October 25, 2022

Register for SECURITY DAY!

Challenge yourself with our Cyber Security Awareness Month Quiz!

Take the Cyber Security Awareness Month Challenges!

This past week's stories:

- **Health records may have been accessed in cyber security breach**
- **University of Guelph says "limited information" accessed during Sept. cyber attack**
- **MPs warned to change email passwords after cyber attack on Canadian government**
- **Hive ransomware hackers begin leaking data stolen from Tata Power energy company**
- **CISA Warns of Daixin Team hackers targeting health organizations with ransomware**
- **Hackers exploit critical VMware flaw to drop ransomware, miners**
- **Cybersecurity labor shortage grows worse in U.S. and worldwide: Report**
- **Half of staff might quit after a cyber attack, report says**
- **Cyber security event targeted by hackers**
- **Ed Sheeran: Hacker who stole singer's unreleased music is jailed**
- **As Russia wages disinfo war, Ukraine's cyber chief calls for global anti-fake news fight**
- **EnergyAustralia hacked after data stolen from Medibank, Optus**
- **Singapore sales portal hacked, leaving two million customers exposed to cyber fraud**

Health records may have been accessed in cyber security breach

Owen Sound Family Health Organization announced this month in a letter to patients that it learned of a data breach in July which exposed patients' personal information.

It notified police and the Office of the Information and Privacy Commissioner of Ontario, which is investigating.

https://www.owensoundsuntimes.com/news/local-news/health-records-may-have-been-accessed-in-cyber-security-breach

Click above link to read more.

Back to top

University of Guelph says "limited information" accessed during Sept. cyber attack

The University of Guelph has released new details about its Sept. 11 cyber attack, saying "limited information has been compromised."

No further details have been released about the type of data that was accessed.

The school said in a media release it is "conducting a thorough review of the affected data on a priority basis."

https://kitchener.ctvnews.ca/university-of-guelph-says-limited-information-accessed-during-sept-cyber-attack-1.6118086

Click above link to read more.

Back to top

MPs warned to change email passwords after cyber attack on Canadian government

Members of Parliament have been asked to change their email passwords and some internet-based services on Parliament Hill have been restricted after what's being described as a "cyber incident."

The threat to the government's information technology infrastructure was identified last Wednesday, said Amelie Crosson, the manager of communications in the Office of the Speaker.

https://www.thestar.com/politics/federal/2022/10/18/mps-warned-to-change-email-passwords-after-cyber-attack-on-canadian-government.html

Click above link to read more.

Back to top

Hive ransomware hackers begin leaking data stolen from Tata Power energy company

The Hive ransomware-as-a-service (RaaS) group has claimed responsibility for a cyber attack against Tata Power that was disclosed by the company less than two weeks ago.

The incident is said to have occurred on October 3, 2022. The threat actor has also been observed leaking stolen data exfiltrated prior to encrypting the network as part of its double extortion scheme.

https://thehackernews.com/2022/10/hive-ransomware-hackers-begin-leaking.html

Click above link to read more.

Back to top

CISA Warns of Daixin Team hackers targeting health organizations with ransomware

U.S. cybersecurity and intelligence agencies have published a joint advisory warning of attacks perpetrated by a cybercrime gang known as the Daixin Team primarily targeting the healthcare sector in the country.

"The Daixin Team is a ransomware and data extortion group that has targeted the HPH Sector with ransomware and data extortion operations since at least June 2022," the agencies said.

https://thehackernews.com/2022/10/cisa-warns-of-daixin-team-hackers.html

Click above link to read more.

Back to top

Hackers exploit critical VMware flaw to drop ransomware, miners

Security researchers observed malicious campaigns leveraging a critical vulnerability in VMware Workspace One Access to deliver various malware, including the RAR1Ransom tool that locks files in password-protected archives.

The issue leveraged in the attacks is CVE-2022-22954, a remote code execution bug triggered through server-side template injection.

https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-vmware-flaw-to-drop-ransomware-miners/

Click above link to read more.

Back to top

Cybersecurity labor shortage grows worse in U.S. and worldwide: Report

Despite the training and hiring of hundreds of thousands of new workers, the cybersecurity industry's labor shortage is only growing worse, not better, according to a new report.

The International Information System Security Certification Consortium, known as ISC2, reports that a survey of 11,799 cybersecurity professionals shows that the total global workforce for security personnel rose over the past year to 4.6 million people, a jump of 11.1 percent.

https://www.crn.com/news/security/report-cybersecurity-labor-shortage-grows-worse-in-u-s-and-worldwide

Click above link to read more.

Back to top

Half of staff might quit after a cyber attack, report says

Experiencing a cyber attack can be so discombobulating for ordinary employees that over half of office workers say they would reconsider working for a company that had recently fallen victim to an incident, with only a third saying they would be unphased. This is according to a study of office workers, C-suite executives and business leaders, and chief information security officers (CISOs) produced for security stack management specialist Encore.

Of further concern was a disconnect highlighted in the report data between how many business leaders and CISOs knew they had experienced an incident in the past 12 months (57%), and how many regular office workers believed they had experienced one (39%).

https://www.computerweekly.com/news/252526433/Half-of-staff-might-quit-after-a-cyber-attack-report-says

Click above link to read more.

Back to top

Cyber security event targeted by hackers

Suspected hackers have attempted to steal credit card details during an online cyber security seminar.

The seminar run by the Australian Institute of Company Directors had to be cancelled after posts to its online platform asked users to click links where credit card details were requested.

https://www.begadistrictnews.com.au/story/7954746/cyber-security-event-targeted-by-hackers/

Click above link to read more.

Back to top

Ed Sheeran: Hacker who stole singer's unreleased music is jailed

A hacker who stole two unreleased songs from Ed Sheeran and sold them on the dark web has been jailed for 18 months.

Adrian Kwiatkowski traded the music by Sheeran and 12 songs by rapper Lil Uzi Vert in exchange for cryptocurrency.

https://www.bbc.com/news/technology-63348753

Click above link to read more.

Back to top

As Russia wages disinfo war, Ukraine's cyber chief calls for global anti-fake news fight

As a hybrid offline and online war wages on in Ukraine, Viktor Zhora, who leads the country's cybersecurity agency, has had a front-row seat of it all.

Zhora is the deputy chairman and chief digital transformation officer at Ukraine's state service of special communication and information protection.

https://www.theregister.com/2022/10/22/ukraine_cybersecurity_chief_mwise/

Click above link to read more.

Back to top

EnergyAustralia hacked after data stolen from Medibank, Optus

EnergyAustralia has become the latest company to fall victim to a cyber attack, with hundreds of people impacted.

The electricity company said the breach involved unauthorised access of the online platform My Account, exposing the data of 323 residential and small business customers.

https://www.news.com.au/technology/online/hacking/energy-australia-hacked-after-data-stolen-from-medibank-optus/news-story/7fd668f480e8ab0b8c227fd772ed530f

Click above link to read more.

Back to top

Singapore sales portal hacked, leaving two million customers exposed to cyber fraud

Carousell, a buy-and-sell digital platform used by around four in ten Singaporeans, has been hacked, leaving almost two million customer details exposed. Furthermore, it's unclear just how long the data was accessible.

The breach was disclosed by the company to a local media news site TODAY on October 21. According to the news outlet, Carousell attributed the breach to the previous week, leaving 1.95 million customers' mobile phone numbers and email addresses exposed.

https://cybernews.com/news/singapore-sales-portal-hacked-leaving-two-million-customers-exposed-to-cyber-fraud/

Click above link to read more.

Back to top

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca