August 15, 2023

Challenge yourself with our Cryptocons Quiz!

This past week's stories:

- **It's time for companies to double down on cybersecurity measures as ransomware attacks rise, say experts**
- **Cyber attack exposes banking information of thousands of Albertans**
- **LifeLabs to pay out at least $4.9 million in proposed class-action settlement over data breach**
- **DARPA launches two-year competition to build AI-powered cyber defenses**
- **Hundreds of executives are falling for Microsoft 365 phishing attacks: Report**
- **How fame-seeking teenagers hacked some of the world's biggest targets**
- **How safe is my data after a hack or leak?**
- **Intel 'Downfall': Severe flaw in billions of CPUs leaks passwords and much more**
- **Charming Kitten targets Iranian dissidents with advanced cyber attacks**
- **For U.S. officials, the world's largest hacking conference isn't all fun and games**
- **When cybersecurity becomes 'HR's problem'**
- **Hackers attacking power generator systems to infect with ransomware**
- **Ford cars Wi-Fi vulnerability let attackers execute remote code**

It's time for companies to double down on cybersecurity measures as ransomware attacks rise, say experts

Experts say it's time for Canadian companies and organizations to double down on cybersecurity measures as they're seeing an increase in ransomware attacks and other cyber incidents across the country.

https://www.cbc.ca/news/canada/calgary/cybersecurity-measures-ransomware-attacks-1.6934486

Click above link to read more.

Back to top

Cyber attack exposes banking information of thousands of Albertans

Records of more than 1.4 million Albertans were the target of a cyber attack on a government service provider last month, the Alberta Dental Services Corporation said this week.

https://calgary.ctvnews.ca/cyber-attack-exposes-banking-information-of-thousands-of-albertans-1.6515469

Click above link to read more.

Back to top

LifeLabs to pay out at least $4.9 million in proposed class-action settlement over data breach

Millions of Canadians affected by the LifeLabs cyberattack nearly four years ago could be eligible for a small piece — anywhere from $50 to $150 — of a proposed class-action settlement worth at least $4.9 million if approved by a court.

https://www.ctvnews.ca/business/lifelabs-to-pay-out-at-least-4-9-million-in-proposed-class-action-settlement-over-data-breach-1.6514511

Click above link to read more.

Back to top

DARPA launches two-year competition to build AI-powered cyber defenses

As a part of an ongoing White House initiative to make software more secure, the Defense Advanced Research Projects Agency (DARPA) plans to launch a two-year contest, the AI Cyber Challenge, that'll task competitors with identifying and fixing software vulnerabilities using AI.

https://techcrunch.com/2023/08/09/darpa-launches-two-year-competition-to-build-ai-powered-cyber-defenses/

Click above link to read more.

Back to top

Hundreds of executives are falling for Microsoft 365 phishing attacks: Report

Threat actors are having recent success defeating multifactor authentication-protected Microsoft 365 cloud accounts using the EvilProxy phishing kit, say researchers at Proofpoint.

https://financialpost.com/technology/hundreds-of-executives-are-falling-for-microsoft-365-phishing-attacks-report

Click above link to read more.

Back to top

How fame-seeking teenagers hacked some of the world's biggest targets

A ragtag bunch of amateur hackers, many of them teenagers with little technical training, have been so adept at breaching large targets, including Microsoft, Okta, Nvidia, and Globant, that the federal government is studying their methods to get a better grounding in cybersecurity.

https://arstechnica.com/security/2023/08/homeland-security-details-how-teen-hackers-breached-some-of-the-biggest-targets/

Click above link to read more.

Back to top

How safe is my data after a hack or leak?

Following news stories in the past few days, it's understandable you might be concerned about your data.

https://www.bbc.com/news/technology-66451970

Click above link to read more.

Back to top

Intel 'Downfall': Severe flaw in billions of CPUs leaks passwords and much more

There is a serious security flaw in billions of Intel CPUs that can let attackers steal confidential data like passwords and encryption keys. Firmware updates can fix it, but at a potential significant performance loss.

https://www.pcworld.com/article/2025589/downfall-serious-security-vulnerability-in-billions-of-intel-cpus-how-to-protect-yourself.html

Click above link to read more.

Back to top

Charming Kitten targets Iranian dissidents with advanced cyber attacks

Germany's Federal Office for the Protection of the Constitution (BfV) has warned of cyber attacks targeting Iranian persons and organizations in the country since the end of 2022.

https://thehackernews.com/2023/08/charming-kitten-targets-iranian.html

Click above link to read more.

Back to top

For U.S. officials, the world's largest hacking conference isn't all fun and games

The easiest way to embarrass yourself at DEF CON, the annual Las Vegas confab of the world's largest collection of hackers: ending up on the Wall of Sheep.

https://www.politico.com/news/2023/08/12/u-s-officials-def-con-hacking-conference-00110946

Click above link to read more.

Back to top

When cybersecurity becomes 'HR's problem'

Morey Haber says he sleeps like a baby. That is, he's up every couple of hours. It's a touch of cybersecurity humor if there is such a thing. Haber is the chief security officer at BeyondTrust, an identity security firm with clients around the world, and in his line of work, he's seen some nightmares—and HR needs to be aware of them.

https://hrexecutive.com/when-cybersecurity-becomes-hrs-problem/

Click above link to read more.

Back to top

Hackers leverage websites hosted on AWS S3 buckets to send phishing links

Hackers use legitimate Amazon Web Services (AWS) S3 buckets to send phishing emails.

https://cybersecuritynews.com/hackers-leverage-websites-hosted-aws/

Click above link to read more.

Back to top

Hackers attacking power generator systems to infect with ransomware

A new variant of SystemBC malware was found to be deployed to a critical infrastructure target. This malware was responsible for the DarkSide Colonial Pipeline Incident in 2021. There have been several Ransomware attacks during the second quarter of 2023.

https://cybersecuritynews.com/power-generator-systems-ransomware/

Click above link to read more.

Back to top

Ford cars Wi-Fi vulnerability let attackers execute remote code

Ford recently identified a buffer overflow flaw in the Wi-Fi driver used by it in the SYNC 3 infotainment system. After the discovery, Ford quickly alerted about this flaw and disclosed the vulnerability publicly.

https://gbhackers.com/ford-cars-wifi-vulnerability/

Click above link to read more.

Back to top

---

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