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

March 31st, 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:

- **Some Ontario beer chain outlets forced to use cash-only after cyber attack 🇨🇦**
- **Staying cyber-healthy during COVID-19 isolation 🇨🇦**
- **RCMP, prime minister warn of text scam related to COVID-19 relief🇨🇦**
- **Scammers have never had a more target-rich environment amid coronavirus pandemic: experts**
- **Hackers Take Advantage of Zoom's Popularity to Push Malware**
- **Phishing Attack Says You're Exposed to Coronavirus, Spreads Malware**
- **FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS**
- **"Corona antivirus" infects victims with malware**
- **Why Microsoft's Office 365 has become an all-access pass for phishers to exploit**

Some Ontario beer chain outlets forced to use cash-only after cyber attack 🇨🇦

https://www.itworldcanada.com/article/some-ontario-beer-chain-outlets-forced-to-use-cash-only-after-cyber-attack/429003

Some of Ontario's 450 industry-owned retail beer outlets known as The Beer Store have been forced to accept only cash for sales after a cyber attack.

On Thursday morning, the company put out the following tweet: "Overnight, we were subjected to a cyber attack and are following internal response protocols. Some of our locations are operating with cash only."

Click link above to read more

Staying cyber-healthy during COVID-19 isolation 🇨🇦

https://cyber.gc.ca/en/news/staying-cyber-healthy-during-covid-19-isolation

Canadians are staying vigilant during this challenging period. We're washing our hands, keeping our distance, coughing into tissues or elbows, and doing our part to keep the healthcare system from becoming overloaded. We're listening to public health officials and provincial and federal leaders, scouring the news, and visiting Canada.ca/coronavirus for new information.

But not everyone has the public's best interests at heart. Cyber threat actors are taking advantage of people's heightened levels of concern and legitimate fear around COVID-19, trying to spread misinformation and scam people out of their money or private data.

Click link above to read more

RCMP, prime minister warn of text scam related to COVID-19 relief 🇨🇦

https://www.nanaimobulletin.com/news/rcmp-prime-minister-warn-of-text-scam-related-to-covid-19-relief/?utm_source=dlvr.it&utm_medium=twitter

There are numerous COVID-19 scams and frauds being perpetrated, but one in particular is raising concern at the moment.

Prime Minister Justin Trudeau, in an address from Ottawa this morning, March 26, said he’s “sorry to say” that there’s a text scam going on around the federal government’s new emergency response benefit.

“I want to remind everyone that the government’s website is the best place to find reliable information on everything we are doing,” Trudeau said.

Click link above to read more

Scammers have never had a more target-rich environment amid coronavirus pandemic: experts

https://globalnews.ca/news/6741981/coronavirus-covid-19-scams/

The coronavirus pandemic has created a perfect storm for scammers seeking to defraud panicked, isolated and emotionally vulnerable targets, experts say.

“I think we are in for a wild ride,” said Frank McKenna, an anti-fraud expert who has studied organized fraud networks in Canada and the United States. “We have this unprecedented global fear and panic. I’ve never seen an environment quite as ripe for fraud as now.”

Click link above to read more

Hackers Take Advantage of Zoom's Popularity to Push Malware

https://www.bleepingcomputer.com/news/security/hackers-take-advantage-of-zooms-popularity-to-push-malware/

Attackers are attempting to take advantage of Zoom's increasing user base since the COVID-19 outbreak started by registering hundreds of new Zoom-themed domains for malicious purposes.

Videoconferencing software company Zoom provides its customers with a cloud-based communication platform that can be used for audio and video conferencing, online meetings, as well as chat and collaboration via mobile, desktop, and telephone systems.

The company has seen a drastic increase of new monthly active users since the start of 2020 as millions of employees are now working from home, adding roughly 2.22 million new ones this year alone while only 1.99 million were added through 2019.

Click link above to read more

Phishing Attack Says You're Exposed to Coronavirus, Spreads Malware

https://www.bleepingcomputer.com/news/security/phishing-attack-says-youre-exposed-to-coronavirus-spreads-malware/

A new phishing campaign has been spotted that pretends to be from a local hospital telling the recipient that they have been exposed to the Coronavirus and that they need to be tested.

With the Coronavirus pandemic affecting all corners of the world, we continue to see phishing actors try to take advantage of the fear and anxiety it is provoking to scare people into opening malicious email attachments.

In a new low, a threat actor is pretending to be from a local hospital telling the recipient that they have been in contact with a colleague, friend, or family member who has tested positive for the COVID-19 virus.

Click link above to read more

FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS

https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/

Hackers from the FIN7 cybercriminal group have been targeting various businesses with malicious USB devices acting as a keyboard when plugged into a computer. Injected commands download and execute a JavaScript backdoor associated with this actor.

In a FLASH alert on Thursday, the FBI warns organizations and security professionals about this tactic adopted by FIN7 to deliver GRIFFON malware.

The attack is a variation of the “lost USB” ruse that penetration testers have used for years in their assessments quite successfully and one incident was analyzed by researchers at Trustwave.

Click link above to read more

"Corona antivirus" infects victims with malware

https://www.techradar.com/news/corona-antivirus-infects-victims-with-malware

Cybercriminals continue to leverage the ongoing coronavirus outbreak for their own gain by launching numerous scam campaigns which use Covid-19 as a lure to trick users into installing a variety of malware and data stealers.

In the latest scam, discovered by Malwarebytes, cybercriminals have set up a website advertising “Corona Antivirus - World's best protection” which tries to trick users into installing antivirus software that supposedly has the capabilities to protect users from becoming infected with the virus in real life. The creators of the site have even provided more details on how their solution works, saying:

“Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.”

Click link above to read more

Why Microsoft’s Office 365 has become an all-access pass for phishers to exploit

https://technewsextra.com/why-microsofts-office-365-has-become-an-all-access-pass-for-phishers-to-exploit/

Cybercriminals are tapping into the widespread use of Office 365 to spread malware in an attempt to steal account credentials, according to email security provider Vade Secure.

Phishing emails are a key way that cybercriminals use social engineering to try to deploy malware. By impersonating well-known companies and products, such emails attempt to ensnare people who use them. And the more popular the product or brand, the greater the number of potential victims. With so many people and organizations using Microsoft Office 365,
phishers
who exploit this brand can target a vast amount of people as a way to steal their account credentials, as described by Vade Secure.

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