Security News Digest

Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

April 30, 2024

Theme of the month: Cloud Authentication
(look for the ✪)

Challenge yourself with our Cloud Authentication Quiz!

What you can do to improve your authentication processes

All Users	Technical Users	Business Owners
Ensure that you are taking advantage of multi-factor authentication (MFA) with your accounts and services whenever it is available. Including social-media, banking, subscriptions services and any apps you may use.	Implement MFA with complimentary authentication tools like Single Sign-On and Token-based authentication to keep a high level of security but removing the need to use multiple passwords for a better user experience.	Security vulnerabilities and threats landscapes are always changing. Have security teams regularly evaluate and report on the types of authentication tools you're using to ensure they are still effective and being used properly.

Check out our **Intro to MFA page** to learn more.

This past week's stories:

🍁 More than $55M has been lost to investment scams in Toronto over the last 9 months. Is 'pig butchering' making it worse?

🍁 London Drugs closes stores until further notice due to cyberattack

Major security flaws expose keystrokes of over 1 billion Chinese keyboard app users

✪Hackers offering admin access to 3000 Fortinet SSL-VPN

Ireland taking part in international cybersecurity exercise

New Qiulong ransomware well-equipped to make waves

ArcaneDoor exploiting Cisco zero-days to attack government networks

New 'Brokewell' Android malware spread through fake browser updates

These are the places where Chinese-owned TikTok is already banned

Cisco says hackers subverted its security devices to spy on governments

AI increases cybersecurity threats amidst IT budget cuts, study warns

Google rejected 2.28 million risky Android apps from Play store in 2023

✪Authentication failure blamed for Change Healthcare ransomware attack

UK becomes first country to ban default bad passwords on IoT devices

More than $55M has been lost to investment scams in Toronto over the last 9 months. Is 'pig butchering' making it worse?

It starts small – an initial investment of just a few hundred dollars.

“Then, the victim will see a small return,” says David Coffey, a detective with the Toronto Police Services’ Financial Crimes Unit(opens in a new tab). “That's how it snowballs, and that’s how people get hooked.”

https://toronto.ctvnews.ca/mobile/more-than-55m-has-been-lost-to-investment-scams-in-toronto-over-the-last-9-months-is-pig-butchering-making-it-worse-1.6818277?cache=ahlalmzxbysj?clipId=89619

Click above link to read more.

Back to top

London Drugs closes stores until further notice due to cyberattack

Retail and pharmacy chain London Drugs says it was the "victim of a cybersecurity incident" Sunday and has shuttered its stores across Western Canada until further notice.

https://www.cbc.ca/news/canada/british-columbia/london-drugs-closure-western-canada-1.7187615

Click above link to read more.

Back to top

Major security flaws expose keystrokes of over 1 billion Chinese keyboard app users

Security vulnerabilities uncovered in cloud-based pinyin keyboard apps could be exploited to reveal users' keystrokes to nefarious actors.

https://thehackernews.com/2024/04/major-security-flaws-expose-keystrokes.html

Click above link to read more.

Back to top

Hackers offering admin access to 3000 Fortinet SSL-VPN

Hackers are now offering administrative access to over 3000 Fortinet SSL-VPN devices.

https://cybersecuritynews.com/hackers-offering-admin-access/

Click above link to read more.

Back to top

Ireland taking part in international cybersecurity exercise

Ireland is taking part in a major international cyber defence training exercise this week.

https://www.rte.ie/news/ireland/2024/0425/1445627-cyber-security/

Click above link to read more.

Back to top

New Qiulong ransomware well-equipped to make waves

The Qiulong ransomware gang, a new cyber threat actor, has emerged targeting Brazilian victims as the group announced their arrival by compromising Dr. Lincoln Graca Neto and Rosalvo Automoveis, two entities located in Brazil.

https://cybersecuritynews.com/new-qiulong-ransomware-emerges/

Click above link to read more.

Back to top

ArcaneDoor exploiting Cisco zero-days to attack government networks

Hackers target Cisco zero-days as they can abuse the widely used networking equipment that contains vulnerabilities which means they can affect many systems and networks in one shot.

https://cybersecuritynews.com/arcanedoor-exploiting-cisco-zero-days/

Click above link to read more.

Back to top

New 'Brokewell' Android malware spread through fake browser updates

Fake browser updates are being used to push a previously undocumented Android malware called Brokewell.

https://thehackernews.com/2024/04/new-brokewell-android-malware-spread.html

Click above link to read more.

Back to top

These are the places where Chinese-owned TikTok is already banned

TikTok is in the cross hairs of authorities in the US, where new legislation threatens a nationwide ban unless its China-based parent ByteDance divests. It would be the biggest blow yet to the popular video-sharing app, which has faced various restrictions around the world.

https://www.scmp.com/news/world/united-states-canada/article/3260539/these-are-places-where-chinese-owned-tiktok-already-banned?module=Europe&pgtype=section

Click above link to read more.

Back to top

Cisco says hackers subverted its security devices to spy on governments

Technology firm Cisco Systems (CSCO.O), opens new tab said that hackers have subverted some of its digital security devices to break in to government networks globally.

https://www.reuters.com/technology/cybersecurity/cisco-says-hackers-subverted-its-security-devices-spy-governments-2024-04-24/

Click above link to read more.

Back to top

AI increases cybersecurity threats amidst IT budget cuts, study warns

A new study warns that cybersecurity measures must be prioritized amidst an increasingly sophisticated threat of artificial intelligence (AI).

https://www.bnnbloomberg.ca/ai-increases-cybersecurity-threats-amidst-it-budget-cuts-study-warns-1.2066664

Click above link to read more.

Back to top

Google rejected 2.28 million risky Android apps from Play store in 2023

Google blocked 2.28 million Android apps from being published on Google Play after finding various policy violations that could threaten user's security.

https://www.bleepingcomputer.com/news/security/google-rejected-228-million-risky-android-apps-from-play-store-in-2023/
Click above link to read more.

Back to top

Authentication failure blamed for Change Healthcare ransomware attack

Absence of adequate remote access authentication has emerged as the probable cause of the infamous Change Healthcare ransomware attack.

https://www.csoonline.com/article/2094609/authentication-failure-blamed-for-change-healthcare-ransomware-attack.html

Click above link to read more.

Back to top

UK becomes first country to ban default bad passwords on IoT devices

Seven years ago, a cyberattack left many of the most popular websites based in the United States inaccessible. For three extended periods on October 21, 2016, internet users were left without their doses of Twitter, CNN and Netflix among other popular sites.

https://therecord.media/united-kingdom-bans-defalt-passwords-iot-devices

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