

January 9, 2024

Challenge yourself with our Quishing Quiz!

Cybersecurity Issue of the Week: **AI**

🌟 Check out our **Security Day AI presentation videos** to learn more.

How to protect yourself based on your user group:

All Users	Technical Users	Business Owners
Learn the nuances of AI generated content so you can successfully detect when something is AI generated.	Always vet your resources and double check information before redistributing or citing it.	Prepare your employees with the tools and knowledge to recognize and detect deepfaked images, video, and audio.

This past week's stories:

🍁 **Toronto Zoo latest public body to be hit by cybersecurity attack**

🍁 **St. Albert plans cybersecurity audit**

🌟🍁 **AI-generated videos a growing threat to elections, Canadian head of cybersecurity warns**

🍁 **USask cybersecurity expert weighs in on AI benefits and risks**

🍁 **Agriculture sector encouraged to look at cyber security**

Malware using Google MultiLogin exploit to maintain access despite password reset

What the cybersecurity workforce can expect in 2024

Russian hackers had covert access to Ukraine's telecom giant for months

SpectralBlur: New macOS backdoor threat from North Korean hackers

Threat actors use social engineering and AI to drive more cyber attacks in 2024, says GlobalData

MoD cybersecurity worst in Whitehall, figures reveal

How strong cybersecurity hygiene can help rural healthcare systems hack off the hackers

NIST issues cybersecurity guide for AI developers

Toronto Zoo latest public body to be hit by cybersecurity attack

The Toronto Zoo announced Monday it's been hit by a recent cybersecurity attack and as a result customer response times may be impacted.

<https://www.cbc.ca/news/canada/toronto/toronto-zoo-cybersecurity-attack-1.7077721>

Click above link to read more.

[Back to top](#)

St. Albert plans cybersecurity audit

The City of St. Albert is planning an audit of its cybersecurity processes, policies, and programs this spring.

<https://www.stalbertgazette.com/local-news/st-albert-plans-cybersecurity-audit-8034806>

Click above link to read more.

[Back to top](#)

AI-generated videos a growing threat to elections, Canadian head of cybersecurity warns

Canada's cybersecurity czar says he doesn't yet know how to publicly "deauthenticate" AI-powered fake videos as his agency warns of the growing threat of disinformation campaigns in upcoming elections.

<https://nationalpost.com/news/canada/ai-videos-growing-threat-elections-cybersecurity>

Click above link to read more.

[Back to top](#)

USask cybersecurity expert weighs in on AI benefits and risks

Artificial intelligence has been taking the world by storm as the powers of tools such as ChatGPT and others have become available to the public.

<https://news.usask.ca/articles/research/2024/usask-cybersecurity-expert-weighs-in-on-ai-benefits-and-risks.php>

Click above link to read more.

[Back to top](#)

Agriculture sector encouraged to look at cyber security

When it comes to cyber security research from the University of Guelph suggests agriculture is behind the curve.

<https://discovermoosejaw.com/articles/agriculture-sector-encouraged-to-look-at-cyber-security>

Click above link to read more.

[Back to top](#)

Malware using Google MultiLogin exploit to maintain access despite password reset

Information stealing malware are actively taking advantage of an undocumented Google OAuth endpoint named MultiLogin to hijack user sessions and allow continuous access to Google services even after a password reset.

<https://thehackernews.com/2024/01/malware-using-google-multilogin-exploit.html>

Click above link to read more.

[Back to top](#)

What the cybersecurity workforce can expect in 2024

For cybersecurity professionals, 2023 was a mixed bag of opportunities and concerns. The good news is that the number of people in cybersecurity jobs has reached its highest number ever: 5.5 million, according to the 2023 ISC2 Global Workforce Study. However, the same study reported that there is still a serious shortfall. To best address threat landscape challenges, the workforce needs to grow at a rate of 12.6 percent a year. In the 2023 study, it only grew by 8.7 percent.

<https://securityintelligence.com/articles/cybersecurity-workforce-trends-2024/>

Click above link to read more.

[Back to top](#)

Russian hackers had covert access to Ukraine's telecom giant for months

Ukrainian cybersecurity authorities have disclosed that the Russian state-sponsored threat actor known as Sandworm was inside telecom operator Kyivstar's systems at least since May 2023.

<https://thehackernews.com/2024/01/russian-hackers-had-covert-access-to.html>

Click above link to read more.

[Back to top](#)

SpectralBlur: New macOS backdoor threat from North Korean hackers

Cybersecurity researchers have discovered a new Apple macOS backdoor called SpectralBlur that overlaps with a known malware family that has been attributed to North Korean threat actors.

<https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.html>

Click above link to read more.

[Back to top](#)

Threat actors use social engineering and AI to drive more cyber attacks in 2024, says GlobalData

A major trend in cybersecurity is the speed and adeptness with which hackers adapt their techniques to leverage technological advances. Attacks making use of social engineering have become more frequent and more expensive in 2023. The profitability and the simplicity of launching social engineering-related cyber attacks will drive an even higher volume of these incidents in 2024, according to GlobalData, a leading data and analytics company.

<https://telecomreseller.com/2024/01/04/threat-actors-tap-social-engineering-and-ai-to-drive-more-cyber-attacks-in-2024-says-globaldata/>

Click above link to read more.

[Back to top](#)

MoD cybersecurity worst in Whitehall, figures reveal

The UK Ministry of Defence has by far the worst protected IT systems of any Whitehall department, with 11 "red-rated" systems.

<https://www.computing.co.uk/news/4161325/mod-cybersecurity-worst-whitehall-figures-reveal>

Click above link to read more.

[Back to top](#)

How strong cybersecurity hygiene can help rural healthcare systems hack off the hackers

Unlike urban areas with readily accessible medical facilities, rural regions often lack nearby healthcare options. Some areas rely on a single hospital within a 100+ mile radius, and a cyberattack on such a hospital could leave thousands without healthcare, with potentially deadly outcomes.

<https://medcitynews.com/2024/01/how-strong-cybersecurity-hygiene-can-help-rural-healthcare-systems-hack-off-the-hackers/>

Click above link to read more.

[Back to top](#)

NIST issues cybersecurity guide for AI developers

No foolproof method exists so far for protecting artificial intelligence systems from misdirection, warns an American standards body, and AI developers and users should be wary of any who claim otherwise.

<https://channeldailynews.com/news/nist-issues-cybersecurity-guide-for-ai-developers/84327>

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.

