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

March 5, 2024

Challenge yourself with our RFID Skimming Quiz!

Cybersecurity theme of the week: **Social Media Security**
✪ Check out our **Top 8 Things Not to Give Social Networking Sites** to learn more.

Wonder what you can do to protect yourself while using social media?

All Users	Technical Users	Business Owners
Use multi-factor authentication (MFA) to access each of your social media accounts.	Keep security software current: Having the latest security software, web browser, and operating system are the best defences against viruses, malware, and other online threats.	Ensure your applications support and are protected by MFA, ask question of your technical teams when you hear news of outages in other applications and have a plan to respond to an outage in your environment.

This past week's stories:

✪ **Facebook, Instagram back online after Meta sees global outage**

🍁 **FINTRAC faces cyber incident**

🍁 **Cyber attack on Hamilton knocks out municipal phone, email**

🍁 **London library 'almost fully recovered' from ransomware attack, CEO says**

These video doorbells have terrible security. Amazon sells them anyway

Industry reactions to NIST Cybersecurity Framework 2.0: Feedback Friday

How to get into cybersecurity with no experience

Ransomware attack on Change Healthcare disrupts U.S. healthcare services, prompting nationwide response

How the 'get to know me' social media challenge could end in tears

North Korea broke into S. Korean chip equipment firms, Seoul's spy agency says

U.S. charges Iranian hacker, offers $10 million reward for capture

'Pig-butchering' scams have netted criminals $75 billion in stolen crypto, study says

‘Cyber-physical attacks’ fueled by AI are a growing threat, experts say

Facebook, Instagram back online after Meta sees global outage

Were you logged out of your Facebook and Instagram accounts Tuesday? You’re not alone.

https://globalnews.ca/news/10336162/facebook-instagram-meta-outage/

Click above link to read more.

Back to top

FINTRAC faces cyber incident

Canada’s federal anti-money laundering agency, FINTRAC, is grappling with a cybersecurity incident.

https://www.investmentexecutive.com/news/from-the-regulators/fintrac-faces-cyber-incident/

Click above link to read more.

Back to top

Cyber attack on Hamilton knocks out municipal phone, email

Hamilton, a municipality of about 570,000 on the shore of Lake Ontario, said Sunday it had suffered a city-wide phone and email “disruption” to municipal and public library services, which included the Bus Check Info Line and the HSRNow transit planning app.

https://www.itworldcanada.com/article/cyber-attack-on-hamilton-knocks-out-municipal-phone-email/559452

Click above link to read more.

Back to top

London library 'almost fully recovered' from ransomware attack, CEO says

More than two months after a ransomware attack left its website, catalogue, and internal network offline for several weeks, officials with the London Public Library say they've managed to get things largely back to normal.

https://www.cbc.ca/news/canada/london/london-library-ransomware-almost-recovered-1.7131984

Click above link to read more.

Back to top

These video doorbells have terrible security. Amazon sells them anyway.

On a recent Thursday afternoon, a Consumer Reports journalist received an email containing a grainy image of herself waving at a doorbell camera she'd set up at her back door.

https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/

Click above link to read more.

Back to top

Industry reactions to NIST Cybersecurity Framework 2.0: Feedback Friday

The cybersecurity framework was originally created for critical infrastructure organizations, but CSF 2.0 is designed to help all organizations reduce risks, regardless of sector, size, or level of security sophistication.

https://www.securityweek.com/industry-reactions-to-nist-cybersecurity-framework-2-0-feedback-friday/

Click above link to read more.

Back to top

How to get into cybersecurity with no experience

Can you break into the world of cybersecurity without experience? It's a question that's been searched countless times according to Google Trends—even peaking in recent years.

https://fortune.com/education/articles/how-to-get-into-cybersecurity-with-no-experience/

Click above link to read more.

Back to top

New Silver SAML attack evades Golden SAML defenses in identity systems

Cybersecurity researchers have disclosed a new attack technique called Silver SAML that can be successful even in cases where mitigations have been applied against Golden SAML attacks.

https://thehackernews.com/2024/02/new-silver-saml-attack-evades-golden.html

Click above link to read more.

Back to top

Ransomware attack on Change Healthcare disrupts U.S. healthcare services, prompting nationwide response

In the early hours of February 21, an unsettling silence enveloped the operations of Change Healthcare, a cornerstone in the U.S. healthcare infrastructure, as it fell victim to a sophisticated ransomware attack by the notorious ALPHV/BlackCat gang. This cyber onslaught not only challenged the resilience of one of the nation's largest healthcare technology companies but also cast a long shadow over hospitals, pharmacies, and clinics across the country, disrupting essential services and putting patient care at risk

https://medriva.com/health/ransomware-attack-on-change-healthcare-disrupts-us-healthcare-services-prompting-nationwide-response

Click above link to read more.

Back to top

How the ‘get to know me’ social media challenge could end in tears

Cybersecurity experts warn that some responses are typical answers to identity verification questions.

Social media challenges are all fun and games until you get hacked or scammed in your relentless pursuit for ‘likes’.

https://enews.com.ng/2024/03/how-the-get-to-know-me-social-media-challenge-could-end-in-tears/

Click above link to read more.

Back to top

North Korea broke into S. Korean chip equipment firms, Seoul's spy agency says

North Korea's hacking groups have broken into at least two South Korean manufacturers of chipmaking equipment, as the country looks to evade sanctions and turn out its own semiconductors for weapons programmes, South Korea's spy agency said on Monday.

https://www.reuters.com/world/asia-pacific/north-korea-broke-into-s-korean-chip-equipment-firms-seouls-spy-agency-says-2024-03-04/

Click above link to read more.

Back to top

U.S. charges Iranian hacker, offers $10 million reward for capture

The U.S. Department of Justice (DoJ) on Friday unsealed an indictment against an Iranian national for his alleged involvement in a multi-year cyber-enabled campaign designed to compromise U.S. governmental and private entities.

https://thehackernews.com/2024/03/us-charges-iranian-hacker-offers-10.html

Click above link to read more.

Back to top

'Pig-butchering' scams have netted criminals $75 billion in stolen crypto, study says

A recent study says a particular kind of fraud — named after the method used by farmers of fattening pigs up before they're slaughtered — has allowed criminals to get away with billions in crypto, often leaving victims penniless.

https://markets.businessinsider.com/news/currencies/crypto-crime-pig-butchering-scam-bitcoing-trafficking-fraud-cryptocurrency-2024-2

Click above link to read more.

Back to top

‘Cyber-physical attacks’ fueled by AI are a growing threat, experts say

When most people hear about cybersecurity hacks they envision frozen monitors, ransomware demands, and DDoS attacks that compromise connectivity for a few hours or even days.

https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.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