





November 3rd, 2020

Challenge yourself during Cyber Security Awareness Month

Try our November - 'Phishing' Quiz

This week's stories:

- **Cyberattack on Montreal's west end health agency leads it to unplug from internet **
- **Cadillac Fairview covertly collected images of 5M shoppers across Canada: privacy commissioners **
- **Over 1M Lazada RedMart accounts sold online after data breach**
- **UHS restores hospital systems after Ryuk ransomware attack**
- **Cyberattack shuts down Saskatchewan Polytechnic**
- **FBI: Hospitals and healthcare providers face imminent ransomware threat**
- **Wroba Mobile Banking Trojan Spreads to the U.S. via Texts**
- **Supreme Court ruling could make robocalls 'virtually unstoppable'**

Cyberattack on Montreal's west end health agency leads it to unplug from internet 

<https://www.cbc.ca/news/canada/montreal/cyber-security-west-island-health-agency-1.5781734>

A health agency in Montreal's west end, the CIUSSS du Centre-Ouest-de-l'Île-de-Montréal, has disconnected from the internet and barred remote access after a cybersecurity intrusion was discovered.

The personal information of staff and patients has not been accessed or compromised, said the health agency's head, Dr. Lawrence Rosenberg, during a news briefing Thursday afternoon.

[Click link above to read more](#)

Cadillac Fairview covertly collected images of 5M shoppers across Canada: privacy commissioners 

<https://globalnews.ca/news/7429905/cadillac-fairview-facial-recognition-investigation-findings/>

An investigation into Cadillac Fairview's use of facial recognition technology at a dozen Canadian malls found the real estate company collected the images of five million unsuspecting shoppers from across the country.

The results of the investigation, conducted by the federal, Alberta and B.C. privacy commissioners, were released on Thursday.

[Click link above to read more](#)

Over 1M Lazada RedMart accounts sold online after data breach

<https://www.bleepingcomputer.com/news/security/over-1m-lazada-redmart-accounts-sold-online-after-data-breach/>

Singapore's largest online grocery store Lazada Redmart has suffered a data breach after 1.1 million user accounts were put up for sale on a hacker forum.

The database dump containing sensitive customer is priced at \$1,500.

[Click link above to read more](#)

UHS restores hospital systems after Ryuk ransomware attack

<https://www.bleepingcomputer.com/news/security/uhs-restores-hospital-systems-after-ryuk-ransomware-attack/>

Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, says that it has managed to restore systems after a September Ryuk ransomware attack.

UHS has over 90,000 employees who provide healthcare services to roughly 3.5 million patients every year through a network of more than 400 healthcare facilities in the US and the UK.

[Click link above to read more](#)

Cyberattack shuts down Saskatchewan Polytechnic

<https://globalnews.ca/news/7436670/cyberattack-saskatchewan-polytechnic/>

Online and in-person classes have been cancelled at Saskatchewan Polytechnic following a cybersecurity attack.

School officials said classes are cancelled until Nov. 5 while IT staff work with outside experts to restore systems, with the first priority restoring online learning.

"The institute continues to assess the extent of the cybersecurity incident with external experts and law enforcement," Sask. Polytech said in a statement.

"There is no reason to conclude at this point that any personal information has been compromised."

[Click link above to read more](#)

FBI: Hospitals and healthcare providers face imminent ransomware threat

<https://www.techrepublic.com/article/fbi-hospitals-and-healthcare-providers-face-imminent-ransomware-threat/?ftag=TR Ea988f1c&bhid=42420269&mid=13150964&cid=2176068089>

The FBI warns of a threat against the healthcare sector from Ryuk ransomware, and one that's already affected some hospitals.

As the coronavirus started to spread earlier this year, a few ransomware gangs promised to leave hospitals and healthcare facilities alone so they could focus on battling the pandemic. So much for those promises. In fact, the healthcare industry continues to be a prime target for ransomware, so much so that the FBI and two other government agencies are now warning this sector of impending attacks using the infamous Ryuk ransomware.

[Click link above to read more](#)

Wroba Mobile Banking Trojan Spreads to the U.S. via Texts

<https://threatpost.com/wroba-mobile-banking-trojan-spreads-us/160785/>

The Roaming Mantis group is targeting the States with a malware that can steal information, harvest financial data and send texts to self-propagate.

The Wroba mobile banking trojan has made a major pivot, targeting people in the U.S. for the first time.

According to researchers at Kaspersky, a wave of attacks are taking aim at U.S. Android and iPhone users in an effort that started on Thursday. The campaign uses text messages to spread, using fake notifications for “package deliveries” as a lure.

[Click link above to read more](#)

Supreme Court ruling could make robocalls ‘virtually unstoppable’

<https://finance.yahoo.com/news/supreme-court-ruling-could-make-robocalls-virtually-unstoppable-195858154.html?guccounter=1>

Facebook (FB) is fighting a case in the Supreme Court. It's not about fake news, foreign influence, censorship, or antitrust issues – it's about robocalls.

This is the second time in 2020 that the Supreme Court has heard a case involving robocalls.

Efforts to fight robocalls through new legislation foundered this year as the divided Congress left out key provisions that defined exactly what a robocall really is.

[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.



Security News Digest
Information Security Branch



OCIO

Office of the
Chief Information Officer