August 9, 2022

Challenge yourself with our Summer Social Media Security quiz!

This past week's stories:

- **Okanagan man hit in online friendship scam**
- **Ski-Doo maker BRP hit by cyberattack, temporarily suspends operations**
- **Which industries in Canada are most in need of cyber insurance?**

Watson College undergraduate contributes to cybersecurity research

Hospitals have low level of accountability for connected device breaches

The 11 most-prevalent malware strains of 2021 fuel cybercrime

Hackers exploit Twitter vulnerability to exposes 5.4 million accounts

Deepfakes pose a growing danger, new research says

Twilio hacked by phishing campaign targeting internet companies

NHS 111 software outage confirmed as cyber-attack

Email marketing firm hacked to steal crypto-focused mailing lists

Ransomware, email compromise are top security threats, but deepfakes increase

---

Okanagan man hit in online friendship scam

A Kelowna, B.C., man was snared in an online scheme that traded false friendship for funds, RCMP said.

The man contacted police July 7, explaining that he'd made friends with who he believed to be a woman living in Ontario then, later, an unnamed foreign country.

https://globalnews.ca/news/9037921/okanagan-man-online-friendship-scam/

Click above link to read more.

Back to top

Ski-Doo maker BRP hit by cyberattack, temporarily suspends operations

BRP Inc said it has been hit by a cyberattack and has suspended operations temporarily.

The maker of Sea-Doo watercraft and Ski-Doo snowmobiles said that it determined Monday that it was “the target of malicious cybersecurity activity” and took immediate measures to contain the situation. Its shares fell 2 per cent to $93.49 in morning trading on the Toronto Stock Exchange.

https://www.theglobeandmail.com/business/article-ski-doo-maker-brp-hit-by-cyberattack-temporarily-suspends-operations/

Click above link to read more.

Back to top

Which industries in Canada are most in need of cyber insurance?

Amid the rising threat of cyberattacks, an increasing number of businesses in the country are turning to cyber insurance to manage their risks, a recent study conducted by the Canadian Internet Registration Authority (CIRA) has revealed.

The organization polled a national representative sample of 500 IT specialists between July and August last year and found that the majority, or 59%, of respondents said their companies have taken out cyber coverage as part of their cyber defence measures. Half of these businesses have purchased cyber cover as part of their business insurance policies, while the other half bought a separate “cybersecurity-specific” policy.

https://www.insurancebusinessmag.com/ca/news/cyber/which-industries-in-canada-are-most-in-need-of-cyber-insurance-416019.aspx

Click above link to read more.

Back to top

Watson College undergraduate contributes to cybersecurity research

Identity thieves are always trying to find new ways to hack into our personal data, but new research — assisted by a Binghamton University undergraduate — is trying to cut off at least one method of attack.

Through a Research Experience for Undergraduates program last summer at Carnegie Mellon University, Jennifer Seibert contributed to an investigation into cache attacks, which target the data stored in a computer or mobile device to increase internet speed. The research, led by Assistant Professor Nathan Beckmann and PhD candidate Brian Schwedock from CMU's School of Computer Science, was a best paper nominee at the International Symposium on Computer Architecture in June.

https://www.binghamton.edu/news/story/3769/watson-college-undergraduate-contributes-to-cybersecurity-research

Click above link to read more.

Back to top

Hospitals have low level of accountability for connected device breaches

Hospitals are not taking basic security actions and have low levels of accountability regarding cyberattacks, ransomware and data theft stemming from breached medical devices, new research suggests.

Over half of respondents in a survey of healthcare executives from cybersecurity firm Cynerio and research group Ponemon Institute reported that senior management did not require assurances that medical or internet-connected device risks were properly monitored or managed.

https://www.cybersecuritydive.com/news/hospitals-medical-device-cyberattacks-cynerio-ponemon/628948/

Click above link to read more.

Back to top

The 11 most-prevalent malware strains of 2021 fuel cybercrime

Malware strains are like a bad habit — the type that can evolve into something far worse. The typical lifespan of the most-prevalent malware strains found in 2021 was at least five years, according to a joint advisory from the Cybersecurity and Infrastructure Security Agency and the Australian Cyber Security Centre.

Malware code bases are commonly reused and transformed into variant strains to add new capabilities and dodge threat hunters. Among the top 11 malware strains of 2021, malicious actors

have used eight for at least five years and circulated two strains for more than a decade, the agencies said.

https://www.cybersecuritydive.com/news/top-malware-strains-CISA/628993/

Click above link to read more.

Back to top

Hackers exploit Twitter vulnerability to exposes 5.4 million accounts

Twitter on Friday revealed that a now-patched zero-day bug was used to link phone numbers and emails to user accounts on the social media platform.

"As a result of the vulnerability, if someone submitted an email address or phone number to Twitter's systems, Twitter's systems would tell the person what Twitter account the submitted email addresses or phone number was associated with, if any," the company said in an advisory.

https://thehackernews.com/2022/08/hackers-exploit-twitter-vulnerability.html

Click above link to read more.

Back to top

Deepfakes pose a growing danger, new research says

Deepfakes are increasingly being used in cyberattacks, a new report said, as the threat of the technology moves from hypothetical harms to real ones.

Reports of attacks using the face- and voice-altering technology jumped 13% last year, according to VMware's annual Global Incident Response Threat Report, which was released Monday. In addition, 66% of the cybersecurity professionals surveyed for this year's report said they had spotted one in the past year.

https://www.cnet.com/tech/services-and-software/deepfakes-pose-a-growing-danger-new-research-says/

Click above link to read more.

Back to top

Twilio hacked by phishing campaign targeting internet companies

Communications giant Twilio has confirmed hackers accessed customer data after successfully tricking employees into handing over their corporate login credentials.

The San Francisco-based company, which allows users to build voice and SMS capabilities — such as two-factor authentication (2FA) — into applications, said in a blog post published Monday that it became aware that someone gained "unauthorized access" to information related to some Twilio customer accounts on August 4.

https://techcrunch.com/2022/08/08/twilio-breach-customer-data/

Click above link to read more.

Back to top

NHS 111 software outage confirmed as cyber-attack

A software outage affecting the NHS 111 service was caused by a cyber-attack, it has been confirmed.

Advanced, a firm providing digital services for NHS 111, said the attack was spotted at 07:00 BST on Thursday.

https://www.bbc.com/news/uk-wales-62442127

Click above link to read more.

Back to top

Email marketing firm hacked to steal crypto-focused mailing lists

Email marketing firm Klaviyo disclosed a data breach after threat actors gained access to internal systems and downloaded marketing lists for cryptocurrency-related customers.

Klaviyo says the breach occurred on August 3rd after hackers stole an employee's login credentials in a phishing attack. These login credentials were then used to access the employee's account and internal Klaviyo support tools.

https://www.bleepingcomputer.com/news/security/email-marketing-firm-hacked-to-steal-crypto-focused-mailing-lists/

Click above link to read more.

Back to top

Ransomware, email compromise are top security threats, but deepfakes increase

While ransomware and business email compromise (BEC) are leading causes of security incidents for businesses, geopolitics and deepfakes are playing an increasing role, according to reports from two leading cybersecurity companies.

VMware's 2022 Global Incident Threat Response Report shows a steady rise in extortionary ransomware attacks and BEC, alongside fresh jumps in deepfakes and zero-day exploits.

https://www.csoonline.com/article/3669476/ransomware-email-compromise-are-top-security-threats-but-deepfakes-increase.html

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer