Spy agency expects foreign actors to attempt to sway public opinion online
- In B.C. and beyond, online and phone fraud is a growth industry
- National security top priority in assessing Huawei's role in Canada's 5G network: minister
- What workers need to learn about cyber security
- Why Satellites Need Cybersecurity Just Like You
- Canada's cybersecurity chief says jury still out on whether Russian disinformation bots are having any impact
- Eastern European Bank Hackers Wield Malicious Hardware
- Equifax breach was 'entirely preventable' had it used basic security measures, says House report
- Linux.org domain hacked, plastered with trolling, filth and anti-transgender vandalism

---

Cybersecurity jobs expected to be in high demand in Canada, experts say

https://globalnews.ca/news/4733898/cybersecurity-jobs-high-demand-canada/

International hackers might be Canada's biggest cyber threat, but the country has a far more basic problem to tackle first — finding and hiring the cybersecurity analysts to take them on.

Canada announced in October that it would be opening a cybersecurity centre in Ottawa. Industry analysts believe they need to hire over 140 front-line analysts, who will be tasked with countering hackers intent on infiltrating Canadian companies for financial gain or hostile nations focused on spreading fake political stories online.

Click link above to read more

Spy agency expects foreign actors to attempt to sway public opinion online

https://www.ctvnews.ca/politics/spy-agency-expects-foreign-actors-to-attempt-to-sway-public-opinion-online-1.4207164

Canada's cyber spy agency is warning that in 2019—an election year—foreign countries are "very likely" to try to sway Canadians' public opinion with misinformation online.

"In the coming year, we anticipate state-sponsored cyber threat actors will attempt to advance their national strategic objectives by targeting Canadians' opinions through malicious online influence activity," says Communications Security Establishment (CSE) in a newly released report on the current cyber threat environment Canada is facing.

Click link above to read more

In B.C. and beyond, online and phone fraud is a growth industry

https://www.bcbusiness.ca/Scamcouver-In-BC-and-beyond-online-and-phone-fraud-is-a-growth-industry

In 2017, Canadians lost nearly $85 million to schemes, scams and rip-offs, according to RCMP Sgt. Guy Paul Larocque, acting officer in charge of the Canadian Anti-Fraud Centre in Ottawa. Of that total, B.C. accounted for $7.9 million—a figure topped by this August, when losses for the year reached $8.7 million. The number of ruses in this cottage industry is vast, from romance burns and extortion to investment fraud. Here are a few.

Click link above to read more

National security top priority in assessing Huawei's role in Canada's 5G network: minister

https://globalnews.ca/news/4747851/huawei-canada-5g-national-security/

National security "comes first" in deciding whether to allow Huawei Technologies to take part in developing Canada's 5G telecommunications network, Infrastructure Minister Francois-Philippe Champagne says.

Canada needs to be prudent and rely on the input of its intelligence services before ruling on whether the Chinese firm should be involved in the next-generation wireless communication system, Champagne said Monday during a roundtable interview with The Canadian Press.

Click link above to read more

What workers need to learn about cyber security

https://www.canadianunderwriter.ca/risk/workers-need-learn-cyber-security-1004149647/

It may seem obvious: Companies' computers, mobile devices and accounts need secure passwords. But many small business owners don't take the time to educate staffers about these very basic forms of cybersecurity. And staffers may not know that their passwords could be easily guessed by hackers and cyberthieves.

Click link above to read more

Why Satellites Need Cybersecurity Just Like You

https://www.space.com/42658-cybersecurity-for-satellites.html

Any modern person who spends time on the internet is familiar with the basic principles of cybersecurity — but imagine you're in charge of a satellite that people around the globe rely on. Suddenly, changing a password every few months and hoping for the best doesn't seem quite vigilant enough.

And cybersecurity is indeed a threat countries need to consider to protect their satellites, Eric Fanning, head of the Aerospace Industries Association, a group of companies working on defense and aerospace, told Space.com.

Click link above to read more

Canada's cybersecurity chief says jury still out on whether Russian disinformation bots are having any impact

https://theprovince.com/news/politics/canadas-cybersecurity-chief-says-jury-still-out-on-whether-russians-disinformation-bots-are-having-any-impact/wcm/c7b1b29c-8abf-4486-b247-f0d852bfafa6

'Not everything is blatantly false,' says Scott Jones. 'Sometimes it's a slight manipulation of the facts — just enough to sow division'

The head of Canada's new cybersecurity centre says the jury is still out on whether state-sponsored disinformation campaigns are actually having any impact on voters' intentions, but that Canadians should still use a "critical eye" when they read news online.

Click link above to read more

Eastern European Bank Hackers Wield Malicious Hardware

https://www.csoonline.com/article/3326301/security/a-layered-approach-to-cybersecurity-people-processes-and-technology.html

Eastern European hackers have been plugging inexpensive hardware into banks' local area networks to help perpetrate heists that have stolen tens of millions of dollars.

The attack campaign, dubbed DarkVishnya - dark cherry - has targeted at least eight Eastern European banks, says Sergey Golovanov, a principal security researcher at Moscow-based endpoint security firm Kaspersky Lab, which was called in to investigate the thefts.

"Each attack had a common springboard: an unknown device directly connected to the company's local network," he says in a blog post. "In some cases, it was the central office, in others a regional office, sometimes located in another country."

Click link above to read more

Equifax breach was 'entirely preventable' had it used basic security measures, says House report

https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/

A House Oversight Committee report out Monday has concluded that Equifax's security practices and policies were sub-par and its systems were old and out-of-date, and bothering with basic security measures — like patching vulnerable systems — could've prevented its massive data breach last year.

It comes a little over a year after Equifax, one of the world's largest credit rating agencies, confirmed its systems had fallen to hackers. Some 143 million consumers around the world were affected — most of which were in the U.S., but also Canada and the U.K. — with that figure later rising to 148 million consumers. Yet, to date, the company has faced almost no repercussions, despite a string of corporate failings that led to one of the largest data breaches in history.

Click link above to read more

Linux.org domain hacked, plastered with trolling, filth and anti-transgender vandalism

https://www.theregister.co.uk/2018/12/07/linuxorg_hacked/

The Linux.org domain was hijacked on Friday morning, with the hacker plastering the message "G3T 0WNED L1NUX N3RDZ" complete with expletives and a very NSFW image.

The real administrator of the site, Mike McLagan, immediately 'fessed up on Reddit, and said the vandal had managed to break into his partner's Network Solutions registrar account and switch Linux.org DNS servers to their own site.

"This evening someone got into my partner's netsol account and pointed linux.org DNS to their own cloudflare account," McLagan wrote, adding: "The production env (web / db) wasn't touched. DNS was simply pointing to another box."

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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