
## October 31, 2023

**Challenge yourself with our Cyber Security Awareness Month Quiz!**

**Take part in Cyber Security Awareness Month: www.gov.bc.ca/cybersecurityawarenessmonth**

Cybersecurity Issue of the Week: **Spyware**

✪ Read our **Spyware Infosheet** to learn more.

This past week's stories:

**Toronto Public Library dealing with cybersecurity 'incident' impacting some services**
**Cyberattack impacting local hospital systems leaves patients in limbo**
**Biden signs executive order to oversee and invest in AI**
**1Password detects suspicious activity following Okta support breach**
**Microsoft warns as Scattered Spider expands from SIM swaps to ransomware**
**Nation state hackers exploiting zero-day in Roundcube webmail software**
**Hackers hijack Facebook business accounts to run malicious ads**
**Hackers launch a chain of exploits via malicious iMessage attachments**
✪ **Israel-Hamas war: Pegasus makers, other blacklisted spyware firms roped in to track hostages in Gaza**
**City navigates recovery from summer cyberattack**
**Key learnings from "big game" ransomware campaigns**
**Oldham Council facing 10,000 cyber attacks a day, report says**
**AI and a tale of two tech earnings reports, company leaders unaware of (or unprepared for) cybersecurity risks**
**Beware of fake Google Chrome update that installs malware**

---

### Toronto Public Library dealing with cybersecurity 'incident' impacting some services

Some online Toronto Public Library services are unavailable after a cybersecurity "incident" was detected on Saturday, the library said Sunday.

https://www.cbc.ca/news/canada/toronto/toronto-public-library-cyber-security-1.7012099

*Click above link to read more.*

Back to top

---

### Cyberattack impacting local hospital systems leaves patients in limbo

With a history of cancer, Kristy Anthony says she was scheduled to have an ultrasound Monday at Windsor Regional Hospital's Met Campus.

https://windsor.ctvnews.ca/cyberattack-impacting-local-hospital-systems-leaves-patients-in-limbo-1.6615354

*Click above link to read more.*

Back to top

---

### Biden signs executive order to oversee and invest in AI

President Joe Biden signed a wide-ranging executive order on artificial intelligence Monday, setting the stage for some industry regulations and funding for the U.S. government to further invest in the technology.

https://www.nbcnews.com/tech/tech-news/biden-signs-executive-order-ai-rcna122468

*Click above link to read more.*

Back to top

---

### 1Password detects suspicious activity following Okta support breach

Popular password management solution 1Password said it detected suspicious activity on its Okta instance on September 29 following the support system breach, but reiterated that no user data was accessed.

https://thehackernews.com/2023/10/1password-detects-suspicious-activity.html

*Click above link to read more.*

Back to top

---

### Microsoft warns as Scattered Spider expands from SIM swaps to ransomware

The prolific threat actor known as Scattered Spider has been observed impersonating newly hired employees in targeted firms as a ploy to blend into normal on-hire processes and takeover accounts and breach organizations across the world.

https://thehackernews.com/2023/10/microsoft-warns-as-scattered-spider.html#:~:text=The%20prolific%20threat%20actor%20known,breach%20organizations%20across%20the%20world.

*Click above link to read more.*

Back to top

---

### Nation state hackers exploiting zero-day in Roundcube webmail software

The threat actor known as Winter Vivern has been observed exploiting a zero-day flaw in Roundcube webmail software on October 11, 2023, to harvest email messages from victims' accounts.

https://thehackernews.com/2023/10/nation-state-hackers-exploiting-zero.html

*Click above link to read more.*

Back to top

---

### Hackers hijack Facebook business accounts to run malicious ads

Cybercriminals have been exploiting Facebook business accounts by gaining unauthorized access to them and launching advertising campaigns under the guise of legitimate account owners. As a result, the victims are forced to bear the financial burden of these fraudulent campaigns.

https://cybersecuritynews.com/hackers-hijack-facebook/#google_vignette

*Click above link to read more.*

Back to top

---

### Hackers launch a chain of exploits via malicious iMessage attachments

In June, a new campaign targeting iPhone and iPad devices was named “TriangleDB.” This malware infection chain consists of a malicious iMessage attachment, which launches a chain of exploits on the affected devices.

https://cybersecuritynews.com/exploits-via-imessage-attachments/

*Click above link to read more.*

Back to top

---

### Israel-Hamas war: Pegasus makers, other blacklisted spyware firms roped in to track hostages in Gaza

Since its ghastly attack on Israel, Hamas has kept hundreds of Israelis including foreigners captive in Gaza. In a major development, Israeli security forces have roped in spyware firms like Pegasus maker to track hostages in the Gaza strip, reported Bloomberg citing sources.

https://www.livemint.com/news/world/israelhamas-war-pegasus-makers-other-backlisted-spyware-firms-roped-in-to-track-hostages-in-gaza-11698332628596.html

*Click above link to read more.*

Back to top

---

### City navigates recovery from summer cyberattack

Hackers broke into the New Haven Public Schools' chief operating officer email and stole millions from the city school system this past summer.

https://yaledailynews.com/blog/2023/10/26/city-navigates-recovery-from-summer-cyberattack/

*Click above link to read more.*

Back to top

---

### Key learnings from "big game" ransomware campaigns

A mid-year crypto crime update released in July by Chainalysis found that cryptocurrency related crime was trending downward. The exception was ransomware, which the company predicted was on pace for its second-biggest year with the resurgence of "big game" hunting. Now, with ransomware attacks against major casino operations dominating the headlines, and these same hackers also hitting large companies in sectors including in manufacturing, retail, and technology, the report seems eerily prescient.

https://www.securityweek.com/key-learnings-from-big-game-ransomware-campaigns/

*Click above link to read more.*

Back to top

## Oldham Council facing 10,000 cyber attacks a day, report says

A council is to spend £682,000 on computer upgrades after bosses said they were fighting off 10,000 cyber attacks a day.

https://www.bbc.com/news/uk-england-manchester-67228223

*Click above link to read more.*

Back to top

---

## AI and a tale of two tech earnings reports, company leaders unaware of (or unprepared for) cybersecurity risks

Tuesday was a big day not just for publicly traded tech companies, but also to show the importance of AI technology. Two of the biggest tech companies—Microsoft and Google parent Alphabet—reported their quarterly earnings after markets closed. Both beat investors' overall forecasts: Alphabet's revenues were up 11% year over year, and Microsoft's by 13% along the same lines of comparison.

https://www.forbes.com/sites/meganpoinski/2023/10/26/ai-and-a-tale-of-two-tech-earnings-reports-company-leaders-unaware-of-or-unprepared-for-cybersecurity-risks/?sh=3793386d2b5c

*Click above link to read more.*

Back to top

---

## Beware of fake Google Chrome update that installs malware

Cybersecurity is constantly changing and facing new challenges.  One of them is the fake Chrome update malware, which has been around for several years and is still active.

https://cybersecuritynews.com/beware-of-fake-google-chrome-update/

*Click above link to read more.*

Back to top

---

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