April 19, 2022

Challenge yourself with our Spring Cleaning quiz!

This past week's stories:

- $200K public relations aid for N.L. cyberattack didn't result in transparency: expert
- Rideau Hall cyberbreach was 'sophisticated' incident, internal documents show
- Ransomware attacks ease after peaks in early 2021 – report
- Thales, the first group to join The Campus Cyber in Paris, La Défense, and lend its expertise to the service of this new ecosystem
- New malware could be 'exceptionally dangerous' for US energy, analysis says
- Focus more on cybersecurity, banks told
- Fox News data leak exposed 13 million records including personally identifiable information and celebrity details
- 'Cyber literacy at the top levels of companies should be a given'
- How cybercriminals are creating malicious hyperlinks that bypass security software
- Neurodiverse candidates find niche in remote cybersecurity jobs
- Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites
- Cyber security breach unearthed in the army, inquiry ordered

---

$200K public relations aid for N.L. cyberattack didn't result in transparency: expert

The Newfoundland and Labrador government signed a $200,000 contract with a public relations company that specializes in crisis management during a cyberattack last fall that took out much of the province's health-care network.

The contract between National Public Relations and the Newfoundland and Labrador Centre for Health Information is dated Oct. 30 and is for strategic counsel on internal and external communications, media monitoring and other public relations help.

https://atlantic.ctvnews.ca/200k-public-relations-aid-for-n-l-cyberattack-didn-t-result-in-transparency-expert-1.5862407

Click above link to read more.

Back to top

Rideau Hall cyberbreach was 'sophisticated' incident, internal documents show

Newly disclosed documents reveal the breach of an internal computer network at Rideau Hall was described to senior government officials as a "sophisticated cyber incident" in the days before the public was told of the security lapse.

Internal government emails, obtained by The Canadian Press through the Access to Information Act, also say officials were "unable to confirm the full extent of the information that was accessed."

https://globalnews.ca/news/8765558/rideau-hall-cyberbreach-2021-incident/

Click above link to read more.

Back to top

Ransomware attacks ease after peaks in early 2021 – report

In its latest report, Corvus Insurance pointed to signs of improvement in overall cybercrime activity at the near end of 2021.

The report involves insights from data scientists, underwriters, cybersecurity professionals and claims managers on what is happening and what is to come for the cyber risk landscape after the recent peaks in the early quarters of 2021.

https://www.insurancebusinessmag.com/ca/news/cyber/ransomware-attacks-ease-after-peaks-in-early-2021--report-402609.aspx

Click above link to read more.

Back to top

Thales, the first group to join The Campus Cyber in Paris, La Défense, and lend its expertise to the service of this new ecosystem

April 2022 saw the arrival of about sixty Thales employees, engineers, consultants, and cybersecurity project managers on the Cyber Campus. To mark the occasion, Patrice Caine underlined its role as a catalyst for international cyber excellence in a context of globalization and a sharp rise in threats.

The Thales teams will soon be joined by teams coming from public and private structures specializing in this field. Thales provides Cyber Campus members with its collaborative platform in the cloud, the first approved "Restricted Diffusion", Cybels Hub, including Cryptobox (document management and sharing) and Citadel Team (screen sharing).

https://financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/thales-the-first-group-to-join-the-campus-cyber-in-paris-la-defense-and-lend-its-expertise-to-the-service-of-this-new-ecosystem

Click above link to read more.

Back to top

New malware could be 'exceptionally dangerous' for US energy, analysis says

Several U.S. government agencies issued an alert warning of the discovery of cyber tools that can allow hackers to overtake computer systems at energy facilities.

Using the tools, a hacker would be able to get into a company's security network and "disrupt critical devices or functions." The alert was released by the Energy and Homeland Security Departments, the FBI and the National Security Agency.

https://abcnews4.com/news/nation-world/us-warns-of-cyber-tools-that-could-target-energy-facilities-cybersecurity-malware-fbi-homeland-security-nsa-fbi-russian-hack-incontroller-mandiant

Click above link to read more.

Back to top

Focus more on cybersecurity, banks told

In view of an increasing number of bank account hacking cases resulting in huge financial losses, the Hyderabad City Police along with the Reserve Bank of India conducted a meeting with representatives of banks here on Thursday.

About 51 urban cooperative banks and other banks participated in the meeting, wherein the police briefed them on cyber security measures to be implemented to prevent such cases.

https://telanganatoday.com/focus-more-on-cybersecurity-banks-told

Click above link to read more.

Back to top

Fox News data leak exposed 13 million records including personally identifiable information and celebrity details

A Fox News data leak reportedly exposed at least 13 million records, including personally identifiable information and content management data via a cloud storage configuration error.

According to a Website Planet research team led by Jeremiah Fowler, the 58 GB trove was left open without a username or password, allowing anybody with an internet connection to access it.

https://www.cpomagazine.com/cyber-security/fox-news-data-leak-exposed-13-million-records-including-personally-identifiable-information-and-celebrity-details/

Click above link to read more.

Back to top

‘Cyber literacy at the top levels of companies should be a given’

One of the most common warnings that I’ve heard from cybersecurity experts over the years is that malicious actors and cybercriminals only have to get it right once, while cybersecurity practitioners have to get it right every single time in order to protect companies and systems.

This requires an immense amount of buy-in from every level of an organisation in order to build up a strong cyber resilience and a good security posture.

https://www.siliconrepublic.com/enterprise/cyber-literacy-board-level-huawei

Click above link to read more.

Back to top

How cybercriminals are creating malicious hyperlinks that bypass security software

Finding ways to sneak past cybersecurity defenses is always uppermost on the minds of cybercriminals. The more easily they can thwart your security tools, the greater the chances that their attacks will be successful. A report released Thursday by email security provider Avanan reveals how a coding practice called Quoted-printable is being used in phishing emails to present malicious links as legitimate.

Hackers who create phishing emails often will turn to certain deceptive coding techniques. As one example, they may encode a letter not by using the actual letter but by using its ASCII code, such as using &#65 to represent the letter a. Your email program doesn’t reveal the ASCII character but rather converts the code into its actual letter.

https://www.techrepublic.com/article/how-cybercriminals-creating-malicious-hyperlinks-bypass-security-software/

Click above link to read more.

Back to top

Neurodiverse candidates find niche in remote cybersecurity jobs

Cat Contillo remembers how uncomfortable she felt during an office internship a few years ago because of reactions to her masculine outfits and her inability to understand sarcasm.

Diagnosed as autistic at 18 years old, she was no fan of the office setting. Now 33, she is thriving in a cybersecurity job, working from home in upstate New York for Huntress Labs Inc., a threat-detection software business that is based in Ellicott City, Md., and has a fully remote workforce.

https://www.wsj.com/articles/neurodiverse-candidates-find-niche-in-remote-cybersecurity-jobs-11649842380

Click above link to read more.

Back to top

Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites

Months before Russian armored vehicles rolled into Ukraine on Feb. 24, companies monitoring satellite networks noticed an uptick in activity.

Hackers were trying to penetrate Ukraine's communications satellite infrastructure, including networks that relay commands to Ukrainian military drones. Meanwhile, Earth observation satellites detected intensifying GPS interference in the region.

https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/

Click above link to read more.

Back to top

Cyber security breach unearthed in the army, inquiry ordered

The intelligence agencies including the Military Intelligence have unearthed a cyber security breach with a report of a foreign origin number traced in a group where the members included the Indian Army's serving personnel.

A source confirmed to TNIE that a cyber security breach has happened.

"Yes, a breach has been traced wherein a Pakistan Intelligence Operative (PIO) has been traced in a WhatsApp group which also included our serving personnel." Any number which is part of the group is termed the PIO.

https://www.newindianexpress.com/nation/2022/apr/19/cyber-security-breach-unearthed-in-the-army-inquiry-ordered-2443952.html

Click above link to read more.

Back to top