May 17, 2022

Challenge yourself with our Cyber Security Superhero quiz!

This past week's stories:

- Sensitive personal data among thousands of files exposed in Elgin cybersecurity incident: Gonyou
- Canada wants G7 nations to have a quick-reaction cybersecurity team after Ukraine attack
- AHS cybersecurity head warns of 'large number of attacks' using health body's name
- CSE cybersecurity centre's new boss says job has been 'dizzying' experience of responding to multiple major cyber incidents
- Long before N.L. cyberattack, report flagged flaws in system
- Canada directs military to take more 'assertive' stance in cyberspace
- UK govt releases free tool to check for email cybersecurity risks
- How a pentester's attempt to be 'as realistic as possible' alarmed cybersecurity firms
- Europe agrees to adopt new NIS2 directive aimed at hardening cybersecurity
- Police officers for cyber security course in India as on-site training resumes
- UK sets out nuclear cybersecurity strategy
- Pro-Russia hackers tried to disrupt the Eurovision Song Contest
- Purdue University Northwest to offer new degree in cybersecurity

---

Sensitive personal data among thousands of files exposed in Elgin cybersecurity incident: Gonyou

A cybersecurity incident that left Elgin County's website and email services offline through the month of April resulted in thousands of county files, some containing highly sensitive personal information, being posted to the dark web, Elgin's chief administrative officer confirmed on Monday.

Officials in the county south of London, Ont., have kept mum about the incident over the last several weeks, but now say that roughly 26,000 files and the information of about 300 people were compromised after an "unauthorized third party" gained access to its network.

https://globalnews.ca/news/8838788/personal-data-files-elgin-cybersecurity-exposure/

Click above link to read more.

Back to top

Canada wants G7 nations to have a quick-reaction cybersecurity team after Ukraine attack

Innovation Minister Francois-Philippe Champagne is pressing G7 countries to establish a quick-reaction group on cybersecurity to help build up resilience to attacks following the invasion of Ukraine.

Champagne suggested to a meeting of G7 digital ministers in Germany that they pool expertise to fend off attacks and protect crucial information-technology infrastructure.

https://globalnews.ca/news/8834047/canada-g7-cybersecurity-ukraine/

Click above link to read more.

Back to top

AHS cybersecurity head warns of 'large number of attacks' using health body's name

Cybercriminals looking to target Albertans are increasingly using Alberta Health Service's name to do so, says the organization's top information security officer.

The attacks — typically in the form of a phishing text or email — started before the pandemic, prompting the health body to issue a warning to Albertans.

https://www.cbc.ca/news/canada/calgary/ahs-cyber-security-phishing-1.6447085

Click above link to read more.

Back to top

CSE cybersecurity centre's new boss says job has been 'dizzying' experience of responding to multiple major cyber incidents

The new head of Canada’s cybersecurity centre says his first months on the job have been a “dizzying” experience of responding to one major incident after another, including a cyberattack from a hostile state against a federal government department in recent months.

“The last eight months have been somewhat a dizzying experience of a number of cyber incidents and managing all these cyber incidents,” Sami Khoury, who was named head of the Communications Security Establishment’s (CSE) Canadian Centre for Cyber Security last August, told the audience at the Cyber UK conference Wednesday.

https://nationalpost.com/news/politics/cse-cybersecurity-centres-new-boss-says-job-has-been-dizzying-experience-of-responding-to-multiple-major-cyber-incidents

Click above link to read more.

Back to top

Long before N.L. cyberattack, report flagged flaws in system

Israeli cyberexperts who reviewed information security arrangements at Newfoundland and Labrador's largest health authority confirmed "numerous vulnerabilities, security concerns and compliance issues" that needed to be addressed within its network.

The details are in a business plan prepared for Eastern Health in September 2020 and recently obtained by CBC/Radio-Canada.

https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cybersecurity-eastern-health-report-1.6447807

Click above link to read more.

Back to top

Canada directs military to take more ‘assertive’ stance in cyberspace

The Canadian government has directed its military to take a more “assertive” stance in cyberspace in anticipation of electronic warfare becoming a more central component in conflict, documents obtained by Global News suggest.

A “cyber playbook” prepared by the Canadian Armed Forces and the Department of National Defence comes as Ottawa pushes for international rules and norms around cyber espionage and warfare.

https://globalnews.ca/news/8827050/canada-military-more-assertive-cyberspace/

Click above link to read more.

Back to top

UK govt releases free tool to check for email cybersecurity risks

The United Kingdom's National Cyber Security Centre (NCSC) has announced a new email security check service to help organizations identify vulnerabilities that could allow attackers to spoof emails or lead to email privacy breaches.

The government agency, which leads the UK's cyber security mission, says the Email Security Check tool requires no sign-ups or personal details.

https://www.bleepingcomputer.com/news/security/uk-govt-releases-free-tool-to-check-for-email-cybersecurity-risks/

Click above link to read more.

Back to top

How a pentester’s attempt to be ‘as realistic as possible’ alarmed cybersecurity firms

Over the last several weeks, researchers at multiple security firms have been scratching their heads trying to figure out who was targeting German companies with what appeared to be a supply chain attack.

On Wednesday, they got their answer: An intern at a threat intelligence firm that was simulating “realistic threat actors” for its clients.

https://therecord.media/how-a-pentesters-attempt-to-be-as-realistic-as-possible-alarmed-cybersecurity-firms/

Click above link to read more.

Back to top

Europe agrees to adopt new NIS2 directive aimed at hardening cybersecurity

The European Parliament announced a "provisional agreement" aimed at improving cybersecurity and resilience of both public and private sector entities in the European Union.

The revised directive, called "NIS2" (short for network and information systems), is expected to replace the existing legislation on cybersecurity that was established in July 2016.

https://thehackernews.com/2022/05/europe-agrees-to-adopt-new-nis2.html

Click above link to read more.

Back to top

Police officers for cyber security course in India as on-site training resumes

Beginning May 2022, the High Commission of India in Guyana will once again be accepting applications for on-site training in India, under the Indian Technical and Economic Cooperation (ITEC) programme, after a stoppage due to Covid-19 pandemic according to release yesterday from the High Commission. The stoppage was due to the COVID-19 pandemic and the attendant protocols.

On Thursday, May 12, the first batch of five officers from Guyana Police Force under ITEC 2022 departed for the Centre for Development of Advanced Computing (C-DAC) for a 4-week specialised training course from 16 May 2022 to 10 June 2022, in Cyber Security & Malware Analytics, and Reverse Engineering to improve the capabilities of Guyana Police Force to fight cybercrime. The team comprises of 5 Guyana Police Force Officers and marks the beginning of training of Guyana Police Force Officers in India under ITEC.

https://www.stabroeknews.com/2022/05/14/news/guyana/police-officers-for-cyber-security-course-in-india-as-on-site-training-resumes/

Click above link to read more.

Back to top

UK sets out nuclear cybersecurity strategy

The UK government has laid out its cybersecurity plans for the country’s civil nuclear sector, focused on more testing, security by design and improved collaboration.

The UK boasts the oldest civil nuclear power program globally, which began in 1956 with the opening of the Calder Hall power station.

https://www.infosecurity-magazine.com/news/uk-sets-out-nuclear-cybersecurity/

Click above link to read more.

Back to top

Pro-Russia hackers tried to disrupt the Eurovision Song Contest

Pro-Russia hackers tried – but failed – to disrupt the Eurovision Song Contest this weekend in an effort to mar a runaway victory by Ukrainian band Kalush Orchestra.

It's the latest in a spate of recent hacks aimed at undermining or embarrassing geopolitical adversaries under a media spotlight.

https://www.washingtonpost.com/politics/2022/05/16/pro-russia-hackers-tried-disrupt-eurovision-song-contest/

Click above link to read more.

Back to top

Purdue University Northwest to offer new degree in cybersecurity

Purdue University Northwest will be offering a Bachelor of Science degree in cybersecurity, pending approval by the Indiana Commission for Higher Education.

PNW students currently enrolled in the computer information technology degree program with a concentration in cybersecurity will be eligible to transition to the new cybersecurity degree.

https://www.nwitimes.com/news/local/education/purdue-university-northwest-to-offer-new-degree-in-cybersecurity/article_1b282c9d-61a1-5712-9268-0fda6a78df04.html

Click above link to read more.

Back to top

OCIOSecurity@gov.bc.ca