

December 12, 2023

Challenge yourself with our Multi-factor Authentication Quiz!

Cybersecurity Issue of the Week: **CYBERSECURITY AWARENESS**

★ Check out our **SAFE COMPUTING RESOURCES** to learn more.

This past year's stories:

🍁 **Canada, allies issue cyber threat alert after hacking plot linked to Russia's FSB exposed**

🍁 **Small Canadian energy producer reports cybersecurity incident**

🍁 **Nova Scotia information commissioner to investigate file-sharing cybersecurity breach**

🍁 **Are companies falling behind on cyber security awareness training?**

New Bluetooth flaw let hackers take over Android, Linux, macOS, and iOS devices

🌐 **Cyber-attacks more likely than fire or theft, Aviva research finds**
Russian hackers exploiting Outlook zero-day to attack NATO member countries

We asked the experts: What cybersecurity trends will shape 2024?

Webinar — psychology of social engineering: Decoding the mind of a cyber attacker

Hackers hijacked water facility that interrupted the supply

SpyLoan scandal: 18 malicious Loan apps defraud millions of Android users

Greece setting up national cybersecurity agency to battle hackers

Canada, allies issue cyber threat alert after hacking plot linked to Russia's FSB exposed

Canada and its Five Eyes allies have issued a joint cybersecurity threat advisory warning of Russian cyberattacks after the British government said it exposed a years-long hacking plot by a group aligned with Russia's Federal Security Service (FSB).

<https://globalnews.ca/news/10155272/russia-cyber-attacks-uk-us-star-blizzard/>

Click above link to read more.

[Back to top](#)

Small Canadian energy producer reports cybersecurity incident

A Calgary oil and gas producer says it has suffered a cybersecurity incident that impacted certain aspects of its business.

<https://www.itworldcanada.com/article/small-canadian-energy-producer-reports-cybersecurity-incident/554760>

Click above link to read more.

[Back to top](#)

Nova Scotia information commissioner to investigate file-sharing cybersecurity breach

Nova Scotia's information and privacy commissioner has launched an investigation into the theft of personal information from a file-transfer system used by the provincial government.

<https://globalnews.ca/news/10154853/nova-scotia-commissioner-investigate-file-sharing-cybersecurity-breach/>

Click above link to read more.

[Back to top](#)

Are companies falling behind on cyber security awareness training?

New data from a Waterloo-based cyber security service suggests hackers have shifted their tactics and companies may not be keeping up.

<https://kitchener.ctvnews.ca/are-companies-falling-behind-on-cyber-security-awareness-training-1.6676430>

Click above link to read more.

[Back to top](#)

New Bluetooth flaw let hackers take over Android, Linux, macOS, and iOS devices

Story text. A critical Bluetooth security flaw could be exploited by threat actors to take control of Android, Linux, macOS and iOS devices.

<https://thehackernews.com/2023/12/new-bluetooth-flaw-let-hackers-take.html>

Click above link to read more.

[Back to top](#)

Cyber-attacks more likely than fire or theft, Aviva research finds

In today's digital world, businesses are just as vulnerable to cyber-attacks as they are to fire and theft. New research from insurance provider Aviva found that businesses are 67% more likely to experience a cyber incident than a physical theft and almost five times as likely to have an attack as a fire.

<https://www.infosecurity-magazine.com/news/cyberattacks-more-likely-than-fire/>

Click above link to read more.

[Back to top](#)

Russian hackers exploiting Outlook zero-day to attack NATO member countries

Using a zero-day exploit in Microsoft Outlook (tracked as CVE-2023-23397), Fighting Ursa Aka APT28 targets at least 30 companies across 14 countries that are probably significant sources of strategic intelligence for the Russian government and military.

<https://cybersecuritynews.com/russian-hackers-exploiting-outlook/>

Click above link to read more.

[Back to top](#)

We asked the experts: What cybersecurity trends will shape 2024?

There's a lot to reflect on how cybersecurity has changed this year, and what there is to be excited about as we enter 2024.

<https://techround.co.uk/news/experts-cybersecurity-trends-2024/>

Click above link to read more.

[Back to top](#)

Webinar — psychology of social engineering: Decoding the mind of a cyber attacker

In the ever-evolving cybersecurity landscape, one method stands out for its chilling effectiveness – social engineering. But why does it work so well? The answer lies in the intricate dance between the attacker's mind and human psychology.

<https://thehackernews.com/2023/12/webinar-psychology-of-social.html>

Click above link to read more.

[Back to top](#)

Hackers hijacked water facility that interrupted the supply

Recently, there was a cyberattack on an Irish water utility that resulted in hackers gaining control of the system and disrupting the water supply.

<https://cybersecuritynews.com/hackers-hijacked-water-utility/>

Click above link to read more.

[Back to top](#)

SpyLoan scandal: 18 malicious Loan apps defraud millions of Android users

Cybersecurity researchers have discovered 18 malicious loan apps for Android on the Google Play Store that have been collectively downloaded over 12 million times.

<https://thehackernews.com/2023/12/spyloan-scandal-18-malicious-loan-apps.html>

Click above link to read more.

[Back to top](#)

Greece setting up national cybersecurity agency to battle hackers

As hackers – ransomware groups and state-backed too – target governments, state agencies, utilities, schools, hospitals and businesses – Greece is creating a national cybersecurity agency to thwart them.

<https://www.thenationalherald.com/greece-setting-up-national-cybersecurity-agency-to-battle-hackers/>

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.

