

October 10, 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 ENGINEERING**

🌟 Read our [**SOCIAL ENGINEERING INFOSHEET**](#) to learn more.

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

🍁 [Survey finds small business owners don't know they're vulnerable to cyber attacks](#)

🍁 [BlackBerry to split cybersecurity, IoT divisions](#)

🍁 [National approach to cyber security education needed as attacks will only get worse: Teacher](#)

[AI: Voice cloning tech emerges in Sudan civil war](#)

[University of Oregon offers new major focusing on cybersecurity](#)

[The top 9 cyber security incidents in September 2023](#)

[Threat actors deployed hundreds of Python packages to steal system data](#)

🌟 [Seniors organization names social engineering its Medicare fraud of the month](#)

[23andMe suffers credential stuffing cyber attack](#)

[Spanish airline Air Europa hit by credit card system breach](#)

[Google makes passkeys the default sign-in for personal accounts](#)

[Activist Hackers Are Racing Into the Israel-Hamas War—for Both Sides](#)

Survey finds small business owners don't know they're vulnerable to cyber attacks

October is Cyber Security Awareness Month and the Insurance Bureau of Canada says it's a good time for business owners to assess their cyber risk.

<https://northernontario.ctvnews.ca/survey-finds-small-business-owners-don-t-know-they-re-vulnerable-to-cyber-attacks-1.6590981>

Click above link to read more.

[Back to top](#)

BlackBerry to split cybersecurity, IoT divisions

BlackBerry has made it official: It plans to split the Canadian company in half.

In a news release Wednesday, the company said its board has decided that separating the IoT and Cybersecurity business units into two independently-operated entities "is the optimal strategic direction for BlackBerry."

<https://www.itworldcanada.com/article/blackberry-to-split-cybersecurity-iot-divisions/548368>

Click above link to read more.

[Back to top](#)

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](#)

AI: Voice cloning tech emerges in Sudan civil war

A campaign using artificial intelligence to impersonate Omar al-Bashir, the former leader of Sudan, has received hundreds of thousands of views on TikTok, adding online confusion to a country torn apart by civil war.

<https://www.bbc.com/news/world-africa-66987869>

Click above link to read more.

[Back to top](#)

University of Oregon offers new major focusing on cybersecurity

With an increasing number of cyber-attacks, the University of Oregon is now offering a degree in cybersecurity. Industry professionals are giving high praise to the University of Oregon for the new major.

https://www.kezi.com/news/university-of-oregon-offers-new-major-focusing-on-cybersecurity/article_916f41de-6322-11ee-bc45-87a16384800a.html

Click above link to read more.

[Back to top](#)

The top 9 cyber security incidents in September 2023

An exploration of the most impactful cyber attacks and data breaches in September 2023

<https://www.cshub.com/attacks/news/top-cyber-security-incidents-september-23>

Click above link to read more.

[Back to top](#)

Threat actors deployed hundreds of Python packages to steal system data

In the open-source ecosystem, shadows shift as collaboration succeeds, attracting both novices and skilled threat actors. A rising threat has been evolving and sharpening its tools in recent months.

<https://cybersecuritynews.com/malicious-python-packages/>

Click above link to read more.

[Back to top](#)

Seniors organization names social engineering its Medicare fraud of the month

In its Sept. 28 news release, StateWide defined social engineering as “the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes,” and added, “Scammers are using social engineering tactics, artificial intelligence, chatbots, and robocalls to commit Medicare fraud.”

<https://hme-business.com/seniors-organization-names-social-engineering-its-medicare-fraud-of-the-month/>

Click above link to read more.

[Back to top](#)

23andMe suffers credential stuffing cyber attack

Biotechnology company 23andMe, which offers genetic testing and genealogy services, has announced that it was the victim of a data breach following a credential stuffing attack.

<https://www.cshub.com/attacks/news/23andme-credential-stuffing>

Click above link to read more.

[Back to top](#)

Spanish airline Air Europa hit by credit card system breach

Spanish airline Air Europa has suffered a cyberattack on its online payment system that let some of its customers' credit card details exposed, the company said on Tuesday.

<https://www.reuters.com/business/aerospace-defense/spanish-airline-air-europa-hit-by-credit-card-system-breach-2023-10-10/>

Click above link to read more.

[Back to top](#)

Google makes passkeys the default sign-in for personal accounts

Google announced today that passkeys are now the default sign-in option across all personal Google Accounts across its services and platforms.

<https://www.bleepingcomputer.com/news/security/google-makes-passkeys-the-default-sign-in-for-personal-accounts/>

Click above link to read more.

[Back to top](#)

Activist Hackers Are Racing Into the Israel-Hamas War—for Both Sides

Since the conflict escalated, hackers have targeted dozens of government websites and media outlets with defacements and DDoS attacks, and attempted to overload targets with junk traffic to bring them down.

<https://www.wired.com/story/israel-hamas-war-hacktivism/>

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.

