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

November 7, 2023

Challenge yourself with our AI Quiz!

Register for Security Day - November 21-22, 2023!

Cybersecurity Issue of the Week: **PHISHING**

✪ Read our **PHISHING INFOSHEET** to learn more.

This past week's stories:

🍁 **Windsor hospital sending cancer patients out-of-town for treatment after cyberattack**
🍁 **What ransomware hackers do with data they extort — and why it can be lucrative**
🍁 **Public institutions, critical infrastructure cyberattacks a growing trend**
🍁 **Canada bans WeChat and Kaspersky apps on government devices**
🍁 **Canadian companies averaged 25 cybersecurity incidents in past year**
Boeing says 'cyber incident' hit parts business after ransom threat
Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive
Huawei, Tencent among top cybersecurity patent holders as China fosters own tech, report says
✪ **Hilb Group cyber attack: 81K people's personal information exposed**
4,076,530 systems hacked using gaming-related cyber attacks
Iranian hackers launches destructive cyberattacks on Israeli tech and education sectors
SecuriDropper: New Android Dropper-as-a-Service bypasses Google's defenses

---

Windsor hospital sending cancer patients out-of-town for treatment after cyberattack

If Windsor's Mike Rovers wants treatment to fight his prostate cancer, he'll have to move to Kitchener for five weeks.

https://windsorstar.com/news/local-news/windsor-regional-hospital-sending-cancer-patients-out-of-town-for-treatment-after-cyberattack

Click above link to read more.

Back to top

What ransomware hackers do with data they extort — and why it can be lucrative

Hospital systems across southwestern Ontario have been offline for 11 days after a ransomware attack that has led to data being exposed online.

https://www.cbc.ca/news/canada/windsor/ransomware-hackers-data-extort-1.7016157

Click above link to read more.

Back to top

Public institutions, critical infrastructure cyberattacks a growing trend

The cyberattack against five southwestern Ontario hospitals in Windsor-Essex, Sarnia and Chatham-Kent this past week is just part of a growing number of such attacks on public institutions and critical infrastructure, says Trish Dyl, the director of corporate training and cyber range at Rogers Cybersecure Catalyst.

https://windsorstar.com/news/local-news/public-institutions-critical-infrastructure-cyberattacks-a-growing-trend

Click above link to read more.

Back to top

Canada bans WeChat and Kaspersky apps on government devices

Canada on Monday (October 31) announced a ban on the use of apps from Tencent and Kaspersky on government mobile devices, citing an "unacceptable level of risk to privacy and security."

https://thehackernews.com/2023/10/canada-bans-wechat-and-kaspersky-apps.html

Click above link to read more.

Back to top

Canadian companies averaged 25 cybersecurity incidents in past year

Eighty-one percent of Canadian organizations had at least 25 cybersecurity incidents in the last 12 months, according to EY's 2023 Cybersecurity Leadership Insights study.

https://www.consulting.ca/news/3761/canadian-companies-averaged-25-cybersecurity-incidents-in-past-year

Click above link to read more.

Back to top

Boeing says 'cyber incident' hit parts business after ransom threat

Boeing, one of the world's largest defense and space contractors, said on Wednesday it is investigating a cyber incident that impacted elements of its parts and distribution business and cooperating with a law enforcement probe into it.

https://www.cnbc.com/2023/11/01/boeing-investigating-cyber-incident-affecting-parts-business.html

Click above link to read more.

Back to top

Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive

A new study suggests cybersecurity skills gaps can be worse than total workforce shortages.

https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html

Click above link to read more.

Back to top

Huawei, Tencent among top cybersecurity patent holders as China fosters own tech, report says

Chinese companies have gained ground in global patent holdings in the cybersecurity technology sector amid growing U.S.-China tensions, according to a report from Nikkei Asia on Sunday.

https://www.cnbc.com/2023/11/06/huawei-tencent-grow-in-patent-holdings-as-china-fosters-own-tech-report.html

Click above link to read more.

Back to top

Hilb Group cyber attack: 81K people’s personal information exposed

The Hilb Group Operating Company, LLC, a Maryland-based company, has disclosed a major data breach that has affected 81,539 individuals, including 105 Maine residents.

https://cybersecuritynews.com/hilb-group-cyber-attack/

Click above link to read more.

Back to top

4,076,530 systems hacked using gaming-related cyber attacks

As the gaming industry grows in income and player base, cybercriminals find it an attractive target. Anticipated and already well-known games are frequently utilized as a lure in malicious campaigns.

https://cybersecuritynews.com/4076530-systems-hacked/

Click above link to read more.

Back to top

Iranian hackers launches destructive cyberattacks on Israeli tech and education sectors

Israeli higher education and tech sectors have been targeted as part of a series of destructive cyber attacks that commenced in January 2023 with an aim to deploy previously undocumented wiper malware.

https://thehackernews.com/2023/11/iranian-hackers-launches-destructive.html

Click above link to read more.

Back to top

SecuriDropper: New Android Dropper-as-a-Service bypasses Google's defenses

Cybersecurity researchers have shed light on a new dropper-as-a-service (DaaS) for Android called SecuriDropper that bypasses new security restrictions imposed by Google and delivers the malware.

https://thehackernews.com/2023/11/securidropper-new-android-dropper-as.html

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer