March 22, 2022

Challenge yourself with our Fraud Prevention quiz!

This past week's stories:

- 'They may already be happening': Canada at higher risk of cyberattacks from Russian hackers after siding with Ukraine
- Guernsey cyber-security warning for islanders and businesses
- Investigation launched after National Research Council is hit by 'cyber incident'
- The HP cybersecurity acquisition made for a world of increasing malware threats
- TransUnion cyber attack – hackers demand R225 million ransom
- Rehab Group victim of cyber attack 'on some of its systems'
- Where is Russia's cyberwar? Researchers decipher its strategy
- How TrueCaller built a billion-dollar caller ID data empire in India
- Greek postal service reports cyber attack
- Cyber attack targeted 21 natural gas producers on the eve of the Russian invasion of Ukraine
- How to prepare now for a possible Russian cyber attack
- White House warns of new intel on Russia mulling cyberattack 'options' against US
- Australian watchdog sues Facebook-owner Meta over scam advertisements
- Microsoft investigating claims of hacked source code repositories

---

'They may already be happening': Canada at higher risk of cyberattacks from Russian hackers after siding with Ukraine

For Farshad Abasi, Russian cyberattacks against Canada are inevitable given Prime Minister Justin Trudeau's decision to be an active participant in sanctioning Russia over its invasion of Ukraine.

“They may already be happening and we don’t even know it,” said Abasi, chief security officer at Forward Security, a Vancouver-based cybersecurity company. “If they haven’t already, they will, and we need to be prepared.”

https://financialpost.com/news/economy/they-may-already-be-happening-canada-at-higher-risk-of-cyberattacks-from-russian-hackers-after-siding-with-ukraine

Click above link to read more.

Back to top

Guernsey cyber-security warning for islanders and businesses

There has been a rise in cyber-attacks since the war in Ukraine began, according to the States of Guernsey and a cyber-security firm.

The States said: "We have seen a noticeable increase in the number of phishing emails since the war began."

The Channel Islands see more than 10 million cyber attacks every month, according to research by Guernsey firm Black Arrow Cyber Consulting.

https://www.bbc.com/news/world-europe-guernsey-60763398

Click above link to read more.

Back to top

Investigation launched after National Research Council is hit by 'cyber incident'

An investigation is underway after the National Research Council reported being hit Friday by what it's calling a "cyber incident."

"Due to a cyber incident, some applications on our website were taken offline and may be unavailable. We are working to bring applications back online as soon as possible," says a banner on the agency's website.

https://www.cbc.ca/news/politics/nrc-cyber-incident-1.6392358

Click above link to read more.

Back to top

The HP cybersecurity acquisition made for a world of increasing malware threats

When Bromium made its debut on the inaugural CNBC Disruptor 50 list in 2013, its pitch was that fighting malware with traditional fire is a losing battle and the only way to wage and win a new war against cyber attackers is to isolate viruses rather than try to keep them out entirely.

“Disruption occurs when customers in a mature market are presented with a fundamentally different, and far more effective, way to solve a problem. Ultimately, the new markets and value networks created by

disruptive products overtake and displace existing market," Bromium CEO Gaurav Banga told CNBC at the time. "As the market embraces this innovative approach, we are able to move towards our ultimate objective — to restore trust in computing."

https://www.cnbc.com/2022/03/17/the-hp-cybersecurity-deal-made-for-a-world-of-malware-threats.html

Click above link to read more.

Back to top

TransUnion cyber attack – hackers demand R225 million ransom

Credit reporting agency TransUnion South Africa is currently in an ongoing battle with a hacker group demanding a $15 million (R225 million) ransom over four terabytes of compromised data.

The hacker group, going by the name N4aughtysecTU, which claims to be based in Brazil, is alleging it breached TransUnion South Africa and accessed 54 million personal records of South Africans.

https://businesstech.co.za/news/cloud-hosting/569658/transunion-cyber-attack-hackers-demand-r225-million-ransom/

Click above link to read more.

Back to top

Rehab Group victim of cyber attack 'on some of its systems'

The Rehab Group has said there is no evidence data has been accessed following a cyber attack on Wednesday.

The charity, which provides services and supports for people with disabilities, said it has informed the Data Protection Commissioner of the attack.

It said the attack targeted "some of its systems".

There has also been "no disruption to services and we will work to ensure this remains the case," the charity said.

https://www.irishexaminer.com/news/arid-40830644.html

Click above link to read more.

Back to top

Where is Russia's cyberwar? Researchers decipher its strategy

When Russia invaded Ukraine last month, many security analysts were expecting a level of cyberwar never seen before, because of Russia's history of such aggression.

There has been low-level activity. Cyberattacks were under way in Ukraine even before Russian forces invaded on 24 February. Hours prior, a type of malware called a wiper circulated on Ukrainian government computing systems, corrupting data. Earlier that week, a massive distributed denial of service

(DDoS) attack, widely attributed to Russia, had flooded Ukrainian bank websites with traffic, making them inaccessible.

https://www.nature.com/articles/d41586-022-00753-9

Click above link to read more.

Back to top

How TrueCaller built a billion-dollar caller ID data empire in India

A weeks-long investigation by The Caravan shows the Swedish company has used India's lack of a comprehensive legal framework surrounding data protection to advance its business.

In October 2021, I called a journalist based in Pakistan, who did not know me. Surprisingly, they greeted me by my name when they received the call. When asked how they identified me, they sent a screenshot of a notification received from the Truecaller app on their phone. The notification had my name, my former employer's name, my designation at my former company, the state I was based in, and the name of my mobile operator. The journalist told me that they had recently installed the Truecaller app from the Google Play Store on an Android phone.

https://restofworld.org/2022/how-truecaller-built-a-billion-dollar-id-data-empire-in-india/

Click above link to read more.

Back to top

Greek postal service reports cyber attack

Hellenic Post (ELTA) said Monday it had isolated all its data center services as a preventive measure following a cyber-attack late Sunday.

It is not known if the hackers managed to gain access to the targeted networks.

https://www.ekathimerini.com/news/1180274/greek-postal-service-reports-cyber-attack/

Click above link to read more.

Back to top

Cyber attack targeted 21 natural gas producers on the eve of the Russian invasion of Ukraine

A new report says that hackers executed a major cyber attack campaign against multiple natural gas producers in the United States ahead of Russia's invasion of Ukraine.

Bloomberg News reported that the cyber attacks targeted at least 21 companies involved in the production, exportation, and distribution of liquified natural gas.

https://www.cpomagazine.com/cyber-security/cyber-attack-targeted-21-natural-gas-producers-on-the-eve-of-the-russian-invasion-of-ukraine/

Click above link to read more.

Back to top

How to prepare now for a possible Russian cyber attack

Good cyber hygiene is always important. But right now, with the threat of Russian cyber-attacks on American computer systems, it's critical.

One of the best ways to protect yourself, your devices, and all the information stored on them is to make sure the software for your operating system, browsers, and apps are all up to date.

https://komonews.com/news/consumer/how-to-prepare-now-for-a-possible-russian-cyber-attack

Click above link to read more.

Back to top

White House warns of new intel on Russia mulling cyberattack 'options' against US

President Joe Biden today warned of "evolving intelligence" that indicates Russia may be getting ready to wage cyberattacks against US interests, calling this "a critical moment" and urging organizations to harden their cybersecurity defenses "immediately" if they have not already done so.

"There is now evolving intelligence that Russia may be exploring options for potential cyberattacks," Biden said in a statement today, noting that the new warning reiterates the threat previously issued by the administration of possible Russian cyber aggression against the US for imposing stiff economic sanctions on Russia.

https://www.darkreading.com/risk/white-house-warns-of-new-intel-on-russia-mulling-cyberattack-options-against-us

Click above link to read more.

Back to top

Australian watchdog sues Facebook-owner Meta over scam advertisements

Australia's competition watchdog filed a lawsuit against Facebook owner Meta Platforms (FB.O) on Friday, alleging the social media giant failed to prevent scammers using its platform to promote fake ads featuring well-known people.

The advertisements, which endorsed investment in cryptocurrency or money-making schemes, could have misled Facebook users into believing they were promoted by famous Australians, the Australian Competition & Consumer Commission (ACCC) said.

https://www.reuters.com/technology/australia-watchdog-sues-facebook-owner-meta-over-false-cryptocurrency-ads-2022-03-17/

Click above link to read more.

Back to top

Microsoft investigating claims of hacked source code repositories

Microsoft says they are investigating claims that the Lapsus$ data extortion hacking group breached their internal Azure DevOps source code repositories and stolen data.

Unlike many extortion groups we read about today, Lapsus$ does not deploy ransomware on their victim's devices.

https://www.bleepingcomputer.com/news/security/microsoft-investigating-claims-of-hacked-source-code-repositories/

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