February 22, 2022

Challenge yourself with our Love Security quiz!

This past week's stories:

- **Concordia to co-lead new $160-million Canadian cybersecurity innovation network**
- **New funding helps advance Canadian leadership in cybersecurity**
- **Cybersecurity stocks provide a haven during a technology selloff**
- **Cyber insurance premiums soar for energy companies**
- **New Linux privilege escalation flaw uncovered in Snap package manager**
- **Organisations deprioritized cybersecurity during supply chain crisis despite rise in attacks, Kaspersky reveals**
- **Red Cross cyberattacks the work of nation-state actors**
- **Cyberattacks on oil surge as hackers target commodities**
- **Cyber attack: Sansad TV YouTube channel back after blackout**
- **Expeditors' operations hit following cyber attack**
- **Younger generation faces increased cyber security risks**
- **OpenSea users lose $2 million worth of NFTs in phishing attack**

Concordia to co-lead new $160-million Canadian cybersecurity innovation network

Every day, a deluge of cyberattacks target the cyber infrastructure of corporations, governmental agencies, and individuals. The damage can be even more potent when the attack involves critical infrastructure components.

To address the cybersecurity challenges in terms of R&D, innovation, and training, and to help institutions and businesses across the country manage cyber threats, the Government of Canada announced $76.4 million in funding over four years to the National Cybersecurity Consortium.

https://www.concordia.ca/news/stories/2022/02/17/concordia-to-co-lead-new-160-million-canadian-cybersecurity-innovation-network.html

Click above link to read more.

Back to top

New funding helps advance Canadian leadership in cybersecurity

On February 17, the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry, announced that the National Cybersecurity Consortium (NCC) will receive up to $80 million to lead the Cyber Security Innovation Network.

The University of Waterloo is one of five founding members of the NCC working with public and private sectors to lead world-class cybersecurity innovation and talent development. Cybersecurity and privacy are emerging as critical challenges our society needs to tackle in the coming decade to secure our future.

https://uwaterloo.ca/news/new-funding-helps-advance-canadian-leadership-cybersecurity

Click above link to read more.

Back to top

Cybersecurity stocks provide a haven during a technology selloff

Many of the tech sector's lockdown winners have long surrendered their outsize pandemic gains, but cybersecurity stocks aren't among them.

The resilience in Zscaler Inc., Crowdstrike Holdings Inc. and Fortinet Inc. is a display of bright growth prospects for these firms amid simmering geopolitical tensions, more employees adopting hybrid working models and the ongoing digital shift, analysts say. Zscaler has fallen 25% from a November peak, but remains up more than 300% over the past two years, while Crowdstrike and Fortinet are still up more than 160%.

https://www.bnnbloomberg.ca/cybersecurity-stocks-provide-a-haven-during-technology-selloff-1.1724976

Click above link to read more.

Back to top

Cyber insurance premiums soar for energy companies

Insurance companies are "very concerned" with the potential for attacks on critical U.S. infrastructure and are raising insurance premiums for energy companies by double and triple digits, according to Michael Gaudet, U.S. energy, power and utility leader within Marsh's financial and professional liability practice. The company is an insurance broker that works with underwriters who provide utilities with cyber insurance.

https://www.cybersecuritydive.com/news/utility-cyber-insurance-premiums/619089/

Click above link to read more.

Back to top

New Linux privilege escalation flaw uncovered in Snap package manager

Multiple security vulnerabilities have been disclosed in Canonical's Snap software packaging and deployment system, the most critical of which can be exploited to escalate privilege to gain root privileges.

Snaps are self-contained application packages that are designed to work on operating systems that use the Linux kernel and can be installed using a tool called snapd.

https://thehackernews.com/2022/02/new-linux-privilege-escalation-flaw.html

Click above link to read more.

Back to top

Organisations deprioritised cybersecurity during supply chain crisis despite rise in attacks, Kaspersky reveals

A new Kaspersky report – produced in association with leading freight transport insurer TT Club – has revealed that despite a rise in cyberattacks during the supply chain crisis, 16% of UK businesses deprioritised cybersecurity last year amid the pandemic, port closures, HGV driver shortages and other challenges associated with Brexit.

Cybercriminals have become ever more sophisticated at exploiting organisational silos, security gaps caused by remote working and the supply chain crisis, to undermine the safety and security of critical systems. So much so that companies across the UK and Benelux reported a 30% rise in the number of cyberattacks they faced during last year, compared to previous years.

https://www.hellenicshippingnews.com/organisations-deprioritised-cybersecurity-during-supply-chain-crisis-despite-rise-in-attacks-kaspersky-reveals/

Click above link to read more.

Back to top

Red Cross cyber attack the work of nation-state actors

A cyber attack on the systems of the International Committee of the Red Cross (ICRC), which resulted in the data of more than 515,000 vulnerable people being compromised, appears to have been the work of an undisclosed nation-state actor, the organisation has revealed.

The attack came to light on 18 January 2022, when the ICRC disclosed that it had been compromised. The compromised data relates to the organisation’s Restoring Family Links programme, which assists people separated from their families due to conflict, migration or disaster, reunites missing persons with their families, and helps people in detention.

https://www.computerweekly.com/news/252513537/Red-Cross-cyber-attack-the-work-of-nation-state-actors

Click above link to read more.

Back to top

Cyberattacks on oil surge as hackers target commodities

Cyberattacks on energy and commodities infrastructure are on the rise, with 35 major incidents recorded over the last five-year period, according to the latest update of the S&P Global Platts Oil Security Sentinel™ research project.

Oil assets and infrastructure emerged as the biggest targets for hackers and cyberattacks since 2017, accounting for a third of all incidents over the period. Electricity networks were the next most vulnerable, making up a quarter of all incidents, data collected by Platts showed.

https://www.spglobal.com/platts/en/market-insights/latest-news/oil/021822-cyberattacks-on-oil-surge-as-hackers-target-commodities

Click above link to read more.

Back to top

Cyber attack: Sansad TV YouTube channel back after blackout

The YouTube channel of Sansad TV, which is operated by Parliament and live-streams House proceedings, came under attack by hackers early Tuesday, after which it was blocked by the social media platform for about 15 hours. It was restored around 6.30 pm.

Sansad TV said in a statement issued earlier in the day that it was “compromised by scamsters”. According to official sources, the channel was initially attacked by hackers soon after midnight and restored around 3 am. It soon came under attack again, they said, leading to the channel being blocked by YouTube for most of the day.

https://indianexpress.com/article/india/cyber-attack-sansad-tv-youtube-channel-back-blackout-7775245/

Click above link to read more.

Back to top

Expeditors’ operations hit following cyber attack

Global operations at Expeditors are facing disruption after the US forwarder became the latest supply chain firm to suffer a cyber attack.

On Sunday, the company told customers that it had suffered a targeted cyber attack. The forwarder said that it was working with global cyber-security experts to resolve the situation but added that systems may be unavailable as it assesses and stabilises its systems and backup procedures are implemented.

https://www.aircargonews.net/freight-forwarder/expeditors-operations-hit-following-cyber-attack/

Click above link to read more.

Back to top

Younger generation faces increased cyber security risk

Internet addiction, lack of awareness of digital citizenship and ineffective parental control have led to increased cybersecurity risks facing the younger generation.

Communications and Multimedia Minister Tan Sri Annuar Musa said this was based on the Executive Report of the Findings of the Cyber Security Awareness Study Among School Students and Parents 2021/2022 (Laporan Eksekutif Dapatan Kajian Tanda Aras Tahap Kesedaran Keselamatan Siber Dalam Kalangan Murid Sekolah dan Ibu Bapa.

https://www.nst.com.my/news/nation/2022/02/773686/younger-generation-faces-increased-cybersecurity-risks

Click above link to read more.

Back to top

OpenSea users lose $2 million worth of NFTs in phishing attack

The non-fungible token (NFT) marketplace OpenSea is investigating a phishing attack that left 17 of its users without more than 250 NFTs worth around $2 million.

NFTs represent data stored on a blockchain, Ethereum in this case, that declares ownership of digital files, typically media files of artwork.

https://www.bleepingcomputer.com/news/security/opensea-users-lose-2-million-worth-of-nfts-in-phishing-attack/

Click above link to read more.

Back to top


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer