



June 23rd, 2020

Try our June - [Connect with Care Quiz](#)

This week's stories:

- [Shopify, BlackBerry, and Ontario to help Canada launch contact tracing app](#) 
- [Why it's critical to shut the doors on cyber attackers now](#)
- [BlueLeaks data dump exposes over 24 years of police records](#)
- [Hackers use Google Analytics to steal credit cards, bypass CSP](#)
- [North Korea's state hackers caught engaging in BEC scams](#)
- [Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack](#)
- [Amazon 'thwarts largest ever DDoS cyber-attack'](#)

Shopify, BlackBerry, and Ontario to help Canada launch contact tracing app

<https://www.itworldcanada.com/article/shopify-blackberry-and-ontario-to-help-canada-launch-contact-tracing-app/432236>

Canadian Prime Minister Justin Trudeau is encouraging Canadians to download a new contact tracing app built on top of a free exposure notification solution developed by Shopify volunteers.

The application will first launch in Ontario early July, with a broader rollout across Canada expected “in the coming weeks.” Ontario is calling its version of the app COVID Alert. Trudeau emphasized that downloading the app will be entirely voluntary. Still, the more downloads it gets, he explained, the easier it will be to track the novel coronavirus that, as of June 18, has killed nearly 8,300 and infected 100,000 Canadians.

[Click link above to read more](#)

Why it's critical to shut the doors on cyber attackers now

<https://www.itworldcanada.com/article/why-its-critical-to-shut-the-doors-on-cyber-attackers-now/432277>

Cyber attacks are on the rise due to vulnerabilities created by the growth in remote work and new technologies. Now, it's time to fix the holes, according to a security expert.

“The attack surface is expanding with the quick transition to working from home,” said Chris Maroun, Global Director of Emerging Technologies with CyberArk, at a recent ITWC webinar. At the same time, emerging technologies, such as IoT and robotic process automation, are also increasing the potential points of attack, he said.

[Click link above to read more](#)

BlueLeaks data dump exposes over 24 years of police records

<https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/>

In what is being referred to as 'BlueLeaks,' a group called Distributed Denial of Secrets (DDoSecrets) has released a 269 GB data dump containing 24 years worth of records from over 200 police departments.

What can be observed "among the hundreds of thousands of documents" comprising FBI reports and bulletins are also full International Bank Account Numbers (IBANs), phone numbers, and email addresses.

DDoSecrets is similar to WikiLeaks, but with a commitment to make secrets public that even WikiLeaks chose to withhold.

[Click link above to read more](#)

Hackers use Google Analytics to steal credit cards, bypass CSP

<https://www.bleepingcomputer.com/news/security/hackers-use-google-analytics-to-steal-credit-cards-bypass-csp/>

Hackers are using Google's servers and the Google Analytics platform to steal credit card information submitted by customers of online stores.

A new method to bypass Content Security Policy (CSP) using the Google Analytics API disclosed last week has already been deployed in ongoing Magecart attacks designed to scrape credit card data from several dozen e-commerce sites.

This new tactic takes advantage of the fact that e-commerce web sites using Google's web analytics service for tracking visitors are whitelisting Google Analytics domains in their CSP configuration (a security standard used to block the execution of untrusted code on web apps).

[Click link above to read more](#)

North Korea's state hackers caught engaging in BEC scams

<https://www.zdnet.com/article/north-koreas-state-hackers-caught-engaging-in-bec-scams/>

At the ESET Virtual World security conference on Tuesday, security researchers from Slovak antivirus maker ESET have disclosed a new operation orchestrated by the Pyongyang regime's infamous state-sponsored hacker crews.

Codenamed "Operation In(ter)ception," this campaign targeted victims for both cyber-espionage and financial theft.

Speaking in a live stream to an audience of thousands, ESET security researcher Jean-Ian Boutin said the attacks have been carried out by members of the Lazarus Group -- codename given by security firms to North Korea's biggest hacking unit, part of the country's intelligence service.

[Click link above to read more](#)

Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack

<https://www.bbc.com/news/world-australia-46096768>

Australia's government and institutions are being targeted by ongoing sophisticated state-based cyber hacks, Prime Minister Scott Morrison says.

Mr Morrison said the cyber attacks were widespread, covering "all levels of government" as well as essential services and businesses.

He declined to identify a specific state actor and said no major personal data breaches had been made.

The attacks have happened over many months and are increasing, he said.

The prime minister said his announcement on Friday was intended to raise public awareness and to urge businesses to improve their defences.

But he stressed that "malicious" activity was also being seen globally, making it not unique to Australia.

[Click link above to read more](#)

Amazon 'thwarts largest ever DDoS cyber-attack'

<https://www.bbc.com/news/technology-53093611>

Amazon says its online cloud, which provides the infrastructure on which many websites rely, has fended off the largest DDoS attack in history.

Distributed denial of service (DDoS) attacks are designed to knock a website offline by flooding it with huge amounts of requests until it crashes.

Amazon Web Services (AWS) said the February attack had fired 2.3Tbps.

That is a little under half of all traffic BT sees on its entire UK network during a normal working day.

The previous record, set in 2018, was 1.7Tbps.

[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:

<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.

