

April 18, 2023

Challenge yourself with our [Drop Shipping Scam Quiz!](#)

[This past week's stories:](#)

- 🍁 [Gateway Casinos to remain closed after cyber attack: Officials](#)
- 🍁 [Cyber attack knocks out service on NCC's website](#)
- 🍁 [Pro-Russia hackers say they were behind Hydro-Quebec cyberattack](#)
- 🍁 [N.W.T. gov't spent \\$716,000 to address November cybersecurity breach](#)
- 🍁 [Pro-Russian hackers suspected in cyber attacks on Canadian ports](#)
- 🍁 [Human-centred approach essential to an effective cybersecurity strategy: Gartner](#)

[WhatsApp introduces new device verification feature to prevent account takeover attacks](#)

[Google launches new cybersecurity initiatives to strengthen vulnerability management](#)

[Wireshark 4.0.5 released – what's new!](#)

[Darktrace denies getting hacked after ransomware group names company on leak site](#)

[Cyber attack: Data from charities stolen in ransomware attack](#)

[ChatGPT account take over vulnerability let hackers gain user's online account](#)

[Russia's data breaches increase 42-fold in 2022 – Report](#)

Gateway Casinos to remain closed after cyber attack: Officials

More than 30 hours after Gateway Casinos and Entertainment abruptly shut down Casino Rama and its other Ontario casinos, the company has confirmed it was a victim of a cyber attack.

<https://www.orilliamatters.com/local-news/gateway-casinos-to-remain-closed-after-cyber-attack-officials-6867813>

Click above link to read more.

[Back to top](#)

Cyber attack knocks out service on NCC's website

A spokesperson for the National Capital Commission said Friday that the federal agency has been the victim of a “denial of service” attack that knocked down its webpage and other services.

<https://ottawacitizen.com/news/local-news/cyber-attack-knocks-out-service-on-nccs-website>

Click above link to read more.

[Back to top](#)

Pro-Russia hackers say they were behind Hydro-Quebec cyberattack

A pro-Russia hacker group has claimed responsibility for a cyber-attack on the Hydro-Quebec website Thursday morning.

<https://montreal.ctvnews.ca/pro-russia-hackers-say-they-were-behind-hydro-quebec-cyberattack-1.6353627>

Click above link to read more.

[Back to top](#)

N.W.T. gov't spent \$716,000 to address November cybersecurity breach

The Northwest Territories government says it spent \$716,000 to address a cyberattack in November.

<https://www.cbc.ca/news/canada/north/n-w-t-gov-t-spent-716-000-to-address-cybersecurity-breach-1.6807899>

Click above link to read more.

[Back to top](#)

Pro-Russian hackers suspected in cyber attacks on Canadian ports

Several ports in Canada suffered multiple cyber attacks this week. The Ports of Halifax, Montreal, and Québec were targeted by a 'denial-of-service attack' which flooded their websites with traffic, causing them to crash.

<https://www.porttechnology.org/news/pro-russian-hackers-suspected-in-cyber-attacks-on-canadian-ports/>

Click above link to read more.

[Back to top](#)

Human-centred approach essential to an effective cybersecurity strategy: Gartner

Security leaders should rethink their balance of investments across technology and human-centric security design practices, Gartner says in a new report detailing the top cybersecurity trends for 2023.

<https://www.itbusiness.ca/news/human-centred-approach-essential-to-an-effective-cybersecurity-strategy-gartner/124740>

Click above link to read more.

[Back to top](#)

WhatsApp introduces new device verification feature to prevent account takeover attacks

Popular instant messaging app WhatsApp on Thursday announced a new account verification feature that ensures that malware running on a user's mobile device doesn't impact their account.

<https://thehackernews.com/2023/04/whatsapp-introduces-new-device.html>

Click above link to read more.

[Back to top](#)

Google launches new cybersecurity initiatives to strengthen vulnerability management

Google on Thursday outlined a set of initiatives aimed at improving the vulnerability management ecosystem and establishing greater transparency measures around exploitation.

<https://thehackernews.com/2023/04/google-launches-new-cybersecurity.html>

Click above link to read more.

[Back to top](#)

Wireshark 4.0.5 released – what's new!

Wireshark, One of the world's most popular network packet analyzers, released Wireshark 4.0.5 with the fixes of several bugs, updated protocol support, and a few enhancements.

<https://cybersecuritynews.com/wireshark-4-0-5/>

Click above link to read more.

[Back to top](#)

Darktrace denies getting hacked after ransomware group names company on leak site

Cybersecurity company Darktrace issued a statement on Thursday after it was named on the leak website of the LockBit ransomware group.

<https://www.securityweek.com/darktrace-denies-getting-hacked-after-ransomware-group-names-firm-on-leak-site/>

Click above link to read more.

[Back to top](#)

Cyber attack: Data from charities stolen in ransomware attack

Hackers have stolen data from charities and community organisations in a cyber attack on a Londonderry-based IT company.

<https://www.bbc.com/news/uk-northern-ireland-65297324>

Click above link to read more.

[Back to top](#)

ChatGPT account take over vulnerability let hackers gain user's online account

A renowned security analyst and bug hunter, Nagli (@naglinagli), recently uncovered a critical security vulnerability in ChatGPT.

<https://cybersecuritynews.com/chatgpt-account-take-over-vulnerability/>

Click above link to read more.

[Back to top](#)

Russia's data breaches increase 42-fold in 2022 – Report

The number of data breaches in Russia surged last year and is on course to increase further in 2023, the RBC news website reported Monday, citing data from cyber-security firms.

<https://www.themoscowtimes.com/2023/04/17/russias-data-leaks-skyrocket-in-2022-rbc-a80851>

Click above link to read more.

[Back to top](#)

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.

