



April 2, 2024

Challenge yourself with our Internet of Things (IoT) Quiz!

Cybersecurity theme of the week: **Phishing**

🌟 Check out our **Phishing Infosheet** to learn more.

Wonder what you can do to protect yourself from phishing attacks?

All Users	Technical Users	Business Owners
Don't click on links in emails you are unfamiliar with or look suspicious.	Familiarize yourself with phishing emails and your organization's process with dealing with them.	Have programs in place to generate awareness for phishing emails and each type of phishing email to train staff to recognize and report phishes.

This past week's stories:

🍁 **Huntsville confirms details of cybersecurity incident**

🍁 **Two-thirds of Canadian organizations expecting cybersecurity incident**

🍁 **University of Winnipeg network still reeling from 'cyber incident'**

Apple ID "push bombing" attack targeting Apple users to steal passwords

Hackers using weaponized virtual hard disk files to deliver Remcos RAT

2 Chrome zero-days exploited at Pwn2Own 2024: Patch now

🌟 **New Darcula phishing service targets iPhone users via iMessage**

Finland blames Chinese hacking group APT31 for parliament cyber attack

Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats

Sellafield nuclear waste dump to be prosecuted for alleged cybersecurity offences

Retailers add tech to meet consumer demand for biometric authentication

Hardest cybersecurity jobs to fill in 2024: Top roles & skills

Huntsville confirms details of cybersecurity incident

The Town of Huntsville is currently investigating a cybersecurity incident that occurred on March 10, 2024. In response to this incident, the Town immediately enacted its incident response protocol and engaged cybersecurity experts to investigate. The impact of the event resulted in service disruptions as systems were brought offline as a precautionary measure.

<https://www.bayshorebroadcasting.ca/2024/03/27/180299/>

Click above link to read more.

[Back to top](#)

Two-thirds of Canadian organizations expecting cybersecurity incident

A new study has revealed that a mere 1% of organizations in Canada have achieved the level of cybersecurity readiness required to effectively defend against modern risks.

<https://www.hcamag.com/ca/specialization/hr-technology/two-thirds-of-canadian-organizations-expecting-cybersecurity-incident/483116>

Click above link to read more.

[Back to top](#)

University of Winnipeg network still reeling from 'cyber incident'

A "cyber incident" at the University of Winnipeg that forced the cancellation of classes on Monday is still affecting several services students rely on, leaving some worried about exams and the safety of their personal information.

<https://www.cbc.ca/news/canada/manitoba/cyber-attack-university-winnipeg-classes-network-1.7156770>

Click above link to read more.

[Back to top](#)

Apple ID "push bombing" attack targeting Apple users to steal passwords

Apple users are falling prey to a sophisticated phishing campaign designed to hijack their Apple IDs through what's known as a "push bombing" or "MFA fatigue" attack.

<https://cybersecuritynews.com/apple-id-push-bombing-attack/>

Click above link to read more.

[Back to top](#)

Hackers using weaponized virtual hard disk files to deliver Remcos RAT

Hackers have been found leveraging weaponized virtual hard disk (VHD) files to deploy the notorious Remote Control Software (RAT), Remcos.

<https://cybersecuritynews.com/deliver-remcos-rat/>

Click above link to read more.

[Back to top](#)

2 Chrome zero-days exploited at Pwn2Own 2024: Patch now

Google patched seven vulnerabilities in the Chrome browser on Tuesday, including two zero-day exploits that were exploited at the Pwn2Own Vancouver 2024 hacking contest.

<https://cybersecuritynews.com/chrome-zero-days-pwn2own-2024-patch-now/>

Click above link to read more.

[Back to top](#)

New Darcula phishing service targets iPhone users via iMessage

A new phishing-as-a-service (PhaaS) named 'Darcula' uses 20,000 domains to spoof brands and steal credentials from Android and iPhone users in more than 100 countries.

<https://www.bleepingcomputer.com/news/security/new-darcula-phishing-service-targets-iphone-users-via-imessage/>

Click above link to read more.

[Back to top](#)

Finland blames Chinese hacking group APT31 for parliament cyber attack

The Police of Finland (aka Poliisi) has formally accused a Chinese nation-state actor tracked as APT31 for orchestrating a cyber attack targeting the country's Parliament in 2020.

<https://thehackernews.com/2024/03/finland-blames-chinese-hacking-group.html>

Click above link to read more.

[Back to top](#)

Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats

The European Union Agency for Cybersecurity (ENISA) publishes the executive summary of this year's 'Foresight Cybersecurity Threats for 2030' presenting an overview of key findings in the top 10 ranking.

<https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats>

Click above link to read more.

[Back to top](#)

Sellafield nuclear waste dump to be prosecuted for alleged cybersecurity offences

The Sellafield nuclear waste dump is to be prosecuted for alleged information technology security offences, the industry watchdog has said.

<https://www.theguardian.com/business/2024/mar/28/sellafield-nuclear-waste-dump-to-be-prosecuted-for-alleged-it-security-offences>

Click above link to read more.

[Back to top](#)

Retailers add tech to meet consumer demand for biometric authentication

With consumers looking for more frictionless authentication, retailers ranging from Whole Foods to Steak 'n Shake are adding biometric payments.

<https://www.pymnts.com/news/retail/2024/retailers-add-tech-meet-consumer-demand-biometric-authentication/>

Click above link to read more.

[Back to top](#)

Hardest cybersecurity jobs to fill in 2024: Top roles & skills

The cybersecurity job market is projected to grow by an impressive 32% through 2032, according to the U.S. Bureau of Labor Statistics (BLS), with about 16,800 openings for information security analysts each year.

<https://www.techopedia.com/hardest-cybersecurity-jobs-to-fill-and-essential-certifications>

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.

