

February 6, 2024

Challenge yourself with our [Employment Scams Quiz!](#)

Cybersecurity theme of the week: **Ransomware**

🌟 Check out our [Ransomware Infosheet](#) to learn more.

Wonder what you can do to protect yourself from ransomware?

All Users	Technical Users	Business Owners
Regularly back up your files and data to ensure they are up to date.	Use the 3-2-1 rule: Make 3 backups of your data, on 2 different types of media, with at least 1 backup offsite for disaster recovery.	Periodically create system backups in case a malware attack succeeds.

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

🍁 [Canada's foreign affairs department hit by data breach](#)

🍁 [How attractive are our Canadian cities to cybersecurity professionals – and why does it matter?](#)

🍁 [Windsor hospital's cyberattack recovery will take most of 2024, CEO says](#)

[Chicago children's hospital network down as experts warn of rising cyber threats](#)

[EU launches first cybersecurity certification for digital products](#)

[Clorox says cyberattack caused \\$49 million in expenses](#)

[80% of comments on major project tweets revealed as phishing scams: SlowMist](#)

[HopSkipDrive says personal data of 155,000 drivers stolen in data breach](#)

[Cyberattack on Pennsylvania courts didn't appear to compromise data, officials say](#)

[Proposals to prevent cyber-attacks on key services](#)

★ [LockBit ransomware group demands \\$11 million from government to unlock files](#)

[Watermarks expose deep fakes and increase cyber security](#)

Canada's foreign affairs department hit by data breach

The Canadian government said on Tuesday that its global affairs department suffered a data breach and that there was unauthorized access to personal information of users including employees.

<https://www.reuters.com/technology/cybersecurity/canadas-foreign-affairs-department-hit-by-data-breach-2024-01-30/>

Click above link to read more.

[Back to top](#)

How attractive are our Canadian cities to cybersecurity professionals – and why does it matter?

Canada was the fifth most targeted country for cyber attacks in the world last year, according to the 2023 Blackberry Threat Report. These attacks hit our corporate and public infrastructure, and affect the livelihood and the lives of all Canadians.

<https://www.itworldcanada.com/article/how-attractive-are-our-canadian-cities-to-cybersecurity-professionals-and-why-does-it-matter/557861>

Click above link to read more.

[Back to top](#)

Windsor hospital's cyberattack recovery will take most of 2024, CEO says

It will take most of this year for Windsor Regional Hospital to fully recover from a cyberattack that rocked five southwestern Ontario hospitals last fall.

<https://windsorstar.com/news/local-news/windsor-hospitals-cyberattack-recovery-will-take-most-of-2024-ceo-says>

Click above link to read more.

[Back to top](#)

Chicago children's hospital network down as experts warn of rising cyber threats

Chicago pediatric hospital Lurie Children's has been forced to take its network offline in the face of a "cybersecurity matter" as experts warn of heightened threats against health systems across the country.

<https://www.statnews.com/2024/02/02/healthcare-cyber-security-lurie-childrens-hospitals-hacking/>

Click above link to read more.

[Back to top](#)

EU launches first cybersecurity certification for digital products

The EU has adopted its first Cybersecurity Certification scheme as part of efforts to boost cybersecurity of IT products and services across member states.

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

Click above link to read more.

[Back to top](#)

Clorox says cyberattack caused \$49 million in expenses

Clorox has confirmed that a September 2023 cyberattack has so far cost the company \$49 million in expenses related to the response to the incident.

<https://www.bleepingcomputer.com/news/security/clorox-says-cyberattack-caused-49-million-in-expenses/>

Click above link to read more.

[Back to top](#)

80% of comments on major project tweets revealed as phishing scams: SlowMist

SlowMist's investigation uncovered a troubling revelation of widespread theft driven by phishing tweets.

<https://cryptopotato.com/80-of-comments-on-major-project-tweets-revealed-as-phishing-scams-slowmist/>

Click above link to read more.

[Back to top](#)

HopSkipDrive says personal data of 155,000 drivers stolen in data breach

Student rideshare startup HopSkipDrive has confirmed a data breach involving the personal data of more than 155,000 drivers.

<https://techcrunch.com/2024/02/05/hopskipdrive-says-personal-data-of-155000-drivers-stolen-in-data-breach/>

Click above link to read more.

[Back to top](#)

Cyberattack on Pennsylvania courts didn't appear to compromise data, officials say

A weekend cyberattack on the website of Pennsylvania's state courts agency disabled some online systems but did not appear to compromise any data and didn't stop the courts from opening Monday, officials said.

<https://ca.finance.yahoo.com/news/pennsylvania-statewide-court-agencys-website-122613463.html>

Click above link to read more.

[Back to top](#)

Proposals to prevent cyber-attacks on key services

New laws are set to be put in place to protect key services from cyber threats, the Manx government has said.

<https://www.bbc.com/news/articles/cd1jz149n5jo>

Click above link to read more.

[Back to top](#)

LockBit ransomware group demands \$11 million from government to unlock files

A devastating ransomware attack by Lockbit recently targeted the charming city of Calvià in Majorca, Spain, which is well-known for its tourism appeal.

<https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/lockbit-ransomware/amp/>

Click above link to read more.

[Back to top](#)

Watermarks expose deep fakes and increase cyber security

"A picture is worth a thousand words", the saying goes, but is that really true? As early as the American Civil War, elements of different photographs were combined to enhance the heroics. A retouching brush was used to erase the disgraced from images of various world events.

<https://www.hamburg-news.hamburg/en/innovation-science/watermarks-expose-deep-fakes-and-increase-cyber-security>

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