







May 11, 2020

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

Save the Date for Security Day – <http://www.gov.bc.ca/securityday>

This week's stories:

- [Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid COVID-19](#) 
- [Canadian privacy commissioners urge caution on COVID-19 tracing apps](#) 
- [Second privacy breach complaint filed against Alberta Health Minister Tyler Shandro](#) 
- [Canada hit by COVID cheque fraud; Webex, Teams under attack, more COVID email scams and three big data breaches](#) 
- [GoDaddy Confirms Data Breach: What Customers Need to Know](#)
- [New Facial Recognition Tech Only Needs Your Eyes and Eyebrows](#)
- [Report: Microsoft's GitHub Account Gets Hacked](#)
- [Bad password habits continue with 53% admitting to using the same password](#)
- [North Korean hackers infect real 2FA app to compromise Macs](#)
- [Hacker group floods dark web with data stolen from 11 companies](#)
- [InfinityBlack Dismantled After Selling Millions of Credentials](#)
- [Thunderbolt ports vulnerable to hands-on hacks](#)

Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid COVID-19



<https://www.cbc.ca/news/canada/toronto/sidewalk-labs-cancels-project-1.5559370>

Sidewalk Labs, a Google-affiliated company, is abandoning its plan to build a high-tech neighbourhood on Toronto's waterfront, citing what it calls unprecedented economic uncertainty.

The project, dubbed Quayside, still didn't have all of the government approvals it needed to go ahead. Toronto citizens and civic leaders had raised concerns about the privacy implications of the project and

how much of the city's developing waterfront Sidewalk Labs wanted to control.

[Click link above to read more](#)

Canadian privacy commissioners urge caution on COVID-19 tracing apps

<https://www.itworldcanada.com/article/canadian-privacy-commissioners-urge-caution-on-covid-19-tracing-apps/430419>

With federal, provincial and territorial leaders discussing a national approach to COVID-19 tracking apps, privacy commissioners across the country have issued a joint statement urging governments to follow at least nine principles.

One is signing “strong contractual measures with developers” before approving an app that ensure that non-authorized parties can’t access collected data, and that data will not be used for any purpose other than its intended public health purpose.

[Click link above to read more](#)

Second privacy breach complaint filed against Alberta Health Minister Tyler Shandro

<https://www.cbc.ca/news/canada/edmonton/second-privacy-complaint-against-shandro-1.5560907>

Alberta Health Minister Tyler Shandro is the subject of another privacy breach complaint — his second in a month — after his political staff accessed and released billing information from an Edmonton clinic to rebut allegations made during an NDP news conference.

The billing information had been anonymized — stripped of data that could identify patients. A health law professor said it is unlikely there was a breach of the provincial Health Information Act (HIA).

[Click link above to read more](#)

Canada hit by COVID cheque fraud; Webex, Teams under attack, more COVID email scams and three big data breaches

<https://www.itworldcanada.com/article/cyber-security-today-canada-hit-by-covid-cheque-fraud-webex-teams-under-attack-more-covid-email-scams-and-three-big-data-breaches/430454>

It didn't take long for cybercriminals to take advantage of the Canadian government's multi-billion dollar pandemic payments program for consumers. Cheques under the Canada Emergency Response Benefit, or CERB, began rolling out in early April. But according to an Israeli security company called Kela Research, criminals soon began selling editable digital copies of cheques on the dark web. A criminal can either purchase a digital file and fill in their own name or have a criminal service do the editing for them. Typically, the cheque is put into a bank by a mobile deposit in what is called a “drop” account, one of a number of accounts that has been opened by criminals some time ago with fake ID and are used for transferring money. Criminals often buy and sell drop accounts from each other.

[Click link above to read more](#)

GoDaddy Confirms Data Breach: What Customers Need To Know

<https://www.forbes.com/sites/daveywinder/2020/05/05/godaddy-confirms-data-breach-what-19-million-customers-need-to-know/#4a214ec31daa>

The world's largest domain registrar, GoDaddy, with 19 million customers, has disclosed a data breach impacting web hosting account credentials.

With more than 19 million customers, 77 million domains managed, and millions of websites hosted, most everyone has heard of GoDaddy. According to Bleeping Computer, which broke the news yesterday evening, an as yet unknown number of customers have been informed that their web hosting account credentials had been compromised.

[Click link above to read more](#)

New Facial Recognition Tech Only Needs Your Eyes and Eyebrows

<https://onezero.medium.com/new-facial-recognition-tech-only-needs-your-eyes-and-eyebrows-9e7dc155cd7f>

The term “facial recognition” typically refers to technology that can identify your entire face. *How* that recognition happens can vary, and can include infrared or lidar technology. Either way, you need the geometry of a person’s entire face to make it work.

But in the coronavirus era, when everyone is advised to wear a mask, exposed faces are increasingly rare. That’s breaking facial recognition systems everywhere, from iPhones to public surveillance apparatuses.

[Click link above to read more](#)

Report: Microsoft’s GitHub Account Gets Hacked

<https://threatpost.com/report-microsofts-github-account-gets-hacked/155587/>

The Shiny Hunters hacking group said it stole 500 GB of data from the tech giant’s repositories on the developer platform, which it owns.

Hackers have broken into Microsoft’s GitHub account and stolen 500 GB of data from the tech giant’s own private repositories on the developer platform, according to published reports.

[Click link above to read more](#)

Bad password habits continue with 53% admitting to using the same password

<https://www.techrepublic.com/article/bad-password-habits-continue-with-53-admitting-to-using-the-same-password/?ftag=TR Ea988f1c&bhid=42420269&mid=12822452&cid=2176068089>

Ahead of World Password Day, a survey finds management is worse than junior staff at practicing good password hygiene, according to SecureAuth.

Just in time for World Password Day Thursday, password reuse remains rampant, with 53% of people admitting they use the same password for different accounts, which exemplifies poor password hygiene, according to a newly released report by identity company SecureAuth.

[Click link above to read more](#)

North Korean hackers infect real 2FA app to compromise Macs

<https://www.bleepingcomputer.com/news/security/north-korean-hackers-infect-real-2fa-app-to-compromise-macs/>

Hackers have hidden malware in a legitimate two-factor authentication (2FA) app for macOS to distribute DacIs, a remote access trojan associated with the North Korean Lazarus group.

DacIs has been used to target Windows and Linux platforms and the recently discovered RAT variant for macOS borrows from them much of the functionality and code.

[Click link above to read more](#)

Hacker group floods dark web with data stolen from 11 companies

<https://www.bleepingcomputer.com/news/security/hacker-group-floods-dark-web-with-data-stolen-from-11-companies/>

A hacking group has started to flood a dark web hacking marketplace with databases containing a combined total of 73.2 million user records over 11 different companies.

For the past week, a hacking group known as Shiny Hunters has been busy selling a steady stream of user databases from alleged data breaches.

[Click link above to read more](#)

InfinityBlack Dismantled After Selling Millions of Credentials

<https://threatpost.com/infinityblack-dismantled-millions-credentials/155525/>

In the Europol-led takedown, police shut down databases with more than 170 million entries.

The InfinityBlack hacking group, which is responsible for selling millions of stolen credentials, has been dismantled.

[Click link above to read more](#)

Thunderbolt ports vulnerable to hands-on hacks

<https://www.scmagazine.com/home/security-news/vulnerabilities/thunderbolt-ports-vulnerable-to-hands-on-hacks/>

A threat actor with just five minutes of direct access to a computer's Thunderbolt port can steal encrypted data and clean out the device's system memory due to seven specific security lapses in the Intel-developed port.

The vulnerabilities, named Thunderspy, were brought to light by Björn Ruytenberg, a graduate student at the Eindhoven University of Technology in the Netherlands, who reported a threat actor would need direct access to the device to implement the hack, but it would only take about five minutes to accomplish the task.

[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.

