



July 9, 2024

Theme of the month: Deepfakes
(look for the 🗑️)

Challenge yourself with our [Deepfakes Quiz!](#)

What you can do to improve your AI security:

All Users	Technical Users	Business Owners
Be aware of the terms and conditions of online services and how they use your data to train their AI algorithms. The full risks involved with this are still unknown.	Provide a clear explanation of how, why, and where an AI system (chatbots, machine-learning and automated decision-making) is used, including a description of the system and its inputs and outputs.	Have your communications team create an ongoing AI awareness campaign to give your employees the tools and knowledge to recognize and detect AI-generated content. This includes, but is not limited to: deepfake images, video, and audio.

Check out our [AI Security Day videos](#) to learn more about AI security.

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

🗑️ 🍁 [Predator Ridge in Vernon, B.C. fully equips resort with AI-based wildfire detection systems](#)

🍁 [EC-Council's Community College Scholarship Initiative supports cybersecurity skills development](#)

[All Co-op cardlock locations across Western Canada back online in light of cybersecurity incident](#)

🗑️ [OpenAI's internal AI details stolen in 2023 breach, NYT reports](#)

[EU opens applications for cybersecurity and digital skills funding](#)

[New SnailLoad side-channel attack let hackers monitor your web activity](#)

[Fix NHS gaps or face more attacks - ex cyber chief](#) [New APT group "CloudSorcerer" targets Russian government entities](#)

Predator Ridge in Vernon, B.C. fully equips resort with AI-based wildfire detection systems

Following a successful pilot project, Predator Ridge in Vernon, B.C., has announced the commercial installation of an AI-based wildfire detection system.

<https://globalnews.ca/news/10609251/predator-ridge-ai-wildfire-detection-sensenet-vernon/amp/>

Click above link to read more.

[Back to top](#)

EC-Council's Community College Scholarship Initiative supports cybersecurity skills development

As a global leader in cybersecurity training and certifications, EC-Council has partnered with College of the North Atlantic (CNA) to support Canadian community colleges by providing additional scholarships for EC-Council learning resources and ancillaries.

<https://educationnewscanada.com/article/education/level/colleges/2/1092129/ec-council-s-community-college-scholarship-initiative-supports-cybersecurity-skills-development.html>

Click above link to read more.

[Back to top](#)

All Co-op cardlock locations across Western Canada back online in light of cybersecurity incident

All 398 Co-op cardlock locations across Western Canada are back online, according to an update on Thursday.

<https://regina.ctvnews.ca/all-co-op-cardlock-locations-across-western-canada-back-online-in-light-of-cybersecurity-incident-1.6951686>

Click above link to read more.

[Back to top](#)

OpenAI's internal AI details stolen in 2023 breach, NYT reports

A hacker gained access to the internal messaging systems at OpenAI last year and stole details about the design of the company's artificial intelligence technologies, the New York Times reported, opens new tab on Thursday.

<https://www.reuters.com/technology/cybersecurity/openais-internal-ai-details-stolen-2023-breach-nyt-reports-2024-07-05/>

Click above link to read more.

[Back to top](#)

EU opens applications for cybersecurity and digital skills funding

The EU Commission has opened applications for over €210m (\$227.3m) in funding for cybersecurity and digital skills programs.

<https://www.infosecurity-magazine.com/news/eu-funding-cybersecurity-funding/>

Click above link to read more.

[Back to top](#)

New SnailLoad side-channel attack let hackers monitor your web activity

Hackers often monitor web activities to gather several types of confidential data.

<https://cybersecuritynews.com/snailload-side-channel-attack/>

Click above link to read more.

[Back to top](#)

Fix NHS gaps or face more attacks - ex cyber chief

A leading cybersecurity expert has warned that the NHS remains vulnerable to further cyber-attacks unless it updates its computer systems.

<https://www.bbc.com/news/articles/czd9glyx414o>

Click above link to read more.

[Back to top](#)

New APT group "CloudSorcerer" targets Russian government entities

A previously undocumented advanced persistent threat (APT) group dubbed CloudSorcerer has been observed targeting Russian government entities by leveraging cloud services for command-and-control (C2) and data exfiltration.

<https://thehackernews.com/2024/07/new-apt-group-cloudsorcerer-targets.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
Cybersecurity and Digital Trust Branch



OCIO

Office of the
Chief Information Officer