

October 24, 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: **SOCIAL MEDIA SECURITY**

🔗 Read our [**SAFETY TIPS FOR SOCIAL NETWORKING INFOSHEET**](#) to learn more.

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

🍁 [Lantzville tech firm collaborates with Microsoft on global cybersecurity report](#)

🍁 [IBM Canada makes uOttawa the home of its first university-based cybersecurity training hub for governments and businesses](#)

🍁 [Canadian organizations averaged 25 cybersecurity incidents in the past year, finds EY survey](#)

[Iran-linked OilRig targets Middle East governments in 8-month cyber campaign](#)

[EU elections at risk with rise of AI-enabled information manipulation](#)

🔗 [Commonwealth Bank sounds alarm on deepfake and social media-based cyber threats](#)

[DoNot Team's new Firebird backdoor hits Pakistan and Afghanistan](#)

[New Artificial Intelligence Solution improves cybersecurity](#)

[New ExelaStealer attack Windows PCs and steals private data](#)

[Philippines faces cybersecurity crisis as hackers expose state secrets, personal data](#)

[Hackers using money-making scripts to deliver multiple malware](#)

[Europol dismantles Ragnar Locker ransomware infrastructure, nabs key developer](#)

Lantzville tech firm collaborates with Microsoft on global cybersecurity report

In a world where hackers attack home computer systems to steal identity, bank and credit card information, there is ever-present danger of cyberattack to hardware that controls everything from traffic lights to gas and water pipelines and the electrical grid.

<https://www.nanaimobulletin.com/local-news/lantzville-tech-firm-collaborates-with-microsoft-on-global-cybersecurity-report-5934566>

Click above link to read more.

[Back to top](#)

IBM Canada makes uOttawa the home of its first university-based cybersecurity training hub for governments and businesses

The University of Ottawa and IBM Canada announced the official opening of the new uOttawa-IBM Cyber Range. IBM's first Cyber Range partnership on a Canadian university campus offers highly realistic cyber response training exercises to help businesses and government organizations across the country better prepare for cyber threats, including how to plan, respond, manage, contain, and remediate cyberattacks.

<https://www.canadianmanufacturing.com/risk-and-compliance/ibm-canada-makes-uottawa-the-home-of-its-first-university-based-cybersecurity-training-hub-for-governments-and-businesses-295435/>

Click above link to read more.

[Back to top](#)

Canadian organizations averaged 25 cybersecurity incidents in the past year, finds EY survey

The EY 2023 Global Cybersecurity Leadership Insights Study finds that 81% of Canadian organizations had experienced at least 25 cybersecurity incidents in the last 12 months, compared to 73% of global respondents.

<https://www.newswire.ca/news-releases/canadian-organizations-averaged-25-cybersecurity-incidents-in-the-past-year-finds-ey-survey-808884037.html>

Click above link to read more.

[Back to top](#)

Iran-linked OilRig targets Middle East governments in 8-month cyber campaign

The Iran-linked OilRig threat actor targeted an unnamed Middle East government between February and September 2023 as part of an eight-month-long campaign.

<https://thehackernews.com/2023/10/iran-linked-oilrig-targets-middle-east.html>

Click above link to read more.

[Back to top](#)

EU elections at risk with rise of AI-enabled information manipulation

The findings of the 2023 Threat Landscape report of the European Union Agency for Cybersecurity (ENISA) highlights need for vigilance ahead of the upcoming European elections in 2024.

<https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation>

Click above link to read more.

[Back to top](#)

Commonwealth Bank sounds alarm on deepfake and social media-based cyber threats

Australia's largest financial institution, the Commonwealth Bank (CBA), has issued an alarming notice about being targeted by cybercriminals who employ sophisticated tactics including social media advertisements laced with malware and deepfake technology, reports the Australian.

<https://au.investing.com/news/stock-market-news/commonwealth-bank-sounds-alarm-on-deepfake-and-social-mediabased-cyber-threats-3005460>

Click above link to read more.

[Back to top](#)

DoNot Team's new Firebird backdoor hits Pakistan and Afghanistan

The threat actor known as DoNot Team has been linked to the use of a novel .NET-based backdoor called Firebird targeting a handful of victims in Pakistan and Afghanistan.

<https://thehackernews.com/2023/10/donot-teams-new-firebird-backdoor-hits.html>

Click above link to read more.

[Back to top](#)

New Artificial Intelligence Solution improves cybersecurity

A groundbreaking new technology called the Artificial Intelligence (AI) Solution has been developed to enhance cybersecurity measures. This innovative solution utilizes advanced AI algorithms, which enable it to detect and prevent cyber threats in real-time. With the ever-increasing complexity and frequency of cyber attacks, this development comes as a profound advancement in protecting sensitive information.

<https://gameishard.gg/news/new-artificial-intelligence-solution-improves-cybersecurity/444637/>

Click above link to read more.

[Back to top](#)

New ExelaStealer attack Windows PCs and steals private data

A new InfoStealer called ExelaStealer emerged in 2023, joining the ranks of other well-known malware like RedLine, Raccoon, and Vidar.

<https://cybersecuritynews.com/new-exelastealer-attack-windows/>

Click above link to read more.

[Back to top](#)

Philippines faces cybersecurity crisis as hackers expose state secrets, personal data

In a recent series of cyber incidents, the Philippines' weak cybersecurity practices have left government websites susceptible to breaches, endangering the security of millions of citizens.

<https://www.wionews.com/world/philippines-faces-cybersecurity-crisis-as-state-secrets-personal-data-exposed-by-hackers-649856>

Click above link to read more.

[Back to top](#)

Hackers using money-making scripts to deliver multiple malware

The FBI warned about attacks on government and non-profit organizations in April, which involved deploying multiple malware strains on victim devices.

<https://cybersecuritynews.com/hackers-using-scripts-deliver-multiple-malware/>

Click above link to read more.

[Back to top](#)

Europol dismantles Ragnar Locker ransomware infrastructure, nabs key developer

Europol on Friday announced the takedown of the infrastructure associated with Ragnar Locker ransomware, alongside the arrest of a "key target" in France.

<https://thehackernews.com/2023/10/europol-dismantles-ragnar-locker.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

Information Security Branch



OCIO

Office of the
Chief Information Officer