

May 7, 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
Use strong passwords that include at least 14 characters, combining uppercase and lowercase letters, numbers, and special characters. The password should not be a dictionary recognizable word, but something unique to you that you can remember. And use a different password each of your accounts.	Implement effective virtual private network (VPN) tunnels to encrypt sensitive data at rest and in transit. Select a VPN Vendor that has a good reputation. Regularly check for software updates and vulnerability patches for your VPN software.	Understand the cyber-risks your business has. Ensure that these risks fall within your risk tolerance and take appropriate measures to mitigate the ones that fall outside of it. Consider reputational impact, financial loss, operational impact, and personal impact when determining your risk tolerance.

Check out our [Passwords Best Practices page](#) to learn more.

[This past week's stories:](#)

🍁 [U.K. bans generic passwords over cybersecurity concerns. Should Canada be next?](#)

🍁 [Hacker demands ransom from B.C. libraries after data breach](#)

🍁 [All provincial employees in B.C. directed to change passwords](#)

☼ [Cuttlefish malware targets routers, harvests cloud authentication data](#)

[Dropbox says hacker accessed passwords, authentication info during breach](#)

[LockBit publishes confidential data stolen from Cannes hospital in France](#)

[Bitcoin forensic analysis uncovers money laundering clusters and criminal proceeds](#)

[Internal communication gaps exposes organizations to cyber attacks](#)

[Amnesty International cites Indonesia as a spyware hub](#)

[Paris Olympics cybersecurity at risk via attack surface gaps](#)

[From teenage cyber-thug to Europe's most wanted](#)

[China-linked hackers suspected in ArcaneDoor cyberattacks targeting network devices](#)

U.K. bans generic passwords over cybersecurity concerns. Should Canada be next?

Story text. The United Kingdom has introduced a new law that bans generic passwords on smart devices in order to protect consumers from cyber attacks.

<https://globalnews.ca/news/10468217/easy-passwords-banned-uk-cybersecurity/>

Click above link to read more.

[Back to top](#)

Hacker demands ransom from B.C. libraries after data breach

Libraries in British Columbia have been targeted by a hacker who threatened to release user data if a ransom was not paid.

<https://www.cbc.ca/news/canada/british-columbia/libraries-cariboo-hacker-data-breach-1.7193435>

Click above link to read more.

[Back to top](#)

All provincial employees in B.C. directed to change passwords

Every provincial employee is receiving emails or memos directing them to change their passwords immediately, CTV News has learned.

<https://bc.ctvnews.ca/all-provincial-employees-in-b-c-directed-to-change-passwords-1.6869968>

Click above link to read more.

[Back to top](#)

Cuttlefish malware targets routers, harvests cloud authentication data

Malware hunters at Lumen's Black Lotus Labs have set eyes on a new malware platform roaming around enterprise-grade and small office/home office (SOHO) routers capable of covertly harvesting public cloud authentication data from internet traffic.

<https://www.securityweek.com/cuttlefish-malware-targets-routers-harvests-cloud-authentication-data/>

Click above link to read more.

[Back to top](#)

Dropbox says hacker accessed passwords, authentication info during breach

Cloud storage company Dropbox reported that a hacker breached company systems on April 24 and gained access to sensitive information like passwords and more.

<https://therecord.media/dropbox-data-breach-notification>

Click above link to read more.

[Back to top](#)

LockBit publishes confidential data stolen from Cannes hospital in France

The LockBit ransomware-as-a-service gang has published what it claims is confidential data stolen from a hospital in Cannes, France.

<https://therecord.media/lockbit-ransomware-hopital-de-cannes-data-published>

Click above link to read more.

[Back to top](#)

Bitcoin forensic analysis uncovers money laundering clusters and criminal proceeds

A forensic analysis of a graph dataset containing transactions on the Bitcoin blockchain has revealed clusters associated with illicit activity and money laundering, including detecting criminal proceeds sent to a crypto exchange and previously unknown wallets belonging to a Russian darknet market.

<https://thehackernews.com/2024/05/bitcoin-forensic-analysis-uncovers.html>

Click above link to read more.

[Back to top](#)

Internal communication gaps exposes organizations to cyber attacks

The alignment between security teams and executive management is crucial.

<https://cybersecuritynews.com/internal-communication-cyber-attacks/>

Click above link to read more.

[Back to top](#)

Amnesty International cites Indonesia as a spyware hub

New research from Amnesty International's Security Lab identifies Indonesia as an emerging hub for surveillance tools and suppliers. The organization found evidence of sales and shipment of "highly invasive spyware and other surveillance technologies" sent to Indonesia from countries like Israel, Greece, Singapore, and Malaysia dating back to 2017 up until last year.

<https://www.darkreading.com/cybersecurity-operations/amnesty-international-cites-indonesia-as-spyware-hub>

Click above link to read more.

[Back to top](#)

Paris Olympics cybersecurity at risk via attack surface gaps

Web applications and other Internet-facing assets related to the 2024 Summer Olympics in Paris appear to be better protected against cyberattacks than previous major sporting events, such as the 2022 FIFA World Cup in Qatar.

<https://www.darkreading.com/vulnerabilities-threats/paris-olympics-cybersecurity-at-risk-via-attack-surface-gaps>

Click above link to read more.

[Back to top](#)

From teenage cyber-thug to Europe's most wanted

A notorious hacker who was one of Europe's most wanted criminals has been jailed for blackmailing 33,000 therapy patients with their stolen session notes.

<https://www.bbc.com/news/articles/cyxe9g4zlgpo>

Click above link to read more.

[Back to top](#)

China-linked hackers suspected in ArcaneDoor cyberattacks targeting network devices

The recently uncovered cyber espionage campaign targeting perimeter network devices from several vendors, including Cisco, may have been the work of China-linked actors, according to new findings from attack surface management firm Censys.

<https://thehackernews.com/2024/05/china-linked-hackers-suspected-in.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.

