

November 28, 2023

Challenge yourself with our [AI Quiz!](#)

Cybersecurity Issue of the Week: **RANSOMWARE**

★ Read our [RANSOMWARE INFOSHEET](#) to learn more.

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

🍁 [Feds aimed secret cybersecurity briefing at energy sector executives: memo](#)

🍁 [Work on 'high-risk' city cybersecurity issue roughly a year overdue](#)

🍁 [Facebook ads scamming customers with fake discounts, says Vancouver Island puzzle company](#)

🍁 [More than 2 million Canadians scammed on Black Friday and Cyber Monday](#)

[New flaws in fingerprint sensors let attackers bypass Windows Hello login](#)

★ [Play ransomware goes commercial - now offered as a service to cybercriminals](#)

[Australia beefs up cyber defences after major breaches](#)

[Fidelity National Financial shuts down network in wake of cybersecurity incident](#)

[North Korean hackers targeting CyberLink users in supply-chain attack](#)

[Cybersecurity firm executive pleads guilty to hacking hospitals](#)

[ClearFake a new malware attacking Mac users via fake browser updates](#)

[Apple's iPhone iOS17 NameDrop feature "major red flag" for cybersecurity, expert says](#)

Feds aimed secret cybersecurity briefing at energy sector executives: memo

Federal security officials have been briefing leaders of major energy and utility firms on cyberthreats, one element of a concerted government effort to underscore the serious risks to the sector.

[Link](#)

Click above link to read more.

[Back to top](#)

Work on 'high-risk' city cybersecurity issue roughly a year overdue

Five of six recommendations to tackle a "high-risk" municipal cybersecurity issue are now about a year overdue, as the city's auditor general lamented alarming delays from city officials.

<https://www.cbc.ca/news/canada/ottawa/work-on-high-risk-city-cybersecurity-issue-roughly-a-year-overdue-1.7041182>

Click above link to read more.

[Back to top](#)

Facebook ads scamming customers with fake discounts, says Vancouver Island puzzle company

David Manga said he first realized he had problems with his popular puzzle company about a month ago, when messages started pouring in about undelivered products.

<https://www.cbc.ca/news/canada/british-columbia/cobble-hill-puzzles-scam-1.7034457>

Click above link to read more.

[Back to top](#)

More than 2 million Canadians scammed on Black Friday and Cyber Monday

More than 2 million Canadians have been scammed in the past on Black Friday or Cyber Monday, according to a new survey by the cybersecurity company NordVPN.

<https://torontosun.com/news/national/more-than-2-million-canadians-scammed-on-black-friday-and-cyber-monday>

Click above link to read more.

[Back to top](#)

New flaws in fingerprint sensors let attackers bypass Windows Hello login

A new research has uncovered multiple vulnerabilities that could be exploited to bypass Windows Hello authentication on Dell Inspiron 15, Lenovo ThinkPad T14, and Microsoft Surface Pro X laptops.

<https://thehackernews.com/2023/11/new-flaws-in-fingerprint-sensors-let.html>

Click above link to read more.

[Back to top](#)

Play ransomware goes commercial - now offered as a service to cybercriminals

The ransomware strain known as Play is now being offered to other threat actors "as a service," new evidence unearthed by Adlumin has revealed.

<https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html>

Click above link to read more.

[Back to top](#)

Australia beefs up cyber defences after major breaches

Australia will give cyber health checks for small businesses, increase cyber law enforcement funding and introduce mandatory reporting of ransomware attacks under a security overhaul announced on Wednesday after a spate of attacks.

<https://www.reuters.com/technology/cybersecurity/australia-goes-cyber-offensive-with-sweeping-resilience-plan-2023-11-22/>

Click above link to read more.

[Back to top](#)

Fidelity National Financial shuts down network in wake of cybersecurity incident

Fidelity National Financial, or FNF, a Fortune 500 company that provides title insurance and settlement services for the mortgage and real estate industries, announced on Tuesday that it was the victim of a "cybersecurity incident that impacted certain FNF systems."

<https://techcrunch.com/2023/11/22/fidelity-national-financial-shuts-down-network-in-wake-of-cybersecurity-incident/>

Click above link to read more.

[Back to top](#)

North Korean hackers targeting CyberLink users in supply-chain attack

In the ever-evolving realm of cybersecurity, Microsoft Threat Intelligence has uncovered a sophisticated supply chain attack orchestrated by the North Korean Hackers Diamond Sleet (ZINC).

<https://cybersecuritynews.com/north-korean-hackers-cyberlink/>

Click above link to read more.

[Back to top](#)

Cybersecurity firm executive pleads guilty to hacking hospitals

The former chief operating officer of a cybersecurity company has pleaded guilty to hacking two hospitals, part of the Gwinnett Medical Center (GMC), in June 2021 to boost his company's business.

<https://www.bleepingcomputer.com/news/security/cybersecurity-firm-executive-pleads-guilty-to-hacking-hospitals/>

Click above link to read more.

[Back to top](#)

ClearFake a new malware attacking Mac users via fake browser updates

Mac users were targeted by a fake browser update chain called 'ClearFake', which was delivered by Atomic Stealer to compromise their systems.

<https://cybersecuritynews.com/clearfake-new-malware-mac/>

Click above link to read more.

[Back to top](#)

Apple's iPhone iOS17 NameDrop feature "major red flag" for cybersecurity, expert says

A number of local police departments have sent out a privacy warning about Apple's latest iOS 17 update for iPhones. The update includes a feature that allows for contact information to easily be shared called "NameDrop."

<https://www.cbsnews.com/philadelphia/news/how-to-turn-off-name-drop-on-iphones-ios17-cybersecurity/>

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.

