Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

March 12, 2024

Challenge yourself with our RFID Skimming Quiz!

Cybersecurity theme of the week: **Ransomware**
✪ Check out our Ransomware Infosheet to learn more.

Wonder what you can do to protect yourself from ransomware?

All Users	Technical Users	Business Owners
Regularly back up your files and data to ensure they are up to date.	Use the 3-2-1 rule: Make 3 backups of your data, on 2 different types of media, with at least 1 backup offsite for disaster recovery.	Periodically create system backups in case a malware attack succeeds.

🍁 **Second Ontario municipality reports cybersecurity incident within three weeks**

🍁 **Alberta government hunting down cyber threats with new website**

🍁 **Pilot cybersecurity training program for women to recruit third cohort**

🍁 **Cyber attacks are getting easier, experts warn after 3rd federal incident**

🍁 **Burnaby students best in Canada in CyberPatriot cybersecurity contest**

Google opens new cybersecurity hub in Japan

✪ **Exit scam: BlackCat ransomware group vanishes after $22 million payout**

Microsoft says Russian state-sponsored hackers trying to breach its systems again

Switzerland: Play ransomware leaked 65,000 government documents

WordPress builder plugin flaw exposes 3,300+ websites to XSS attack

Belfast cyber security firm secures first of new generation of urban self-drive vehicles in England

New network code on cybersecurity for EU electricity sector

[Are private conversations truly private? A cybersecurity expert explains how end-to-end encryption protects you]

[Watch out: These PyPI Python packages can drain your crypto wallets]

Second Ontario municipality reports cybersecurity incident within three weeks

The Town of Huntsville says its municipal office will remain closed for a second day today and some council meetings are being rescheduled as specialists investigate a cybersecurity incident.

Click above link to read more.

Back to top

Alberta government hunting down cyber threats with new website

Officials with the provincial government have announced a new website that connects Alberta cybersecurity leaders and supports organizations as they respond to threats.

https://rdnewsnow.com/2024/03/07/alberta-government-hunting-down-cyber-threats-with-new-website/

Click above link to read more.

Back to top

Pilot cybersecurity training program for women to recruit third cohort

A pilot program aimed at training women and non-binary persons for careers in cybersecurity will soon start recruiting its third group of students.

https://www.itworldcanada.com/article/pilot-cybersecurity-training-program-for-women-to-recruit-third-cohort/560116

Click above link to read more.

Back to top

Cyber attacks are getting easier, experts warn after 3rd federal incident

High-profile cyber incidents involving Canada’s financial intelligence unit FINTRAC, the RCMP and Global Affairs Canada since the start of the year are not isolated cases, experts warn.

https://globalnews.ca/news/10336867/canadian-cyber-attacks-rise/

Click above link to read more.

Back to top

Burnaby students best in Canada in CyberPatriot cybersecurity contest

Cybersecurity students from Burnaby were tops in Canada in a contest that bills itself as the world's largest cyber defense competition.

https://www.burnabynow.com/local-news/burnaby-students-best-in-canada-in-cyberpatriot-cybersecurity-contest-8407643#google_vignette

Click above link to read more.

Back to top

Google opens new cybersecurity hub in Japan

The region faces a growing cyber threat from a range of actors, including criminal gangs looking for big payouts and state-backed actors pursuing intelligence or sabotage, according to governments and security firms.

https://www.france24.com/en/live-news/20240307-google-opens-new-cybersecurity-hub-in-japan

Click above link to read more.

Back to top

Exit scam: BlackCat ransomware group vanishes after $22 million payout

The threat actors behind the BlackCat ransomware have shut down their darknet website and likely pulled an exit scam after uploading a bogus law enforcement seizure banner.

https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html

Click above link to read more.

Back to top

Microsoft says Russian state-sponsored hackers trying to breach its systems again

Microsoft (MSFT.O), opens new tab said on Friday that a Russian state-sponsored hacking group named Midnight Blizzard was trying to breach its systems again, by using information it stole from the tech giant's corporate emails in January.

https://www.reuters.com/technology/cybersecurity/microsoft-says-cyber-threat-actor-has-been-able-access-internal-systems-2024-03-08/

Click above link to read more.

Back to top

Switzerland: Play ransomware leaked 65,000 government documents

The National Cyber Security Centre (NCSC) of Switzerland has released a report on its analysis of a data breach following a ransomware attack on Xplain, disclosing that the incident impacted thousands of sensitive Federal government files.

https://www.bleepingcomputer.com/news/security/switzerland-play-ransomware-leaked-65-000-government-documents/

Click above link to read more.

Back to top

WordPress builder plugin flaw exposes 3,300+ websites to XSS attack

A recent surge in attacks from a new malware campaign exploits a known vulnerability in the WordPress plugin Popup Builder, infecting over 3,300 websites with XSS attacks.

https://gbhackers.com/wordpress-builder-plugin-flaw/

Click above link to read more.

Back to top

Belfast cyber security firm secures first of new generation of urban self-drive vehicles in England

Belfast cyber security specialist Angoka has provided active protection for the operation of the Sunderland Advanced Mobility Shuttle (SAMS), marking a significant milestone in the city's journey towards self-driving transportation.

https://www.newsletter.co.uk/business/belfast-cyber-security-firm-secures-first-of-new-generation-of-urban-self-drive-vehicles-in-england-4550789

Click above link to read more.

Back to top

New network code on cybersecurity for EU electricity sector

The European Commission has today adopted the first-ever EU network code on cybersecurity for the electricity sector. Foreseen under the Electricity Regulation (EU) 2019/943 (Article 59) and in the 2022 EU Action Plan to digitalise the energy system, this delegated act is an important step to improve the cyber resilience of critical EU energy infrastructure and services. It will support a high, common level of cybersecurity for cross-border electricity flows in Europe. The dossier now passes to the Council and European Parliament to scrutinise the text and the rules will enter into force once this period is over.

https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en?prefLang=es

Click above link to read more.

Back to top

Are private conversations truly private? A cybersecurity expert explains how end-to-end encryption protects you

Imagine opening your front door wide and inviting the world to listen in on your most private conversations. Unthinkable, right? Yet, in the digital realm, people inadvertently leave doors ajar, potentially allowing hackers, tech companies, service providers and security agencies to peek into their private communications.

https://theconversation.com/are-private-conversations-truly-private-a-cybersecurity-expert-explains-how-end-to-end-encryption-protects-you-224477

Click above link to read more.

Back to top

Watch out: These PyPI Python packages can drain your crypto wallets

Threat hunters have discovered a set of seven packages on the Python Package Index (PyPI) repository that are designed to steal BIP39 mnemonic phrases used for recovering private keys of a cryptocurrency wallet.

https://thehackernews.com/2024/03/watch-out-these-pypi-python-packages.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

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