



## Security News Digest

Information Security Branch



**OCIO**




Office of the  
Chief Information Officer

**May 26, 2020**

Try our May Quiz – [Cyber Safety at Home](#)

Join Us for Security Day May 27<sup>th</sup> – <http://www.gov.bc.ca/securityday>

### **This week's stories:**

- [Canada still lacks cybersecurity 'street smarts' says CIRA director](#) 
- [Ontario health unit website leaves COVID-19 test results and names accessible](#) 
- [Spy agency flags possible security breaches at Canadian pandemic research facilities](#) 
- [Hackers leak credit card info from Costa Rica's state bank](#)
- [How to mitigate your business risk in the new normal](#)
- [Virtual cybersecurity school teaches kids to fix security flaws and hunt down hackers](#)
- [Voter info for millions of Indonesians shared on hacker forum](#)
- [8 states targeted in CARES Act scams from cybercrime group](#)

---

### **Canada still lacks cybersecurity 'street smarts' says CIRA director**

<https://www.itworldcanada.com/article/canada-still-lacks-cybersecurity-street-smarts-says-cira-director/431107>

While the federal government combats hostile foreign intelligence services seeking the country's biggest secrets, hackers and fraudsters are keen on cashing in on the fear the novel coronavirus has created, targeting both individuals and businesses across Canada. The air duct folks are offering "special" air filters to protect from COVID-19, and "financial advisors" are offering financial aid or loans to help struggling businesses survive local shutdown orders. Meanwhile, work from home policies are in effect across thousands of companies, and the resulting IT sprawl is giving security leaders headaches and cyber criminals fresh new attack surfaces to chew on.

*[Click link above to read more](#)*

---

### **Ontario health unit website leaves COVID-19 test results and names accessible**

<https://www.itworldcanada.com/article/ontario-health-unit-website-leaves-covid-19-test-results-and-names-accessible/431080>

While privacy experts worry proposed COVID-19 mobile contact tracing apps will reveal personal information of users, a northern Ontario health authority has admitted a privacy breach has happened the usual way: A website configuration mistake.

The North Bay Parry Sound District Health Unit said Thursday that results of coronavirus tests of 3,000 area residents were accidentally accessible for anyone with some computer knowledge to read on the Health Unit's COVID-19 data dashboard this week. The dashboard has information related to the number of COVID-19 tests and confirmed cases in the area.

[\*Click link above to read more\*](#)

---

## **Spy agency flags possible security breaches at Canadian pandemic research facilities**



<https://www.cbc.ca/news/politics/cse-research-compromises-1.5577744>

Canada's cyber spy agency says authorities are investigating possible security breaches at Canadian organizations doing COVID-19-related research — less than a week after it warned that Canadian intellectual property linked to the pandemic is a "valuable target" for state-sponsored actors.

"We've seen some compromises in research organizations that we've been helping to mitigate and we're still continuing to look through what's the root cause of those," said Scott Jones, head of the Communications Security Establishment's Cyber Centre, during an appearance in front of the Commons industry, science and technology committee this evening.

[\*Click link above to read more\*](#)

---

## **Hackers leak credit card info from Costa Rica's state bank**

<https://www.bleepingcomputer.com/news/security/hackers-leak-credit-card-info-from-costa-ricas-state-bank/>

Maze ransomware operators have published credit card data stolen from the Bank of Costa Rica (BCR). They threaten to leak similar files every week.

The hackers are doing this in support of their claim to have breached BCR in the past and the bank's denial of these intrusions.

[\*Click link above to read more\*](#)

---

## **How to mitigate your business risk in the new normal**

<https://www.itworldcanada.com/article/how-to-mitigate-your-business-risk-in-the-new-normal/430882>

With billions around the world now in lockdown, businesses have activated sometimes dated continuity plans that never envisioned their entire staff working from home.

The challenges to adjust to the so-called "new normal" of working from home has generally happened in two phases:

The first phase of "getting remote and getting connected" saw companies provide workers with whatever equipment was easily available and then connect them together with a patchwork of systems that would the business to move forward. It has not been a frictionless exercise, but for the most part IT teams sweating through long nights delivered on the promise of a connected and productive workforce.

[\*Click link above to read more\*](#)

---

## **Virtual cybersecurity school teaches kids to fix security flaws and hunt down hackers**

<https://www.cnn.com/2020/05/20/tech/virtual-cyber-security-school/index.html>

When Christopher Boddy was 14 years old, he'd log onto his computer after school to spend hours playing a game that taught him the basics of digital forensics, ethical hacking and cryptography.

It may not have been a typical after-school activity, but it was just what the UK government hoped for when it launched its Cyber Discovery program three years ago: It inspired Boddy, now 17, to consider a career in cybersecurity.

[Click link above to read more](#)

---

### **Voter info for millions of Indonesians shared on hacker forum**

<https://www.bleepingcomputer.com/news/security/voter-info-for-millions-of-indonesians-shared-on-hacker-forum/>

A threat actor has shared the 2014 voter information for close to 2 million Indonesians on a well-known hacker forum and claims they will release a total of 200 million at a later date.

In the forum post, the threat actor states that the voter records are stored in individual PDF files that they took from the KPU, the general election commission of Indonesia.

[Click link above to read more](#)

---

### **8 states targeted in CARES Act scams from cybercrime group**

<https://www.techrepublic.com/article/8-states-targeted-in-cares-act-scams-from-cybercrime-group/?ftag=TR Ea988f1c&bhid=42420269&mid=12849801&cid=2176068089>

At least eight US states and the federal government have lost millions of dollars due to cybercrime scams targeting unemployment benefits and funding from the CARES Act proceeds, according to the Secret Service and the cybersecurity company Agari. In a report that has been grabbing headlines all week, Agari CEO and founder Patrick Peterson said Scattered Canary, a cybercrime group the company traced to Nigeria, has been able to fool the IRS and state governments into sending out more than \$4 million to fraudulent accounts.

[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/information-technology/information-security/security-news-digest>

**To learn more about information security issues and best practices, visit us at:**

<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.



# Security News Digest

Information Security Branch



**OCIO**

Office of the  
Chief Information Officer