





March 17th, 2020

Try our March Quiz – [Protecting Mobile Devices](#)

Cyber Hygiene for Corvid019 - <https://cyber.gc.ca/en/guidance/cyber-hygiene-covid-19>

This week's stories:

- [Canada can learn from U.S. cyber report, says expert](#) 
- [Only one woman applied for information security job, a clear signal that 'something isn't working right'](#) 
- [COVID-19 Testing Center Hit By Cyberattack](#)
- [US Govt Shares Tips on Securing VPNs Used by Remote Workers](#)
- [Surveillance Firm Banjo Used a Secret Company and Fake Apps to Scrape Social Media](#)
- [Media and e-commerce brands are top targets for phishing attacks](#)
- [Hackers are working harder to make phishing and malware look legitimate](#)
- [Clearer rules needed for facial recognition technology](#)
- [The bad guys are arming themselves with AI, but so are we, says Darktrace's country manager for Canada](#)

Canada can learn from U.S. cyber report, says expert 

<https://www.itworldcanada.com/article/canada-can-learn-from-u-s-cyber-report-says-expert/428387>

Canadian political and cyber leaders can learn lessons from a new U.S. congressional report on how the U.S. federal government should defend against internet-based threats, says a security expert.

The report by the bipartisan Cyberspace Solarium Commission issued Wednesday is "pretty cutting edge," said Christian Leuprecht a security and defence expert at Royal Military College and Queen's University in Kingston, Ont.

[Click link above to read more](#)

Only one woman applied for information security job, a clear signal that 'something isn't working right' 

<https://www.itworldcanada.com/article/only-one-woman-applied-for-information-security-job-a-clear-signal-that-something-isnt-working-right/428421>

Women are slowly increasing their numbers in cybersecurity-related jobs across Canada.

Still, Gayleen Gray, the assistant-vice-president and CTO of McMaster University was stunned at the response to her recent job posting for director of information security at the Hamilton, Ont. institution.

"Of 100 applications, just one woman," she told the Canadian Women in Cyber Security conference in Toronto this week. "That's awful... Something isn't working right."

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

COVID-19 Testing Center Hit By Cyberattack

<https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/>

Hospitals around the world struggle with ever-growing waves of COVID-19 infections but the efforts in one testing center in Europe are being hampered by cybercriminal activity.

Computer systems at the University Hospital Brno in the Czech Republic have been shut down on Friday due to a cyberattack that struck in the wee hours of the day.

This comes at a time when there are more than 140 confirmed infections in the country and around 4,800 people in quarantine. The government has declared a state of emergency and imposed stern restrictions on crossing the border.

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

US Govt Shares Tips on Securing VPNs Used by Remote Workers

<https://www.bleepingcomputer.com/news/security/us-govt-shares-tips-on-securing-vpns-used-by-remote-workers/>

The Department of Homeland Security's cybersecurity agency today shared tips on how to properly secure enterprise virtual private networks (VPNs) seeing that a lot of organizations have made working from home the default for their employees in response to the Coronavirus disease (COVID-19) pandemic.

"As organizations elect to implement telework, the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity," an alert published today says.

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

Surveillance Firm Banjo Used a Secret Company and Fake Apps to Scrape Social Media

https://www.vice.com/en_us/article/z3bgky/banjo-ai-used-secret-company-and-fake-apps-to-scrape-facebook-twitter

Banjo, an artificial intelligence firm that works with police used a shadow company to create an array of Android and iOS apps that looked innocuous but were specifically designed to secretly scrape social media, Motherboard has learned.

The news signifies an abuse of data by a government contractor, with Banjo going far beyond what companies which scrape social networks usually do. Banjo created a secret company named Pink Unicorn Labs, according to three former Banjo employees, with two of them adding that the company developed the apps. This was done to avoid detection by social networks, two of the former employees said.

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

Media and e-commerce brands are top targets for phishing attacks

<https://www.techrepublic.com/article/media-and-e-commerce-brands-are-top-targets-for-phishing-attacks/?ftag=TRa988f1c&bhid=42420269>

Phishing attacks try to trick unsuspecting users by mimicking well-known brands and companies. The idea is to create an email or webpage that emulates the look and layout of a legitimate brand. Though many brands are vulnerable to spoofed emails and pages, some are more popular than others among cybercriminals, according to a blog post from Akamai.

For its latest research released on Tuesday, Akamai discovered 1,221 domains, or 1,381 URLs, associated with phishing campaigns during late 2019 and early 2020. More than 20 different brands were used in these campaigns. But the majority of the brands, a full 84%, were from media and e-commerce industries. The rest of the URLs hit companies in the financial, high tech, and dating industries.

[Click link above to read more](#)

Hackers are working harder to make phishing and malware look legitimate

<https://www.techrepublic.com/article/hackers-are-working-harder-to-make-phishing-and-malware-look-legitimate/?ftag=TR Ea988f1c&bhid=42420269>

Even though the overall volume of malware dropped in 2019, phishing and business email compromise (BEC) went up sharply, according to Trend Micro's 2019 Cloud App Security Roundup. The company detected over a million instances of malware in 2018 and 960,000 in 2019. Trend Micro blocked nearly 400,000 attempted BEC attacks in 2018, which is 271% more than the previous year and 35% more credential phishing attempts than in 2018.

More than 11 million of the 12.7 million high-risk emails blocked in 2019 were phishing related, making up 89% of all blocked emails.

[Click link above to read more](#)

Clearer rules needed for facial recognition technology

<https://rabble.ca/columnists/2020/02/clearer-rules-needed-facial-recognition-technology>

In a previous column, I wrote about the dangers that some police technology poses for civil liberties. In that column, I addressed technology that police used to identify certain geographic areas as being more prone to crime in order to direct their forces to those areas (or perhaps to "target" those areas under the guise of a computer program "identifying" them). Now, with Toronto police Chief Mark Saunders' recent admission that some officers in the Toronto Police Service have been using a piece of facial recognition technology called Clearview AI software (named for the company that developed the software) since at least October 2019, we have another example of how law enforcement can use technology in a way that seriously threatens our civil liberties.

Clearview AI has apparently mined the internet for billions of photos of people, largely from social media sites and the open web (whereas other facial recognition technology providers relied upon government sources such as mugshots and driver's license photos).

[Click link above to read more](#)

The bad guys are arming themselves with AI, but so are we, says Darktrace's country manager for Canada

<https://www.itworldcanada.com/article/the-bad-guys-are-arming-themselves-with-ai-but-so-are-we-says-darktraces-country-manager-for-canada/427925>

David Masson is confident that the use of sophisticated artificial intelligence by hackers is not a matter of if, but a matter of when.

The Canadian country manager for security firm Darktrace, who has been involved in cybersecurity since the Cold War, is adamant that the same algorithms that helped Darktrace develop intelligent defence capabilities that mimic the human immune system will be used by hackers to deliver massive blows to enterprises and public infrastructure.

[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

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.

