
## February 20, 2024

**Challenge yourself with our Employment Scams Quiz!**

Cybersecurity theme of the week: **AI**

✪ Check out our **Security Day AI presentations** to learn more.

## Wonder what you can do to protect yourself from AI fraud?

| All Users | Technical Users | Business Owners |
|---|---|---|
| Research and understand the many ways that AI are used maliciously, and how you can detect them. Common forms of AI fraud include: Deepfaked images and video, deepfaked audio (voice cloning), phishing attacks, fake news dissemination, and more. | Always vet your resources and double check information before redistributing or citing it. | Prepare your employees with the tools and knowledge to recognize and detect deepfaked images, video, and audio. |

This past week's stories:

🍁 **Ottawa willing to improve cybersecurity bill, ministers tell MPs**

🍁 **Anand: Federal experts 'in constant contact' to address cyber incident at health insurance provider for public servants**

🍁 **'High impact' cyber attacks at Canadian banks nearly tripled in one year: regulator**

🍁 **Okanagan-Skaha school district offline after cybersecurity incident**

✪ **Google launches a slew of AI initiatives to enhance cybersecurity**

**Midnight Blizzard and Cloudflare-Atlassian cybersecurity incidents: What to know**

**Microsoft says it caught hackers from China, Russia and Iran using its AI tools**

**Iran-backed hackers interrupt UAE, UK and Canadian programming with fake AI news broadcast**

**Water Hydra group exploits Microsoft Defender SmartScreen zero-day flaw**

---

### Ottawa willing to improve cybersecurity bill, ministers tell MPs

Two senior Canadian cabinet ministers have told a parliamentary committee that the government is willing to make changes to its proposed cybersecurity legislation for federally regulated critical infrastructure providers to strengthen the bill.

https://www.itworldcanada.com/article/ottawa-willing-to-improve-cybersecurity-bill-ministers-tell-mps/558902

*Click above link to read more.*

Back to top

---

### Anand: Federal experts 'in constant contact' to address cyber incident at health insurance provider for public servants

The federal government says cyber security and privacy experts are “in constant contact” with public benefits providers to address a recent “cyber incident” impacting MSH International (MSH), and to protect the personal information of government employees.

https://www.ctvnews.ca/canada/anand-federal-experts-in-constant-contact-to-address-cyber-incident-at-health-insurance-provider-for-public-servants-1.6768913

*Click above link to read more.*

Back to top

---

### 'High impact' cyber attacks at Canadian banks nearly tripled in one year: regulator

Canada’s banking watchdog says it’s worried about the increasing number of “high impact” cyberattacks against banks that lead to service disruptions or data leaks, which have nearly tripled in the last year.

https://nationalpost.com/news/canada/cyber-attacks-at-canadian-banks-nearly-tripled

*Click above link to read more.*

Back to top

---

### Okanagan-Skaha school district offline after cybersecurity incident

The entire School District 67 is offline after a cybersecurity incident on Tuesday.

https://www.vernonmorningstar.com/news/okanagan-skaha-school-district-offline-after-cybersecurity-incident-7318190

*Click above link to read more.*

Back to top

---

### Google launches a slew of AI initiatives to enhance cybersecurity

The company also announced $2 million in research grants and strategic partnerships to support research at several institutes, including The University of Chicago, Carnegie Mellon, and Stanford.

https://www.csoonline.com/article/1308071/google-launches-a-slew-of-ai-initiatives-to-enhance-cybersecurity.html

*Click above link to read more.*

Back to top

---

### Midnight Blizzard and Cloudflare-Atlassian cybersecurity incidents: What to know

The Midnight Blizzard and Cloudflare-Atlassian cybersecurity incidents raised alarms about the vulnerabilities inherent in major SaaS platforms. These incidents illustrate the stakes involved in SaaS breaches — safeguarding the integrity of SaaS apps and their sensitive data is critical but is not easy. Common threat vectors such as sophisticated spear-phishing, misconfigurations and vulnerabilities in third-party app integrations demonstrate the complex security challenges facing IT systems.

https://thehackernews.com/2024/02/midnight-blizzard-and-cloudflare.html

*Click above link to read more.*

Back to top

---

### Microsoft says it caught hackers from China, Russia and Iran using its AI tools

State-backed hackers from Russia, China, and Iran have been using tools from Microsoft-backed OpenAI to hone their skills and trick their targets, according to a report published on Wednesday.

https://www.reuters.com/technology/cybersecurity/microsoft-says-it-caught-hackers-china-russia-iran-using-its-ai-tools-2024-02-14/

*Click above link to read more.*

Back to top

---

## Iran-backed hackers interrupt UAE, UK and Canadian programming with fake AI news broadcast

A group of hackers linked to Iran have interrupted BBC and a host of other European TV streaming services in Britain, the United Arab Emirates and Canada, Microsoft stated in a report earlier this month, noting a marked acceleration of Iranian cyber attacks since Hamas's October 7 attack on Israel. The programming was interrupted with a fake news report on Gaza featuring graphic images and what appeared to be an AI-generated anchor – the first time Iran has used AI in this way in its influence operations.

https://www.france24.com/en/middle-east/20240214-iran-hackers-interrupt-uae-uk-canadian-programming-fake-ai-news-cyber-attacks

*Click above link to read more.*

Back to top

---

## Water Hydra group exploits Microsoft Defender SmartScreen zero-day flaw

Threat actors exploit Microsoft Defender SmartScreen zero-day flaws to circumvent the security mechanisms designed to protect users from malicious websites and downloads.

https://cybersecuritynews.com/water-hydra-smartscreen-zero-day-flaw/

*Click above link to read more.*

Back to top

---

## Microsoft, OpenAI warn of nation-state hackers weaponizing AI for cyber attacks

Nation-state actors associated with Russia, North Korea, Iran, and China are experimenting with artificial intelligence (AI) and large language models (LLMs) to complement their ongoing cyber attack operations.

https://thehackernews.com/2024/02/microsoft-openai-warn-of-nation-state.html

*Click above link to read more.*

Back to top

---

### ISC2 collaborates with IBM to launch entry-level cybersecurity certificate

ISC2 – the world's leading nonprofit member organization for cybersecurity professionals – announced a partnership with IBM (NYSE: IBM) to launch the IBM and ISC2 Cybersecurity Specialist Professional Certificate. The new entry-level program, available exclusively via the Coursera platform, is designed to prepare prospective cybersecurity professionals for a career in the field. By completing a joint 12-course series, incorporating the domains from ISC2's Certified in Cybersecurity (CC) certification training, candidates with no previous experience can obtain the in-demand skills and hands-on experience required for a cybersecurity specialist role in four months.

https://www.itsecurityguru.org/2024/02/16/isc2-collaborates-with-ibm-to-launch-entry-level-cybersecurity-certificate/

*Click above link to read more.*

Back to top

---

### Lockbit cybercrime gang disrupted by Britain, US and EU

Lockbit, a notorious cybercrime gang that holds its victims' data to ransom, has been disrupted in a rare international law enforcement operation, the gang and U.S. and UK authorities said on Monday.

https://www.reuters.com/technology/cybersecurity/lockbit-cybercrime-gang-disrupted-by-international-police-operation-2024-02-19/

*Click above link to read more.*

Back to top

---

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