






**February 12<sup>th</sup>, 2019**

February is [Cyberbullying](#) Month

**This week's stories:**

- [Hackers targeting Canadian banks, mining companies, expert tells MPs](#) 
- [P.E.I. whistleblowers sue former premier, officials after privacy breach](#) 
- [Laptop likely holds key to missing \\$180 million in cryptocurrency: experts](#) 
- [Microsoft extends Account Guard to Canada for political parties using Office365](#)
- [Almost 60 per cent of Canadian firms surveyed were victims of cyber attacks: Report](#)
- [Bell 'comfortable' if Ottawa bans Huawei for 5G networks](#)
- [How safe are teen apps?](#)
- [Russia considers 'unplugging' from internet](#)
- [Apple to pay teenager who found FaceTime bug](#)
- [Big trouble Down Under as Australian MPs told to reset their passwords amid hack attack fears](#)

---

**Hackers targeting Canadian banks, mining companies, expert tells MPs** 

<https://www.canadiansecuritymag.com/news/data-security/hackers-targeting-canadian-banks-mining-companies-expert-tells-mps>

Foreign hackers have targeted Canadian banks, mining companies and government institutions in recent years to steal valuable secrets and spread malware, a leading cybersecurity analyst warns.

In February 2017, multiple major Canadian financial institutions were exposed to the risk of state-sponsored cybertheft from North Korea in a scheme to redirect people to malicious downloads that would seize control of their computer, says Christopher Porter, chief intelligence strategist at California-based security firm FireEye.

[Click link above to read more](#)

---

**P.E.I. whistleblowers sue former premier, officials after privacy breach** 

<https://www.canadiansecuritymag.com/news/data-security/pei-whistleblowers-sue-former-premier-officials-after-privacy-breach>

CHARLOTTETOWN — Three whistleblowers whose private information was leaked from Prince Edward Island's government to the Liberal Party are suing a former premier and other top officials for a total of \$1.3 million in damages for the economic and emotional toll on their lives.

The lawsuit says that after the three women came forward at a 2011 news conference with allegations of

bribery and fraud in the province's business immigration program, personal information designed to damage their claims was deliberately given out to the media by top Liberals.

[Click link above to read more](#)

---

## Laptop likely holds key to missing \$180 million in cryptocurrency: experts

[https://www.canadiansecuritymag.com/news/data-security/laptop-likely-holds-key-to-missing-\\$180-million-in-cryptocurrency-experts](https://www.canadiansecuritymag.com/news/data-security/laptop-likely-holds-key-to-missing-$180-million-in-cryptocurrency-experts)

HALIFAX — In an office in Toronto, there's a laptop that could contain the keys to unlock \$180 million in digital assets — virtual money possibly lost after the recent death of the whiz kid who founded one of Canada's largest cryptocurrency exchanges.

Gerald Cotten, a 30-year-old Nova Scotia resident and CEO of QuadrigaCX, was travelling in India on Dec. 9 when he died suddenly. His widow, Jennifer Robertson, has said Cotten was the only person with access to the laptop and the digital keys to the so-called cold wallets that are believed to hold the missing Bitcoins and other cryptocurrencies.

[Click link above to read more](#)

---

## Microsoft extends Account Guard to Canada for political parties using Office365

<https://www.itworldcanada.com/article/microsoft-extends-account-guard-to-canada-for-political-parties-using-office365/414964>

To help ensure Canadian candidates, political parties and think tanks using certain Microsoft products suffer as few interferences as possible the company has extended its Account Guard service to this country.

Microsoft said last week the security service is offered at no additional cost to customers in the political space using Office 365, Hotmail or Outlook.com to help protect them from cybersecurity threats.

[Click link above to read more](#)

---

## Almost 60 per cent of Canadian firms surveyed were victims of cyber attacks: Report

<https://www.itworldcanada.com/article/almost-60-per-cent-of-canadian-firms-surveyed-were-victims-of-cyber-attacks-report/414952>

Canadian organizations are getting tougher in fighting online attackers but not tough enough, if a new report from a security vendor is representative.

In its annual security study Scalar Decisions said that over the past year Canadian organizations have increased their focus on identifying assets on the network, prioritizing deployment of cyber security solutions, and patching on-premise infrastructure. However, it found there are still key cyber resilience weaknesses including

[Click link above to read more](#)

---

## Bell 'comfortable' if Ottawa bans Huawei for 5G networks

<https://www.itworldcanada.com/article/bell-comfortable-if-ottawa-bans-huawei-for-5g-networks/414863>

Bell Canada's chief executive says his company is prepared if Ottawa forbids telcos from buying 5G equipment from Huawei Technologies because of government worries about Chinese government influence over companies headquartered there.

Both Bell and Telus have a lot of Huawei equipment in their 3G and 4G cellular networks, exclusively in their base stations. According to news reports they are worried a blanket ban on Huawei networking

equipment — not only for the soon-to-be-constructed super-fast 5G network but also on their existing gear — would be very costly.

[Click link above to read more](#)

---

### **How safe are teen apps?**

<https://www.theguardian.com/technology/2019/feb/10/how-safe-are-teen-apps>

Since 14-year-old Molly Russell killed herself in 2017, the apps and services our teenagers and children use — and their safety — have become a key concern for parents. Last week, the digital minister, Margot James, stated that “the tragic death of Molly Russell is the latest consequence of a social media world that behaves as if it is above the law”. James went on to announce plans to introduce a legally binding code and duty of care towards young users for social media companies.

[Click link above to read more](#)

---

### **Russia considers 'unplugging' from internet**

<https://www.bbc.com/news/technology-47198426>

Russia is considering whether to disconnect from the global internet briefly, as part of a test of its cyber-defences.

The test will mean data passing between Russian citizens and organisations stays inside the nation rather than being routed internationally.

A draft law mandating technical changes needed to operate independently was introduced to its parliament last year.

The test is expected to happen before 1 April but no exact date has been set.

[Click link above to read more](#)

---

### **Apple to pay teenager who found FaceTime bug**

<https://www.bbc.com/news/technology-47169462>

A US teenager who discovered a security flaw in Apple's FaceTime video-calling system has been given a bug bounty.

Apple has not revealed the exact amount it is giving 14-year-old Grant Thompson but it is believed to include money to help pay for his education.

The teenager found a bug that meant he could briefly eavesdrop on recipients to a group FaceTime call.

[Click link above to read more](#)

---

### **Big trouble Down Under as Australian MPs told to reset their passwords amid hack attack fears**

[https://www.theregister.co.uk/2019/02/08/australia\\_parliament\\_password\\_reset/](https://www.theregister.co.uk/2019/02/08/australia_parliament_password_reset/)

The Australian Parliament has reset all passwords on the parliamentary computing network following an unspecified security incident.

In a joint statement on February 8, the legislature's presiding officers — Speaker of the Australian House of Representatives Tony Smith, and Scott Ryan, President of the Australian Senate — said the action was “undertaken for abundance of caution” in response to an incident that occurred overnight and Friday morning.

[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](mailto: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](http://www.gov.bc.ca/informationsecurity)



BRITISH  
COLUMBIA



**OCIO**  
Office of the Chief Information Officer