January 30, 2024

Challenge yourself with our Quishing Quiz!

Cybersecurity theme of the week: **Deep Fakes**

✪ Check out our Security Day Presentation on Deep Fakes to learn more.

Wonder what you can do to protect yourself from deep fakes?

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: Deep faked images and video, deep faked 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 deep faked images, video, and audio. Ways to spot a deep fake include looking for the following: a lack of blinking (deep fakes don't blink), no side profiles, poor-quality images and video, faster video speed length than normal, and difference in colours.

This past week's stories:

- Failure to launch: Cybersecurity pros discuss how to solve the resource crisis
- Google Canada commits $1.3 million to bolster Quebec's cybersecurity ecosystem and launches cybersecurity education certificate
- Quebec City ambulance dispatch hit by ransomware attack
- HP Enterprise discloses hack by suspected state-backed Russian hackers
- Cybersecurity law forces Porsche to kill gas-powered Macan in Europe
- 3000+ discussions on dark web posts to use ChatGPT for illegal purposes
- Denmark announces $13 million for Ukraine's cybersecurity
- ✪ Taylor Swift deepfakes spark calls in Congress for new legislation

23andMe admits it didn’t detect cyberattacks for months

QR code phishing soars 587%: Users falling victim to social engineering scams

Crypto hackers stole around $1.7 bln in 2023 – report

Energy giant Schneider Electric hit by Cactus ransomware attack

How a mistakenly published password exposed Mercedes-Benz source code

---

Failure to launch: Cybersecurity pros discuss how to solve the resource crisis

As part of IT World Canada’s partnership with the Canadian Cybersecurity Network, we are featuring a replay of a recent panel discussion featuring cybersecurity professionals discussing the issues that we face in gaining and retaining talent.

https://www.itworldcanada.com/article/failure-to-launch-cybersecurity-pros-discuss-how-to-solve-the-resource-crisis/557306

Click above link to read more.

Back to top

Google Canada commits $1.3 million to bolster Quebec's cybersecurity ecosystem and launches cybersecurity education certificate

Google Canada announced new support for Quebec's cybersecurity ecosystem. Google.org will provide a $1.3 million grant to the Multidisciplinary Institute for Cybersecurity and Cyber Resilience (IMC2) to support research that addresses the rising global cyber risks.

https://www.newswire.ca/news-releases/google-canada-commits-1-3-million-to-bolster-quebec-s-cybersecurity-ecosystem-and-launches-cybersecurity-education-certificate-889831871.html

Click above link to read more.

Back to top

Quebec City ambulance dispatch hit by ransomware attack

The ambulance dispatch centre in Quebec City was the victim of a ransomware cyber attack this week.

https://montreal.ctvnews.ca/quebec-city-ambulance-dispatch-hit-by-ransomware-attack-1.6743464

Click above link to read more.

Back to top

HP Enterprise discloses hack by suspected state-backed Russian hackers

Hewlett Packard Enterprise disclosed Wednesday that suspected state-backed Russian hackers broke into its cloud-based email system and stole data from cybersecurity and other employees.

https://apnews.com/article/russian-hackers-hewlett-packard-enterprise-microsoft-sec-breach-cozy-bear-d4e88ded0a47d010216e11f41132f72c

Click above link to read more.

Back to top

Cybersecurity law forces Porsche to kill gas-powered Macan in Europe

Porsche just revealed the new, second-generation Macan, and it's all electric. It seems like a bold move for Porsche, going EV with its best-selling model, but the company is hedging its bets. A Porsche spokesperson confirmed to Motor1 that the gas model will live on in the US for the foreseeable future.

https://www.motor1.com/news/706105/porsche-continuing-gas-macan-sales/

Click above link to read more.

Back to top

3000+ discussions on dark web posts to use ChatGPT for illegal purposes

For the multitude of malicious activities, threat actors could exploit ChatGPT due to its conversational abilities, such as generating convincing phishing messages, crafting sophisticated social engineering attacks, and automating the production of misleading content.

https://cybersecuritynews.com/3000-discussions-on-dark-web-posts/

Click above link to read more.

Back to top

Denmark announces $13 million for Ukraine's cybersecurity

Denmark has allocated 91 million Danish kroner ($13.3 million) for projects to support the cybersecurity and cyber defense of Ukraine's Armed Forces and Defense Ministry, the Danish Defense Ministry said on Jan. 24.

https://news.yahoo.com/denmark-announces-13-million-ukraines-125254673.html

Click above link to read more.

Back to top

Taylor Swift deepfakes spark calls in Congress for new legislation

US politicians have called for new laws to criminalise the creation of deepfake images, after explicit faked photos of Taylor Swift were viewed millions of times online.

https://www.bbc.com/news/technology-68110476

Click above link to read more.

Back to top

23andMe admits it didn’t detect cyberattacks for months

In a data breach notification letter filed with regulators this weekend, 23andMe revealed that hackers started breaking into customers’ accounts in April 2023 and continued through most of September.

https://techcrunch.com/2024/01/25/23andme-admits-it-didnt-detect-cyberattacks-for-months/

Click above link to read more.

Back to top

QR code phishing soars 587%: Users falling victim to social engineering scams

Check Point Software Technologies, a cybersecurity solutions provider, has published new research illustrating a typical QR code attack. In this attack, scammers utilize QR codes to redirect users to a credential harvesting page, adjusting the redirection chain based on the user’s device.

https://www.hackread.com/qr-code-phishing-social-engineering-scams/

Click above link to read more.

Back to top

Crypto hackers stole around $1.7 bln in 2023 – report

Hackers of cryptocurrency platforms stole around $1.7 billion in 2023, around 54.3% lower than the year before, a Chainalysis report showed on Wednesday.

https://www.reuters.com/technology/cybersecurity/crypto-hackers-stole-around-17-bln-2023-report-2024-01-24/

Click above link to read more.

Back to top

Energy giant Schneider Electric hit by Cactus ransomware attack

Energy management and automation giant Schneider Electric suffered a Cactus ransomware attack leading to the theft of corporate data, according to people familiar with the matter.

https://www.bleepingcomputer.com/news/security/energy-giant-schneider-electric-hit-by-cactus-ransomware-attack/

Click above link to read more.

Back to top

How a mistakenly published password exposed Mercedes-Benz source code

Mercedes-Benz accidentally exposed a trove of internal data after leaving a private key online that gave “unrestricted access” to the company’s source code, according to the security research firm that discovered it.

https://techcrunch.com/2024/01/26/mercedez-benz-token-exposed-source-code-github/

Click above link to read more.

Back to top

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