June 27, 2023

Challenge yourself with our Spear Phishing quiz!

This past week's stories:

- **Calgary-based Suncor Energy says it suffered a cyber security incident**
- **Cybersecurity breaches more than double among Canadian businesses: report**
- **Are you being 'botfished'? A cybersecurity expert's advice for how to spot an AI dating scam**
- **Canadian infosec pros wish they'd spent more time on security when migrating to cloud: Survey**
- **University of Windsor partners with California cybersecurity firm**

Cybercrime group 'Muddled Libra' targets BPO sector with advanced social engineering

Chinese state-backed hackers accidentally infected a European hospital with malware

SMS phishers harvested phone numbers, shipment data from UPS tracking tool

Don't make these mistakes when investing in cryptocurrency

U.S. Cybersecurity Agency adds 6 flaws to known exploited vulnerabilities catalog

Over 33% of employees are clicking malicious links – phishing report

Microsoft fell prey to a DDoS attack by Anonymous Sudan

UK hacker busted in Spain gets 5 years over Twitter hack and more

NSA: BlackLotus bootkit patching won't prevent compromise

Calgary-based Suncor Energy says it suffered a cyber security incident

A Canadian oil company is the latest to report it experienced a cyber security incident.

https://calgary.ctvnews.ca/calgary-based-suncor-energy-says-it-suffered-a-cyber-security-incident-1.6455796

Click above link to read more.

Back to top

Cybersecurity breaches more than double among Canadian businesses: report

A new report has found that the number of successful cybersecurity breaches has more than doubled for Canadian businesses in the past year, despite a downward trend in cyberattacks overall.

https://www.ctvnews.ca/business/cybersecurity-breaches-more-than-double-among-canadian-businesses-report-1.6445282

Click above link to read more.

Back to top

Are you being 'botfished'? A cybersecurity expert's advice for how to spot an AI dating scam

Does your cat like lasagna?

It’s a question one cybersecurity expert recommends people ask if they think they’re speaking with a bot on a dating app or website.

https://bc.ctvnews.ca/are-you-being-botfished-a-cybersecurity-expert-s-advice-for-how-to-spot-an-ai-dating-scam-1.6448793

Click above link to read more.

Back to top

Canadian infosec pros wish they’d spent more time on security when migrating to cloud: Survey

Despite storing more than half their data to the cloud, Canadian organizations only allocate 34 per cent of their cybersecurity budgets to cloud security, according to a new survey from Telus.

https://www.itworldcanada.com/article/canadian-infosec-pros-wish-theyd-spent-more-time-on-security-when-migrating-to-cloud-survey/541516

Click above link to read more.

Back to top

University of Windsor partners with California cybersecurity firm

The University of Windsor's SHIELD Automotive Cybersecurity Centre of Excellence is partnering with California-based Keysight Technologies Inc. to provide engineering students with access to the company's advanced cybersecurity training platform technology.

https://windsorstar.com/news/local-news/university-of-windsor-partners-with-california-cybersecurity-firm

Click above link to read more.

Back to top

Cybercrime group 'Muddled Libra' targets BPO sector with advanced social engineering

A threat actor known as Muddled Libra is targeting the business process outsourcing (BPO) industry with persistent attacks that leverage advanced social engineering ploys to gain initial access.

https://thehackernews.com/2023/06/cybercrime-group-muddled-libra-targets.html

Click above link to read more.

Back to top

Chinese state-backed hackers accidentally infected a European hospital with malware

A cybersecurity incident at a European hospital highlights the uncontrolled spread of malware by hackers connected to the Chinese military, researchers have found.

https://therecord.media/china-apt-infected-european-hospital

Click above link to read more.

Back to top

Don’t make these mistakes when investing in cryptocurrency

People are becoming increasingly interested in cryptocurrencies as they find them a great way to build their wealth. However, as seen over the years, digital currencies are marked by high volatility, causing investors to make mistakes they regret. The good news is that there is a lot of information available on how to safely trade Bitcoin and other cryptocurrencies, as well as what mistakes to avoid.

https://www.eyeonannapolis.net/2023/06/dont-make-these-mistakes-when-investing-in-cryptocurrency/

Click above link to read more.

Back to top

SMS phishers harvested phone numbers, shipment data from UPS tracking tool

The United Parcel Service (UPS) says fraudsters have been harvesting phone numbers and other information from its online shipment tracking tool in Canada to send highly targeted SMS phishing (a.k.a. “smishing”) messages that spoofed UPS and other top brands. The missives addressed recipients by name, included details about recent orders, and warned that those orders wouldn’t be shipped unless the customer paid an added delivery fee.

https://krebsonsecurity.com/2023/06/sms-phishers-harvested-phone-numbers-shipment-data-from-ups-tracking-tool/?

Click above link to read more.

Back to top

U.S. Cybersecurity Agency adds 6 flaws to known exploited vulnerabilities catalog

The U.S. Cybersecurity and Infrastructure Security Agency has added a batch of six flaws to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

https://thehackernews.com/2023/06/us-cybersecurity-agency-adds-6-flaws-to.html

Click above link to read more.

Back to top

Over 33% of employees are clicking malicious links – phishing report

Several data breaches were reported this year that were typically due to ransomware attacks, phishing campaigns, and other social engineering techniques, resulting in millions of dollars losing organizations worldwide.

https://cybersecuritynews.com/clicking-malicious-links/

Click above link to read more.

Back to top

Microsoft fell prey to a DDoS attack by Anonymous Sudan

For several weeks now, cybercriminals have been highly active, orchestrating attacks against some of the world's largest organizations. Recently, Microsoft was at the receiving end of a Distributed Denial-of-Service (DDoS) attack by Storm-1359, also known as Anonymous Sudan, that resulted in service disruptions.

https://techwireasia.com/2023/06/microsoft-ddos-attack-caused-by-anonymous-sudan/

Click above link to read more.

Back to top

UK hacker busted in Spain gets 5 years over Twitter hack and more

Some hacks become so notorious that they acquire a definite article, even if the word THE ends up attached to a very general technical term.

https://nakedsecurity.sophos.com/2023/06/26/uk-hacker-busted-in-spain-gets-5-years-over-twitter-hack-and-more/?utm_source=dlvr.it&utm_medium=linkedin

Click above link to read more.

Back to top

NSA: BlackLotus bootkit patching won't prevent compromise

The US National Security Agency (NSA) is urging systems administrators to go beyond patching in order to protect Windows 10 and 11 machines from the BlackLotus bootkit malware.

https://www.darkreading.com/vulnerabilities-threats/nsa-blacklotus-bootkit-patchings-prevent-compromise

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.