January 24, 2023

Challenge yourself with our Cyber Security Resolutions Quiz!

This past week's stories:

- **Feds confirm National Research Council was hit by cyber attack**
- **Why London's IT staff say $1M is needed to protect the city from cyber attacks**
- **B.C. school district investigating data breach affecting up to 19,000 people**
- **Exco Technologies hit by cybersecurity incident at three factories**
- **Nunavut power utility's servers hit by cyber attack**
- **Cambrian College amps up cybersecurity program as industry hits 'turning point'**
- **Canada: Cybersecurity chief warns about data-harvesting apps**

Mailchimp hit again by social media attack

KFC, Pizza Hut parent shuts UK restaurants after cyber attack

Cyber-crime gangs' earnings slide as victims refuse to pay

PayPal data breach – thousands of users' accounts compromised

Roaming Mantis spreading mobile malware that hijacks Wi-Fi routers' DNS settings

---

Feds confirm National Research Council was hit by cyber attack

A "cyber incident" that knocked the National Research Council offline last year was a foreign attack, the agency confirms. It would not elaborate, according to Blacklock's Reporter.

"The audit report will not be published," the council said in a statement.

https://www.westernstandard.news/news/feds-confirm-national-research-council-was-hit-by-cyber-attack/article_0dec93d0-98ce-11ed-b487-83f76e4ff3bf.html

Click above link to read more.

Back to top

Why London's IT staff say $1M is needed to protect the city from cyber attacks

The City of London could spend more than $1 million to shore up and maintain municipal cyber-defences if a proposed amendment to the budget is approved by council.

The total price tag of $1,009,000 was carefully thought out by city staffers, who say the need was identified through a series of reviews and projects designed to test for vulnerabilities and gauge the City's current security situation.

"Cities across the globe, including London, are seeing increases in the volume, diversity and complexity of cyber attacks," said Mat Daley, the director of information technology services for the City of London.

https://www.cbc.ca/news/canada/london/london-cyber-attack-defence-1.6719410

Click above link to read more.

Back to top

B.C. school district investigating data breach affecting up to 19,000 people

The Maple Ridge-Pitt Meadows School District is warning its school community about a data breach involving more than 19,000 records.

In a bulletin posted Thursday, the district said it is investigating how files containing first names, last names, schools/departments, district email addresses and student grades were released.

https://globalnews.ca/news/9425599/b-c-school-district-data-breach/

Click above link to read more.

Back to top

Exco Technologies hit by cybersecurity incident at three factories

Exco Technologies Ltd. says three of its factories have been hit by what it is calling a cybersecurity incident.

The company says it has taken steps to secure its systems and mitigate the impact to the company's data and operations and that it is in the process of bringing the systems it temporarily disabled back online.

https://www.midlandtoday.ca/national-business/exco-technologies-hit-by-cybersecurity-incident-at-three-factories-6420034

Click above link to read more.

Back to top

Nunavut power utility's servers hit by cyber attack

The territorial utility that provides power to Nunavut can't say yet if customer data was copied after a cyber attack earlier this week.

Qulliq Energy Corporation (QEC) was targeted in a cyberattack on last weekend, the firm said on Thursday. "QEC's network was breached, and the corporation took immediate actions to contain the situation."

https://www.itworldcanada.com/article/nunavut-power-utilitys-servers-hit-by-cyber-attack/522899

Click above link to read more.

Back to top

Cambrian College amps up cybersecurity program as industry hits 'turning point'

As cyberattacks appear to be more common, a new program at Cambrian College in Sudbury is equipping students with tools to fight them.

The Cybersecurity Graduate Certificate (CSEC) Program is getting ready to graduate its third intake of students, co-ordinator Myles Peterson told CBC News.

And it comes at a good time, as several high-profile attacks have raised the awareness, and concern, around cybersecurity.

https://www.cbc.ca/news/canada/sudbury/cyber-security-cambrian-college-1.6721325

Click above link to read more.

Back to top

Canada: Cybersecurity chief warns about data-harvesting apps

Story text. Canada's top cybersecurity chief has warned Canadians to exercise caution when using apps that could leave their data in the "wrong hands." The warning comes amid Chinese-owned social media app TikTok facing data-harvesting claims from across the world.

Prime Minister Justin Trudeau had stated last month that Canadian electronic spy agency is keeping an eye out for security threats from Tik Tok. In neighbouring US, Republican Senators has moved to ban TikTok earlier this month. Tik To, which has reportedly over a billion users worldwide is widely popular in both US and Canada. "You have to ask yourself the question, do they need to access that information? Why does an application need to access all of my contact list? Why does it need to access my calendar, my email, my phone records, my [texts]?" Sami Khoury, head of the Communications Security Establishment (CSE) Canadian Centre for Cyber Security told CBC News.

https://hwnews.in/news/international/canada-cybersecurity-chief-warns-about-data-harvesting-apps/

Click above link to read more.

Back to top

Mailchimp hit again by social media attack

Accounts of 133 corporate customers of email marketing service provider Mailchimp have been hacked after employees fell for a social media attack, the third time the company has been compromised in less than a year.

"On January 11, the Mailchimp Security team identified an unauthorized actor accessing one of our tools used by Mailchimp customer-facing teams for customer support and account administration," the company said in a statement. "The unauthorized actor conducted a social engineering attack on Mailchimp employees and contractors, and obtained access to select Mailchimp accounts using employee credentials compromised in that attack."

https://www.itworldcanada.com/article/mailchimp-hit-again-by-social-media-attack/522825

Click above link to read more.

Back to top

KFC, Pizza Hut parent shuts UK restaurants after cyber attack

Yum! Brands, the organisation behind iconic restaurant and fast food franchises including KFC, Pizza Hut and Taco Bell, was forced to close approximately 300 outlets across the UK on Wednesday 18 January following a ransomware attack by an as-yet unspecified group.

The US-based restaurant operator said that on detecting the incident, it implemented planned response protocols, deployed containment measures to prevent the malware spreading – including taking certain systems offline – and implemented enhanced monitoring for further activity.

https://www.computerweekly.com/news/252529373/KFC-Pizza-Hut-parent-shuts-UK-restaurants-after-cyber-attack

Click above link to read more.

Back to top

Cyber-crime gangs' earnings slide as victims refuse to pay

Cryptocurrency experts at Chainalysis say ransomware groups extorted at least $457m (£370m) from victims in 2022 - $311m less than the year before.

The true figures are likely to be higher, but experts agree that fewer victims are paying.

However, while there has been a drop in criminal revenue, the number of attacks is rising.

https://www.bbc.com/news/technology-64323980

Click above link to read more.

Back to top

PayPal data breach – thousands of users' accounts compromised

The unauthorized parties used login credentials to access PayPal user accounts, according to a PayPal notification of a security incident.

Between December 6 and December 8, 2022, hackers gained unauthorized access to the accounts of thousands of individuals. A total of 34,942 accounts were reportedly accessed by threat actors employing a 'credential stuffing attack'.

https://cybersecuritynews.com/paypal-data-breach/

Click above link to read more.

Back to top

Roaming Mantis spreading mobile malware that hijacks Wi-Fi routers' DNS settings

Threat actors associated with the Roaming Mantis attack campaign have been observed delivering an updated variant of their patent mobile malware known as Wroba to infiltrate Wi-Fi routers and undertake Domain Name System (DNS) hijacking.

Kaspersky, which carried out an analysis of the malicious artifact, said the feature is designed to target specific Wi-Fi routers located in South Korea.

https://thehackernews.com/2023/01/roaming-mantis-spreading-mobile-malware.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