Security News Digest

Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

June 11, 2024

Theme of the month: SIM Swapping
(look for the ✪)

Challenge yourself with our **SIM Swapping Quiz**!

What you can do to improve your mobile device security:

All Users	Technical Users	Business Owners
Avoid using public wi-fi to connect to the internet, as it can leave you vulnerable to attacks. Only connect to trusted networks that are password-protected or use mobile data.	Ensure that any attempts to tamper with mobile device operating systems are blocked, logged, and actioned immediately.	Ensure that employees are aware of and understand the policies associated with using their work devices for personal use.

Check out this Cyber Safety for Mobile Workers info sheet to learn more about mobile device security.

This past week's stories:

🍁 Lighthouse Labs announces launch of ICT Ignite Cyber program to enhance employability of cybersecurity learners

🍁 Cybersecurity standards emerging in Canada as ransomware business booms

'Russian criminals' behind hospitals cyber attack

Celebrity TikTok accounts compromised using zero-click attack via DMs

The AI debate: Google's guidelines, Meta's GDPR dispute, Microsoft's recall backlash

Ransomware actor exploited CoinMiner attacker's proxy server

Wineloader mimic as ambassador of India to start the infection chain

Microsoft to disable NTLM, transition to Kerberos authentication

Microsoft to help rural hospitals defend against rising cybersecurity attacks

EmailGPT vulnerability let attackers access sensitive data

✪ SIM card swapping: The dangerous cell phone scam everyone needs to know about

✪ Hackers target OKX customers in suspected SIM swap attack

Lighthouse Labs announces launch of ICT Ignite Cyber program to enhance employability of cybersecurity learners

Today, Lighthouse Labs is excited to announce that its Cyber Security Bootcamp funded by Upskill Canada (powered by Palette Skills) and the Government of Canada now offers paid internships supported by Riipen, the leading experiential learning platform.

https://www.businesswire.com/news/home/20240604809243/en/Lighthouse-Labs-Announces-Launch-of-ICT-Ignite-Cyber-Program-to-Enhance-Employability-of-Cybersecurity-Learners

Click above link to read more.

Back to top

Cybersecurity standards emerging in Canada as ransomware business booms

The ransomware business is booming in Canada.

https://www.ctvnews.ca/sci-tech/cybersecurity-standards-emerging-in-canada-as-ransomware-business-booms-1.6914093

Click above link to read more.

Back to top

'Russian criminals' behind hospitals cyber attack

Russian hackers are behind the cyber attack on a number of major London hospitals, according to the former chief executive of the National Cyber Security Centre.

https://www.bbc.com/news/articles/cxee7317kgmo

Click above link to read more.

Back to top

Celebrity TikTok accounts compromised using zero-click attack via DMs

Popular video-sharing platform TikTok has acknowledged a security issue that has been exploited by threat actors to take control of high-profile accounts on the platform.

https://thehackernews.com/2024/06/celebrity-tiktok-accounts-compromised.html

Click above link to read more.

Back to top

The AI debate: Google's guidelines, Meta's GDPR dispute, Microsoft's recall backlash

Google is urging third-party Android app developers to incorporate generative artificial intelligence (GenAI) features in a responsible manner.

https://thehackernews.com/2024/06/the-ai-debate-googles-guidelines-metas.html

Click above link to read more.

Back to top

Ransomware actor exploited CoinMiner attacker’s proxy server

Hackers can hide their names and access blocked websites or networks by using proxy servers, which help make these systems anonymous.

https://cybersecuritynews.com/ransomware-exploits-coinminer-proxy/

Click above link to read more.

Back to top

Wineloader mimic as ambassador of India to start the infection chain

ARC Labs delved into the intricacies of the Wineloader backdoor, a sophisticated tool used in spearphishing campaigns linked to the notorious APT29 group, also known as NOBELIUM or COZY BEAR.

https://cybersecuritynews.com/wineloader-mimic-as-ambassador/

Click above link to read more.

Back to top

Microsoft to disable NTLM, transition to Kerberos authentication

Microsoft has made an announcement regarding the gradual phasing out of all versions of NTLM (NT LAN Manager).

https://cybersecuritynews.com/microsoft-to-disable-ntlm/

Click above link to read more.

Back to top

Microsoft to help rural hospitals defend against rising cybersecurity attacks

On Monday, Microsoft Corp. announced a new cybersecurity program to support hospitals serving more than 60 million people living in rural America.

https://www.prnewswire.com/news-releases/microsoft-to-help-rural-hospitals-defend-against-rising-cybersecurity-attacks-302168139.html

Click above link to read more.

Back to top

EmailGPT vulnerability let attackers access sensitive data

A new prompt injection vulnerability has been discovered in the EmailGPT service. This API service and Google Chrome plugin help users write emails in Gmail using OpenAI’s GPT model.

https://cybersecuritynews.com/emailgpt-vulnerability/

Click above link to read more.

Back to top

SIM card swapping: The dangerous cell phone scam everyone needs to know about

According to the Pew Research Center, almost all American adults (97%) own a cell phone. While that statistic isn't surprising, it does show how many of us are susceptible to a dangerous scam: SIM swapping.

https://clark.com/cell-phones/sim-card-swapping/

Click above link to read more.

Back to top

Hackers target OKX customers in suspected SIM swap attack

Hackers have allegedly targeted OKX, stealing funds from at least two accounts in a sophisticated attack involving SMS risk notifications and the creation of new API keys.

https://crypto.news/hackers-target-okx-customers-in-suspected-sim-swap-attack/

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