Security News Digest
Cybersecurity and Digital Trust Branch

OCIO Office of the Chief Information Officer

June 25, 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
If your mobile device for work is lost or stolen, report it immediately to your organization's security team and request that a remote lock or wipe be conducted.	Ensure that mobile devices capable of connecting to your network are enrolled into an approved Mobile Device Management (MDM) system before they are used to store confidential information.	Ensure your organization has a proper asset disposal process to ensure information stored on mobile devices doesn't fall into the wrong hands when the device is retired.

Check out our Protecting Mobile Devices quiz to learn more about mobile device security.

This past week's stories:

🍁 **AI safety, cybersecurity experts take on key roles at Schwartz Reisman Institute for Technology and Society**
🍁 **Hamilton spent $5.7 million recovering from February ransomware attack: report**
French diplomatic entities targeted in Russian-linked cyber attacks
CDK cyberattack shuts down auto dealerships across the U.S. Here's what to know
Cybersecurity exec sentenced in medical center hacking

✪ **Android flaw lets hackers break in with a text message**

U.S. to ban Kaspersky cybersecurity products over security concerns
Military-themed email scam spreads malware to infect Pakistani users
Australian regulator blames lack of multi-factor authentication for Medibank hack
UN chief warns of rising cybersecurity incidents and malicious use of digital technology
Demand for better cybersecurity fuels a booming job market
Poland spending $760 million on cybersecurity after attack

AI safety, cybersecurity experts take on key roles at Schwartz Reisman Institute for Technology and Society

A leading expert in cybersecurity and two renowned AI safety researchers are set to take on leading roles at the University of Toronto's Schwartz Reisman Institute for Technology and Society.

https://educationnewscanada.com/article/education/level/university/1/1089252/ai-safety-cybersecurity-experts-take-on-key-roles-at-schwartz-reisman-institute-for-technology-and-society.html

Click above link to read more.

Back to top

Hamilton spent $5.7 million recovering from February ransomware attack: report

The City of Hamilton has spent $5.7 million dealing with the ongoing impacts of a ransomware attack in February.

https://www.cbc.ca/news/canada/hamilton/ransomware-recovery-update-1.7238622

Click above link to read more.

Back to top

French diplomatic entities targeted in Russian-linked cyber attacks

State-sponsored actors with ties to Russia have been linked to targeted cyber attacks aimed at French diplomatic entities, the country's information security agency ANSSI said in an advisory.

https://thehackernews.com/2024/06/french-diplomatic-entities-targeted-in.html

Click above link to read more.

Back to top

CDK cyberattack shuts down auto dealerships across the U.S. Here's what to know

CDK Global, a company that provides auto dealerships across the U.S. with software for managing sales and other services, has been hacked, prompting the company to temporarily shut down most of its systems.

https://www.cbsnews.com/news/cdk-cyber-attack-outage-auto-dealerships-cbs-news-explains/

Click above link to read more.

Back to top

Cybersecurity exec sentenced in medical center hacking

An Atlanta cybersecurity executive who hacked the Gwinnett Medical Center’s computer system in an alleged attempt to boost business for his cash-strapped company has been sentenced to two years of home detention after paying more than $800,000 in restitution.

https://www.govtech.com/security/cybersecurity-exec-sentence-in-medical-center-hacking

Click above link to read more.

Back to top

Android flaw lets hackers break in with a text message

Cyber security firm Zimperium on Monday warned of a flaw in the world’s most popular smartphone operating system that lets hackers take control with a text message.

https://guardian.ng/android-flaw-lets-hackers-break-in-with-a-text-message/

Click above link to read more.

Back to top

U.S. to ban Kaspersky cybersecurity products over security concerns

The Biden administration will ban cybersecurity company Kaspersky Lab from selling products in the United States over concerns the firm is closely tied to Russia and poses a security risk.

https://globalnews.ca/news/10580200/kaspersky-cyber-product-us-ban/

Click above link to read more.

Back to top

Military-themed email scam spreads malware to infect Pakistani users

Cybersecurity researchers have shed light on a new phishing campaign that has been identified as targeting people in Pakistan using a custom backdoor.

https://thehackernews.com/2024/06/military-themed-emails-used-to-spread.html

Click above link to read more.

Back to top

Australian regulator blames lack of multi-factor authentication for Medibank hack

Australia's data protection regulator reveals in court documents that the 2022 attack on health insurance provider Medibank was likely caused by a lack of multi-factor authentication, allowing hackers to access the company's IT systems.

https://therecord.media/medibank-hack-australian-government-report-mfa

Click above link to read more.

Back to top

UN chief warns of rising cybersecurity incidents and malicious use of digital technology

UN Secretary General António Guterres warned that cyber threats have become “disturbingly common”.

https://www.euronews.com/next/2024/06/21/un-chief-warns-of-rising-cybersecurity-incidents-and-malicious-use-of-digital-technology

Click above link to read more.

Back to top

Demand for better cybersecurity fuels a booming job market

When Nana Pokuaah isn’t working at a pharmacy, she’s in school — though it might not look like it.

https://www.washingtonpost.com/business/2024/06/21/cybersecurity-job-demand-boot-camps/

Click above link to read more.

Back to top

Poland spending $760 million on cybersecurity after attack

Visitors to the Polish Press Agency (PAP) website on May 31 at 2 p.m. Polish time were met with an unusual message. Instead of the typical daily news, the state-run newspaper had supposedly published a story announcing that a partial mobilization, which means calling up specific people to serve in the armed forces, was ordered by Polish Prime Minister Donald Tusk beginning on July 1, 2024.

https://securityintelligence.com/news/poland-cybersecurity-spending-increases/

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
Cybersecurity and Digital Trust Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer