
**Theme of the month: SIM Swapping**
**(look for the ✪)**

Challenge yourself with our **SIM Swapping Quiz**!

## What you can do to improve your mobile device security:

| All Users | Technical Users | Business Owners |
|---|---|---|
| Avoid using public wi-fi to connect to the internet, as it can leave you vulnerable to attacks. Only connect to trusted networks that are password-protected or use mobile data. | Ensure that any attempts to tamper with mobile device operating systems are blocked, logged, and actioned immediately. | Ensure that employees are aware of and understand the policies associated with using their work devices for personal use. |

**Check out Cyber Safety for Mobile Workers Info Sheet to learn more about mobile device security.**

This past week's stories:

**Toronto school board reports ransomware attack on test environment**
**Microsoft employees' cybersecurity contributions will factor into their pay**
**Cryptojacking campaign targets misconfigured Kubernetes clusters**
**After cybersecurity event, Seattle Public libraries slowly coming back online**
**Microsoft, Google offer cybersecurity resources for rural hospitals**
**Hospitals cyber attack impacts 800 operations**
**EU cybersecurity label should not discriminate against Big Tech, European groups say**
**Cybersecurity burnout due to stress, fatigue and mental health is costing hundreds of millions in lost productivity**
**✪ Cryptomathic is Belgium's digital wallet mobile app security provider**
**Four tips for ensuring a strong cybersecurity workforce**

## Hackers abuse Windows search functionality to deploy malware
## Chinese automaker partnership bolsters electric vehicle cybersecurity

---

### Toronto school board reports ransomware attack on test environment

Hackers attempted to attack a technology testing environment used by the Toronto District School Board (TDSB) with ransomware, officials said Wednesday.

https://therecord.media/toronto-school-board-ransomware-attack

*Click above link to read more.*

Back to top

---

### Microsoft employees' cybersecurity contributions will factor into their pay

Microsoft will evaluate its employees' cybersecurity contributions in reviews that will factor into their compensation, Brad Smith, the company's vice chair and president, said ahead of a Thursday U.S. House committee hearing on the software maker's security practices.

https://www.cnbc.com/2024/06/13/microsoft-employees-cybersecurity-work-will-factor-into-their-pay.html

*Click above link to read more.*

Back to top

---

### Cryptojacking campaign targets misconfigured Kubernetes clusters

Cybersecurity researchers have warned of an ongoing cryptojacking campaign targeting misconfigured Kubernetes clusters to mine Dero cryptocurrency.

https://thehackernews.com/2024/06/cryptojacking-campaign-targets.html

*Click above link to read more.*

Back to top

---

### After cybersecurity event, Seattle Public libraries slowly coming back online

Seattle Public Library reached an important milestone Thursday as it recovers from last months cybersecurity event.

https://www.kiro7.com/news/local/after-cybersecurity-event-seattle-public-libraries-slowly-coming-back-online/T74OA4UQNNH3RJ4KINNOFVHJ5Q/

*Click above link to read more.*

Back to top

---

### Microsoft, Google offer cybersecurity resources for rural hospitals

Microsoft and Google have pledged to help rural hospitals prevent cyberattacks by offering free or discounted cybersecurity resources. The commitment from the tech giants is part of a White House-led initiative to bolster cybersecurity in the healthcare sector.

https://healthitsecurity.com/news/microsoft-google-offer-cybersecurity-resources-for-rural-hospitals

*Click above link to read more.*

Back to top

---

### Hospitals cyber attack impacts 800 operations

More than 800 planned operations and 700 outpatient appointments were rearranged in the first week after a cyber attack hit London hospitals, it has been revealed.

https://www.bbc.com/news/articles/cd11v377eywo

*Click above link to read more.*

Back to top

---

### EU cybersecurity label should not discriminate against Big Tech, European groups say

A proposed cybersecurity certification scheme (EUCS) for cloud services should not discriminate against Amazon (AMZN.O), opens new tab, Alphabet's (GOOGL.O), opens new tab Google and Microsoft (MSFT.O), opens new tab, 26 industry groups across Europe warned on Monday.

https://www.reuters.com/technology/cybersecurity/eu-cybersecurity-label-should-not-discriminate-against-big-tech-european-groups-2024-06-17/

*Click above link to read more.*

Back to top

---

## Cybersecurity burnout due to stress, fatigue and mental health is costing hundreds of millions in lost productivity

It's no secret that cybersecurity professionals are facing the squeeze, with many being hospitalized in the aftermath of ransomware attacks.

https://www.techradar.com/pro/cybersecurity-burnout-due-to-stress-fatigue-and-mental-health-is-costing-hundreds-of-millions-in-lost-productivity

*Click above link to read more.*

Back to top

---

## Cryptomathic is Belgium's digital wallet mobile app security provider

Tech from Cryptomathic has been deployed in Belgium's digital identity wallet, one of the first to go live in the new era of digital ID. A press release says the Federal Government of Belgium has launched MyGov.be, a single app providing access to a wide range of digital public services, information and official documents, in line with the European Digital Identity Framework Regulation, eIDAS 2.0.

https://www.biometricupdate.com/202406/cryptomathic-is-belgiums-digital-wallet-mobile-app-security-provider

*Click above link to read more.*

Back to top

---

## Four tips for ensuring a strong cybersecurity workforce

A common lament among CISOs and other executives is that the lack of skilled security talent hinders their ability to effectively defend against an increasingly hostile threat landscape. Further, those leaders struggle with upskilling existing staff.

https://www.forbes.com/sites/forbestechcouncil/2024/06/14/four-tips-for-ensuring-a-strong-cybersecurity-workforce/

*Click above link to read more.*

Back to top

---

## Hackers abuse Windows search functionality to deploy malware

Hackers use Windows Search's vulnerability to penetrate different layers and rooms in the client's systems and execute unauthorized code by using bugs in the search functionality itself.

https://cybersecuritynews.com/hackers-abuse-windows-search/

*Click above link to read more.*

Back to top

---

### Chinese automaker partnership bolsters electric vehicle cybersecurity

Chinese automaker BYD is leveraging cybersecurity software from Karamba Security to protect its connected vehicles.

https://www.iotworldtoday.com/transportation-logistics/chinese-automaker-partnership-bolsters-electric-vehicle-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.


Security News Digest
Cybersecurity and Digital Trust Branch
OCIO
Office of the
Chief Information Officer