May 10, 2022

Challenge yourself with our Cyber Security Superhero quiz!

This past week's stories:

Newfoundland and Labrador cyberattack cost nears $16 million, no details whether ransom paid

Costs related to the cyberattack on the province's health-care system in October are approaching $16 million.

Health Minister Dr. John Haggie told reporters Wednesday just over $5 million of that nearly $16 million covers credit monitoring for people whose data was accessed. He said a small amount covers consulting and legal fees, but the bulk of it was for staff overtime in the four regional health authorities.

https://www.saltwire.com/atlantic-canada/news/newfoundland-and-labrador-cyberattack-cost-nears-16-million-no-details-whether-ransom-paid-100725568/

Click above link to read more.

Back to top

Internal data breach discovered at IKEA Canada, impacts 95,000 Canadians

Ikea Canada has revealed an internal data breach impacting 95,000 Canadians, Global News has learned.

One of those impacted, Calgarian Arthur Gallant, said he received an email from the retailer last week, advising him his privacy had been breached.

https://globalnews.ca/news/8812708/ikea-canada-internal-data-breach-95000-records/amp/

Click above link to read more.

Back to top

Protect and defend with new Camosun cybersecurity program

“The way business is being done has changed dramatically in recent years. More and more, employees are connecting over VPNs, working from home, and are far more global than they have ever been before,” says Ian Cameron, Instructor, Electronics and Computer Engineering. “As all companies rely on computer systems it is vital that businesses invest in cybersecurity experts to protect them against both cyber-attacks and data theft."

To cater to this demand, Camosun is offering two new programs in Cybersecurity and Network technology this fall. These programs have a practical career-oriented approach, giving students the knowledge and hands-on experience they need to be able to install, repair, secure and maintain computers, servers, and computer networks.

https://camosun.ca/news/protect-defend-new-camosun-cybersecurity-program

Click above link to read more.

Back to top

What does the conflict in Ukraine mean for UK cyber security?

The recent discovery in Ukraine of ‘wiper’ malware, a denial-of-service assault which paralyses websites by bombarding them with information requests, has accelerated a rush by businesses to bolster their defences should it spread.

Microsoft has also detected a new malware named ‘FoxBlade’ which has focused on stealing health, insurance and transportation data from Ukrainian essential services.

https://www.businessleader.co.uk/what-does-the-conflict-in-ukraine-mean-for-uk-cyber-security/

Click above link to read more.

Back to top

Screen-sharing scams on the rise, watchdog warns

They ask their victim to share the screen and enable remote access - which hands over control of their device and, potentially their bank account.

About 2,100 cases have been reported to the FCA since July 2020.

More than £25m was stolen in the 15 months from January 2021.

https://www.bbc.com/news/technology-61323399

Click above link to read more.

Back to top

Chinese hackers caught stealing intellectual property from multinational companies

An elusive and sophisticated cyberespionage campaign orchestrated by the China-backed Winnti group has managed to fly under the radar since at least 2019.

Dubbed "Operation CuckooBees" by Israeli cybersecurity company Cybereason, the massive intellectual property theft operation enabled the threat actor to exfiltrate hundreds of gigabytes of information.

https://thehackernews.com/2022/05/chinese-hackers-caught-stealing.html

Click above link to read more.

Back to top

Apple, Google and Microsoft back new passwordless sign-in standard

Apple, Google and Microsoft have backed a password less sign-in standard created by the Fast Identity Online [FIDO] Alliance and the World Wide Web Consortium.

A statement issued by the Alliance claimed such a standard would make the Internet more secure and usable.

https://itwire.com/business-it-news/security/apple,-google-and-microsoft-back-new-passwordless-sign-in-standard.html

Click above link to read more.

Back to top

Security “mindshift” set needed to protect organisations

Manual investigation, third parties, customers and law enforcement are catching far more cybersecurity threats more than software solutions, says Chris Fisher, director of security engineering APJ at cybersecurity company Vectra.

That’s despite cybersecurity being a focus of IT spending – in the second half of 2021, Gartner reported that nearly three quarters of ANZ CIOs had indicated that cybersecurity would be their biggest area of investment in 2022.

https://www.itnews.com.au/feature/security-mindset-shift-needed-to-protect-organisations-579730

Click above link to read more.

Back to top

Microsoft launches cybersecurity services to help clients fight off ransomware and other attacks

Microsoft's security business is growing faster than any of its main products, and now the company is adding heft to its offerings with three new services designed to help organizations spot and respond to cybersecurity incidents.

Microsoft is among the leaders in cloud software and infrastructure, which means its technology is already the backbone for many businesses of all sizes. That puts the company in position to not only make security software available to its client base, but also offer consulting-oriented services in a market where demand far exceeds supply.

https://www.cnbc.com/2022/05/09/microsoft-launches-security-experts-services-boosting-security-spend.html

Click above link to read more.

Back to top

Cybersecurity skills gap contributed to 80% of breaches according to new Fortinet report

Fortinet®, a global leader in broad, integrated, and automated cybersecurity solutions, today released its 2022 Cybersecurity Skills Gap Report. The new global report reveals that the cybersecurity skills shortage continues to have multiple challenges and repercussions for organizations, including the occurrence of security breaches and subsequently loss of money. As a result, the skills gap remains a top concern for C-level executives and is increasingly becoming a board-level priority. The report also suggests ways the skills gap can be addressed, such as through training and certifications to increase employees' education.

Sandra Wheatley, SVP Marketing, Threat Intelligence and Influencer Communications at Fortinet says, "According to the Fortinet report released today, the skills gap isn't just a talent shortage challenge, but it's also severely impacting business, making it a top concern for executive leaders worldwide. Through Fortinet's Training Advancement Agenda (TAA) and Training Institute programs, we are committed to tackling the challenges revealed in the report through various initiatives, including programs focused on cybersecurity certifications and recruiting more women into cyber. As part of this commitment, Fortinet has pledged to train 1 million professionals to increase cyber skills and awareness and make a dent in the skills gap by 2026."

https://www.zawya.com/en/press-release/research-and-studies/cybersecurity-skills-gap-contributed-to-80-of-breaches-according-to-new-fortinet-report-f3flyogl

Click above link to read more.

Back to top

Nokia launches groundbreaking cybersecurity-focused testing lab in the U.S.

Nokia today announced the launch of its Advanced Security Testing and Research (ASTaR) lab, located in Dallas, Texas. It is the first end-to-end 5G testing lab in the U.S. focused solely on cybersecurity. ASTaR's holistic approach to researching and testing secure solutions and potential network threat mitigations will go beyond looking at individual network elements and also focus on the larger context of network use and abuse scenarios.

In the 5G era, the nature and scale of information networks are evolving, as are the nature and scale of security threats. More avenues of attack are open to hackers, state actors and corporate espionage due to many types of interworking endpoints, extensive use of open-source software and large-scale use of 5G in a variety of industries. Network security resilience must be maintained as the attack scenarios are constantly changing.

https://www.globenewswire.com/news-release/2022/05/09/2438665/0/en/Nokia-launches-groundbreaking-cybersecurity-focused-testing-lab-in-the-U-S.html

Click above link to read more.

Back to top

Cyber-security chiefs warn of malicious app risk

A new report by the UK's National Cyber Security Centre (NCSC) has warned of the threats posed by malicious apps.

While most people will be familiar with apps downloaded on to smartphones, devices from smart TVs to smart speakers now also have them.

https://www.bbc.com/news/technology-61323395

Click above link to read more.

Back to top