August 16, 2022

Challenge yourself with our Summer Social Media Security quiz!

This past week's stories:

- Government announces support for Canada's preparedness against cyberattacks
- Cybersecurity company CyberCatch partners with Ridge Canada
- Canadian recreational vehicle maker BRP, Ontario Cannabis Store dealing with cyber attacks
- Waterloo public board confirms student database also accessed in cyberattack
- Cisco confirms data breach, hacked files leaked
- Germany to mandate minimum security standards for web browsers in government
- Back to school means more cyber concerns
- Cybersecurity has never been more unstable than it is now
- Security firm finds cyber vulnerabilities at Indian online insurance aggregator
- Russia's Shuckworm cyber group launching ongoing attacks on Ukraine
- NHS IT suppliers held to ransom by hackers
- Sophos reveals latest ransomware trend impacting organizations
- Callback phishing attacks see massive 625% growth since Q1 2021

Government announces support for Canada's preparedness against cyberattacks

From electronic espionage to ransomware, the threats to Canadians from malicious cyber activity – including cyberattacks – are greater than ever. In the future this will also include the quantum threat, whereby quantum computers will be able to easily hack through much of the existing encryption that we rely on today. Given the significant risk that it poses, the Government of Canada is redoubling efforts to protect Canadians from the quantum threat.

The Minister of Public Safety, the Honourable Marco Mendicino, today announced federal support for Canada's cyber defenses. Quantum-Safe Canada will receive $675,000 for their project Laying the Foundations for a Quantum-Safe Canada, which raises awareness and preparedness of the quantum threat. This funding is made available under the Cyber Security Cooperation Program.

https://www.miragenews.com/government-announces-support-for-canadas-837652/

Click above link to read more.

Back to top

Cybersecurity company CyberCatch partners with Ridge Canada

Cybersecurity software-as-a-service company CyberCatch has entered into a strategic partnership with Canadian cyber-focused managing general agent Ridge Canada Cyber Solutions (RCCS).

Through the partnership, the two companies will help Canada's small and medium organizations (SMOs) secure proper cyber insurance and meet security standards.

https://www.insurancebusinessmag.com/ca/news/cyber/cybersecurity-company-cybercatch-partners-with-ridge-canada-416498.aspx

Click above link to read more.

Back to top

Canadian recreational vehicle maker BRP, Ontario Cannabis Store dealing with cyber attacks

One of the country's biggest manufacturers of recreational vehicles is still struggling with the aftereffects of a cyber attack.

Quebec-based BRP Inc., better known as Bombardier Recreational Products, said Monday it had been hit by "malicious cybersecurity activity."

https://www.itworldcanada.com/article/canadian-recreational-vehicle-maker-brp-ontario-cannabis-store-dealing-with-cyber-attacks/497252

Click above link to read more.

Back to top

Waterloo public board confirms student database also accessed in cyberattack

The Waterloo Region District School Board (WRDSB) says an investigation into a cyberattack in July has found that databases containing the personal information of some students was accessed along with current and past employees.

In July, the school board said it was notified of unauthorized access to its IT system. The Ontario Provincial Police launched an investigation, alongside the school board's own internal team, and the school board released the findings late Friday afternoon.

https://www.cbc.ca/news/canada/kitchener-waterloo/wrdsb-cyber-1.6550129

Click above link to read more.

Back to top

Cisco confirms data breach, hacked files leaked

Cisco has confirmed a breach of its network, where the attacker used voice phishing to convince an employee to accept a malicious multifactor authentication (MFA) push. The breach resulted in cyberattackers gaining access to the company's virtual private network (VPN) and the theft of an unspecified number of files from its network, the company stated on Aug. 10.

The attacker compromised a Cisco employee's personal Google account, which gave them access to the worker's business credentials through the synchronized password store in Google Chrome. To bypass the MFA protecting access to Cisco's corporate VPN, the attacker attempted voice phishing, or vishing, and repeatedly pushed MFA authentication requests to the employee's phone. Eventually, the worker either inadvertently, or through alert fatigue, accepted the push request, giving the attacker access to Cisco's network.

https://www.darkreading.com/attacks-breaches/cisco-confirms-data-breach-hacked-files-leaked

Click above link to read more.

Back to top

Germany to mandate minimum security standards for web browsers in government

Germany is mandating the use of secure, modern web browsers across government networks with a proposal for minimum standards currently open to consultation.

The Federal Office for Information Security (BSI) released a draft set of minimum standards in July. The agency hopes that the standards will bolster governmental cyber-resilience and better protect sensitive data. Leading browsers incorporate multiple features that block or mitigate a variety of common web-based attacks.

https://portswigger.net/daily-swig/germany-to-mandate-minimum-security-standards-for-web-browsers-in-government

Click above link to read more.

Back to top

Back to school means more cyber concerns

As the 2022-2023 school year looms, so do ongoing cyber threats directly targeting schools, universities and school district administrations.

In 2021, there were an average of over 1500 attacks on education and research organization per week and these numbers are expected to continue to rise through 2022.

https://securityboulevard.com/2022/08/back-to-school-means-more-cyber-concerns/

Click above link to read more.

Back to top

Cybersecurity has never been more unstable than it is now

The world of cybersecurity is nearing a point of no return, with the number of data breaches, password leaks, and cyber attacks on businesses reaching a level that has never been seen before. Currently, there is a cyberattack on a company every 39 seconds, with each successful attack costing businesses millions of dollars.

While cybersecurity has been an issue for decades, this problem is only growing, with recent years seeing a dramatic rise in the number of cases recorded. In 2021 alone, 30,000 websites were hacked every single day, with there being an average of 50% more attacks per week than in 2020.

https://www.hackread.com/cybersecurity-never-been-unstable-than-it-is-now/

Click above link to read more.

Back to top

Security firm finds cyber vulnerabilities at Indian online insurance aggregator

Last month, a cybersecurity startup told a major Indian online insurance brokerage that it had found critical vulnerabilities in the company's Internet-facing network that could expose sensitive personal and financial data of at least 11 million customers to malicious hackers.

The startup followed the standard playbook for ethical hackers, giving Policybazaar, the insurance aggregator, time to fix the flaws and notify the authorities. It didn't ask for permission in advance to test Policybazaar's system, but said it deemed itself justified, in part because it had employees who were customers.

https://www.thebharatexpressnews.com/security-firm-finds-cyber-vulnerabilities-at-indian-online-insurance-aggregator/

Click above link to read more.

Back to top

Russia's Shuckworm cyber group launching ongoing attacks on Ukraine

The Russia-linked cyber group Shuckworm is continuing to target Ukrainian organizations with infostealing malware. According to Symantec's Threat Hunter Team, part of Broadcom Software, much of the current activity is an extension of attacks that were reported by the Computer Emergency Response Team of Ukraine (CERT-UA) in July.
Shuckworm (aka, Gamaredon, Armageddon) is an eight-year-old cyber crime group that focuses almost exclusively on Ukraine, Symantec said.

https://www.techrepublic.com/article/russias-shuckworm-cyber-group-launching-ongoing-attacks-on-ukraine/

Click above link to read more.

Back to top

NHS IT suppliers held to ransom by hackers

A cyber-attack on a major IT provider of the NHS has been confirmed as a ransomware attack.

Advanced, which provides digital services like patient check-in and NHS 111, says it may take three to four weeks to fully recover.

Ransomware hackers take control of IT systems, steal data and demand a payment from victims to recover.

https://www.bbc.com/news/technology-62506039

Click above link to read more.

Back to top

Sophos reveals latest ransomware trend impacting organizations

Sophos, a global expert in next-generation cybersecurity, has announced in the Sophos X-Ops Active Adversary whitepaper, 'Multiple Attackers: A Clear and Present Danger', that Hive, LockBit and BlackCat, three prominent ransomware gangs, consecutively attacked the same network.

The first two attacks took place within two hours, and the third attack took place two weeks later. Each ransomware gang left its own ransom demand, and some of the files were triple encrypted.

https://securitybrief.com.au/story/sophos-reveals-latest-ransomware-trend-impacting-orgs

Click above link to read more.

Back to top

Callback phishing attacks see massive 625% growth since Q1 2021

Hackers are increasingly moving towards hybrid forms of phishing attacks that combine email and voice social engineering calls as a way to breach corporate networks for ransomware and data extortion attacks.

According to Agari's Q2 2022 cyber-intelligence report, phishing volumes have only increased by 6% compared to Q1 2022. However, the use of 'hybrid vishing' is seeing a massive 625% growth.

https://www.bleepingcomputer.com/news/security/callback-phishing-attacks-see-massive-625-percent-growth-since-q1-2021/

Click above link to read more.

Back to top

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

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

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

OCIOSecurity@gov.bc.ca