Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer

April 14, 2020

Try our April Quiz – Working Remotely

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

This week's stories:

- **Canadian health researchers and firms targeted with COVID-19 phishing** 🇨🇦
- **Canadian passengers from virus-stricken Zaandam cruise ship hit by federal gov't privacy breach** 🇨🇦
- **Russian hackers tried to steal San Francisco airport Windows accounts**
- **Give employees rules on how to choose videoconferencing platforms**
- **We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World**
- **Google can still use Bluetooth to track your Android phone when Bluetooth is turned off**
- **Who has banned Zoom? Google, NASA, and more**

Canadian health researchers and firms targeted with COVID-19 phishing

https://www.itworldcanada.com/article/canadian-health-researchers-and-firms-targeted-with-covid-19-phishing/429551

COVID-19 phishing scams have been reportedly going out to consumers, trying to get them to buy face masks, protective gear, phony medical cures as well as give up bank or government login credentials to get government-backed coronavirus financial aid.

But governments and health-related institutions also have to be on the lookout for scams, Palo Alto Networks warned today.

Click link above to read more

Canadian passengers from virus-stricken Zaandam cruise ship hit by federal gov't privacy breach

https://www.cbc.ca/news/business/zaandam-cruise-privacy-breach-canadians-1.5531124

After enduring a cruise with a COVID-19 outbreak and four deaths, the 247 Canadian passengers who were aboard the Holland America Line ship, the MS Zaandam, face a new problem: a privacy breach by the federal government.

"Didn't we go through enough? Now we have to have a breach too?" said passenger Margaret Tilley of Nanaimo, B.C. "I'm just very angry that they would allow something like this to happen."

In a detailed email Global Affairs Canada sent Canadian passengers during the Easter holiday weekend, it explained that, "due to an administrative error," it had mistakenly sent them an email on April 1 with an attachment containing personal information on each passenger — including their address, date of birth, email, phone number and passport number.

Click link above to read more

Russian hackers tried to steal San Francisco airport Windows accounts

https://www.bleepingcomputer.com/news/security/russian-hackers-tried-to-steal-san-francisco-airport-windows-accounts/

The hack of employee web sites belonging to the San Francisco International Airport has been attributed to a Russian hacker group who used the SMB protocol to steal Windows passwords.

Last week BleepingComputer broke the story that the San Francisco International Airport (SFO) experienced a cyberattack in March 2020 whose goal was to steal the Windows logins for employees of the airport.

Click link above to read more

Give employees rules on how to choose videoconferencing platforms

https://www.itworldcanada.com/article/basic-security-hygiene-is-key-and-more-advice-on-securing-videoconferencing-platforms/429496

When the COVID-19 crisis broke open a month ago and forced organizations to make employees work from home, video conferencing was seen as a way to allow managers to keep on top of what staff are doing.

Now, amid recent complaints that Zoom and others have security and privacy flaws, a Forrester Research advisor is urging management to give employees rules on how to choose a collaboration platform and use it securely.

Click link above to read more

We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World

https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9

In an attempt to stem the tide of the coronavirus pandemic, more than 25 governments around the world have instituted temporary or indefinite efforts to single out infected individuals or maintain quarantines. Many of these efforts, in turn, undermine personal privacy.

It’s a complex trade-off: Governments need information to create containment strategies and know where to focus resources. At the same time, governments have a way of holding onto tools that undermine citizens’ privacy long after the moment of crisis has passed. Take, for example, the United States’ 2001 Patriot Act, which was passed in response to the 9/11 attacks. The Patriot Act gave the government broad surveillance powers with little oversight, including demanding customer data from telecoms without court approval. Twenty years later, it’s still around.

Click link above to read more

Google can still use Bluetooth to track your Android phone when Bluetooth is turned off

https://qz.com/1169760/phone-data/

When it comes to tracking the precise location of an Android user’s phone, Google appears to use every means available—including Bluetooth-based location information transmitted to the company when the user might think they have Bluetooth turned off entirely.

A Quartz investigation found that a user can turn Bluetooth off on their smartphone running Google’s Android software, and the phone will continue to use Bluetooth to collect location-related data and transmit that data to Google. It does this by sending Google, among other things, the unique identifier codes of Bluetooth broadcasting devices it encounters. Such devices, known as beacons, are often used in stores, museums, and other public places to help phones ascertain their locations within buildings. Alphabet-owned Google does the tracking in part so advertisers can target “more useful” digital ads to users, but Quartz discovered that the company taps into an array of signals that can yield an individual’s whereabouts even when the user thinks they’ve disabled such tracking.

Click link above to read more

Who has banned Zoom? Google, NASA, and more

https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/?ftag=TREa988f1c&bhid=42420269&mid=12787571&cid=2176068089

Video conferencing app Zoom has had a massive increase in users because of new remote work requirements due to the COVID-19 pandemic. That spike in users also exposed a growing list of security flaws: Zoom bombing trolls have emerged, user email addresses and photos have leaked, calls aren't being end-to-end encrypted, and flaws found in the Zoom installer allow an attacker to gain root access to computers that run a malicious version of it. Even Zoom CEO Eric Yuan admitted the company moved too fast and made missteps.

These security flaws have prompted some organizations, companies, governments, government agencies, and schools to ban Zoom or restrict its use. The following list will be updated if more organizations ban or restrict the use of Zoom.

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

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
BRITISH COLUMBIA
OCIO | Office of the Chief Information Officer