

October 17, 2023

Challenge yourself with our Cyber Security Awareness Month Quiz!

Take part in Cyber Security Awareness Month: www.gov.bc.ca/cybersecurityawarenessmonth

Cybersecurity Issue of the Week: **AI**

★ Register for **SECURITY DAY** to learn more.

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

🍁 **National approach to cyber security education needed as attacks will only get worse: Teacher**

🍁 **Cybersecurity training, research centre opens at University of Calgary**

🍁 **Half of Canadian SMBs say keeping on top of cybersecurity threats is their biggest challenge**

Beyond the front lines: How the Israel-Hamas war impacts the cybersecurity industry

The 10 biggest cyber security trends in 2024 everyone must be ready for now

★ **How AI can fuel financial scams online, according to industry experts**

How I got started: Attack surface management

Israeli cyber security professionals band together amid Gaza war

Google initiates the end of passwords, making passkeys the default for users

FBI, CISA warn of rising AvosLocker ransomware attacks against critical infrastructure

Don't call it quishing: QR code phishing on the rise

Discord still a hotbed of malware activity — Now APTs join the fun

National approach to cyber security education needed as attacks will only get worse: Teacher

Timothy King remembers getting a spam email to his work account that appeared to be from his school board's IT department asking for his login information.

<https://www.cbc.ca/news/canada/kitchener-waterloo/national-approach-cyber-security-education-needed-1.6989633>

Click above link to read more.

[Back to top](#)

Cybersecurity training, research centre opens at University of Calgary

A new centre designed to research and train to defend against cybercrimes has been opened at the University of Calgary.

<https://globalnews.ca/news/10015879/cybersecurity-training-centre-opens-in-calgary/>

Click above link to read more.

[Back to top](#)

Half of Canadian SMBs say keeping on top of cybersecurity threats is their biggest challenge

Sage, the leader in accounting, financial, HR and payroll technology for small and mid-sized businesses (SMBs), today releases a new report, Cybersecurity for SMBs: Navigating Complexity and Building Resilience.

<https://financialpost.com/globe-newswire/half-of-canadian-smbs-say-keeping-on-top-of-cybersecurity-threats-is-their-biggest-challenge>

Click above link to read more.

[Back to top](#)

Beyond the front lines: How the Israel-Hamas war impacts the cybersecurity industry

While the mainstream media is covering the tragic and heartbreaking events of the war in Israel in detail, SecurityWeek wanted to look at a specific issue — the effect of this war on Israeli cybersecurity firms. These firms are globally important to the cybersecurity ecosystem.

<https://www.securityweek.com/the-israel-hamas-war-and-its-effect-on-the-cybersecurity-industry/>

Click above link to read more.

[Back to top](#)

The 10 biggest cyber security trends in 2024 everyone must be ready for now

By the end of the coming year, the cost of cyber attacks on the global economy is predicted to top \$10.5 trillion.

<https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=148db9b15f13>

Click above link to read more.

[Back to top](#)

How AI can fuel financial scams online, according to industry experts

There is growing fraud online in which scammers manufacture other identities to dupe financial institutions or their customers out of money -- and the crimes are only expected to grow more frequent with the increasing prevalence of artificial intelligence, experts say.

<https://abcnews.go.com/Technology/ai-fuel-financial-scams-online-industry-experts/story?id=103732051>

Click above link to read more.

[Back to top](#)

How I got started: Attack surface management

As the threat landscape multiplies in sophistication and complexity, new roles in cybersecurity are presenting themselves more frequently than ever before. For example, attack surface management.

<https://securityintelligence.com/articles/how-i-got-started-attack-surface-management/>

Click above link to read more.

[Back to top](#)

Israeli cyber security professionals band together amid Gaza war

As Israeli children listened to their teacher over Zoom, the image of a gun-toting man in fatigues appeared on the screen, according to a screenshot shared with Reuters. In another case, a video showed a billboard in the central Israeli city of Holon displaying images of rockets and a burning Israeli flag.

<https://www.reuters.com/world/middle-east/israeli-cyber-security-professionals-band-together-amid-gaza-war-2023-10-12/>

Click above link to read more.

[Back to top](#)

Google initiates the end of passwords, making passkeys the default for users

Google, a well-known tech giant, has introduced a new feature called “passwordless by default”. This feature aims to simplify the login process for users by eliminating the need for traditional passwords and instead relying on passkeys for authentication purposes.

<https://cybersecuritynews.com/google-initiates-the-end-of-passwords/>

Click above link to read more.

[Back to top](#)

FBI, CISA warn of rising AvosLocker ransomware attacks against critical infrastructure

The AvosLocker ransomware gang has been linked to attacks against critical infrastructure sectors in the U.S., with some of them detected as recently as May 2023.

<https://thehackernews.com/2023/10/fbi-cisa-warn-of-rising-avoslocker.html>

Click above link to read more.

[Back to top](#)

Don't call it quishing: QR code phishing on the rise

There's a new trend emerging in cybercrime, AT&T warns – embedding malicious QR codes into phishing attempts. The attack has been dubbed “quishing,” but the term isn't getting any love among the cybersecurity community on Reddit.

<https://cybernews.com/security/quishing-qr-code-phishing-on-the-rise/>

Click above link to read more.

[Back to top](#)

Discord still a hotbed of malware activity — Now APTs join the fun

Discord continues to be a breeding ground for malicious activity by hackers and now APT groups, with it commonly used to distribute malware, exfiltrate data, and targeted by threat actors to steal authentication tokens.

<https://www.bleepingcomputer.com/news/security/discord-still-a-hotbed-of-malware-activity-now-apt-join-the-fun/>

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



OCIO

Office of the
Chief Information Officer