## August 8, 2023

**Challenge yourself with our Cryptocons Quiz!**

This past week's stories:

- **VIU falling short with cybersecurity measures, says B.C. auditor general**
- **Cyberattack on B.C. health websites may have taken personal information**
- **These smart features are designed to improve your cybersecurity hygiene**

**Microsoft flags growing cybersecurity concerns for major sporting events**

**Microsoft exposes Russian hackers' sneaky phishing tactics via Microsoft Teams chats**

**Retailers are failing to train employees in cybersecurity**

**New version of Rilide data theft malware adapts to Chrome Extension Manifest V3**

**Malicious apps use sneaky versioning technique to bypass Google Play Store scanners**

**Chrome security update: 15 critical vulnerabilities fixed, over $60,000 rewarded**

**Cybersecurity attack affects patient operations at Waterbury Health**

**Microsoft called out for 'blatantly negligent' cybersecurity practices**

**A cyberattack has disrupted hospitals and health care in several states**

**Deep-fake content is worming its way into our lives through our newsfeeds**

---

### VIU falling short with cybersecurity measures, says B.C. auditor general

Vancouver Island University is falling short in managing cybersecurity, an audit by the province's auditor general has found.

https://www.nanaimobulletin.com/news/viu-falling-short-with-cybersecurity-measures-says-bc-auditor-general-1291058

*Click above link to read more.*

Back to top

---

### Cyberattack on B.C. health websites may have taken personal information

The Health Employers Association of B.C says someone illegally breached one of its servers recently in a cyberattack.

https://vancouversun.com/news/local-news/cyberattack-bc-health-websites-may-have-taken-personal-information

*Click above link to read more.*

Back to top

---

### These smart features are designed to improve your cybersecurity hygiene

Canadians are online – and on their devices – more than ever before. While today's online experience reflects incredible advancements in technology and convenience, it also means that users have to pay that much more attention to what they share online.

https://www.theglobeandmail.com/business/adv/article-these-smart-features-are-designed-to-improve-your-cybersecurity/

*Click above link to read more.*

Back to top

---

### Microsoft flags growing cybersecurity concerns for major sporting events

Microsoft is warning of the threat malicious cyber actors pose to stadium operations, warning that the cyber risk surface of live sporting events is "rapidly expanding."

https://thehackernews.com/2023/08/microsoft-flags-growing-cybersecurity.html

*Click above link to read more.*

Back to top

---

## Microsoft exposes Russian hackers' sneaky phishing tactics via Microsoft Teams chats

Microsoft on Wednesday disclosed that it identified a set of highly targeted social engineering attacks mounted by a Russian nation-state threat actor using credential theft phishing lures sent as Microsoft Teams chats.

https://thehackernews.com/2023/08/microsoft-exposes-russian-hackers.html

*Click above link to read more.*

Back to top

---

## Retailers are failing to train employees in cybersecurity

Recent reports have found that over the past year there have been approximately 2.39 million instances of cybercrime and retail accounts for 62% of cybersecurity attacks in commerce, meaning businesses and employees need to be prepared.

https://www.retail-insight-network.com/news/retailers-are-failing-to-train-employees-in-cybersecurity/

*Click above link to read more.*

Back to top

---

## New version of Rilide data theft malware adapts to Chrome Extension Manifest V3

Cybersecurity researchers have discovered a new version of malware called Rilide that targets Chromium-based web browsers to steal sensitive data and steal cryptocurrency.

https://thehackernews.com/2023/08/new-version-of-rilide-data-theft.html

*Click above link to read more.*

Back to top

---

## Malicious apps use sneaky versioning technique to bypass Google Play Store scanners

Threat actors are leveraging a technique called versioning to evade Google Play Store's malware detections and target Android users.

https://thehackernews.com/2023/08/malicious-apps-use-sneaky-versioning.html

*Click above link to read more.*

Back to top

---

### Chrome security update: 15 critical vulnerabilities fixed, over $60,000 rewarded

Google has published a security update for Chrome, updating the Stable channel for Mac and Linux to 115.0.5790.170 and 115.0.5790.170/.171 for Windows. The release of this upgrade will take place over the coming days/weeks.

https://cybersecuritynews.com/chrome-security-update-patch-now/

*Click above link to read more.*

Back to top

---

### Cybersecurity attack affects patient operations at Waterbury Health

A cybersecurity attack is affecting patient operations at Waterbury Health locations on Thursday.

https://www.wfsb.com/2023/08/03/cybersecurity-attack-affects-patient-operations-waterbury-health/

*Click above link to read more.*

Back to top

---

### Microsoft called out for 'blatantly negligent' cybersecurity practices

Microsoft is facing mounting criticism in the wake of last month's attack on Azure. In a post on LinkedIn, Amit Yoran, the CEO of the cybersecurity company Tenable, says Microsoft's cybersecurity track record is "even worse than you think" — and he has an example to back it up.

https://www.theverge.com/2023/8/3/23819237/microsoft-azure-breach-blatantly-negligent-cybersecurity-practices

*Click above link to read more.*

Back to top

---

### A cyberattack has disrupted hospitals and health care in several states

A cyberattack has disrupted hospital computer systems in several states, forcing some emergency rooms to close and ambulances to be diverted, and many primary care services remained closed on Friday as security experts worked to determine the extent of the problem and resolve it.

https://abcnews.go.com/Health/wireStory/cyberattack-disrupted-hospitals-health-care-states-102017847

*Click above link to read more.*

Back to top

---

**Deep-fake content is worming its way into our lives through our newsfeeds**

We are long past the point where an untrained eye can distinguish signs of artificial intelligence-generated images or videos, popularly known as "deep-fakes."

https://thehill.com/opinion/cybersecurity/4139646-deep-fake-content-is-worming-its-way-into-our-lives-through-our-newsfeeds/

*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.