July 11, 2023

Challenge yourself with our Malvertising Quiz!

This past week's stories:

- **Cybercriminals can break voice authentication with 99% success rate**
- **'Unauthorized party' obtained Petro-Points members' contact information in IT breach, company says**
- **Suncor swaps out laptops after cybersecurity incident as energy sector takes stock of risks**
- **Canadian cybersecurity agency and FBI issue advisory over rising 'Truebot' cyberattacks**
- **HWL Ebsworth hack: Russian gang released 'sensitive personal and government information', Australia's cybersecurity chief says**
- **RedEnergy stealer-as-a-ransomware threat targeting energy and telecom sectors**
- **Harvard University web flaw exposed it to remote attacks**
- **ChatGPT to ThreatGPT: Generative AI impact in cybersecurity and privacy**
- **ISACA joins European Cyber Security Organisation (ECSO) to strengthen cybersecurity and digital skills in Europe**
- **Most Fortinet FortiGate firewalls remain vulnerable to critical CVE**
- **UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach**
- **Top Cybersecurity Jobs Available Now in 2023**

Cybercriminals can break voice authentication with 99% success rate

Computer scientists at the University of Waterloo have discovered a method of attack that can successfully bypass voice authentication security systems with up to a 99% success rate after only six tries.

https://www.helpnetsecurity.com/2023/07/06/voice-authentication-insecurity/

Click above link to read more.

Back to top

'Unauthorized party' obtained Petro-Points members' contact information in IT breach, company says

An unauthorized party obtained Petro-Points members' basic contact information in a cybersecurity incident that happened roughly two weeks ago, the company said Thursday.

https://www.cbc.ca/news/canada/calgary/petro-points-suncor-it-breach-1.6899274

Click above link to read more.

Back to top

Suncor swaps out laptops after cybersecurity incident as energy sector takes stock of risks

Suncor is replacing employee computers after a cybersecurity incident last week shut down debit and credit processing at Petro-Canada gas stations across the country, among a series of other security measures at the Calgary-based company.

https://www.cbc.ca/news/canada/calgary/suncor-cybersecurity-incident-energy-sector-1.6898118

Click above link to read more.

Back to top

Canadian cybersecurity agency and FBI issue advisory over rising 'Truebot' cyberattacks

The Canadian Centre for Cyber Security has issued a joint advisory with the FBI and other U.S. agencies about increasing attacks from "Truebot" malware.

https://www.ctvnews.ca/sci-tech/canadian-cybersecurity-agency-and-fbi-issue-advisory-over-rising-truebot-cyber-attacks-1.6471754

Click above link to read more.

Back to top

HWL Ebsworth hack: Russian gang released 'sensitive personal and government information', Australia's cybersecurity chief says

Sensitive and personal government information has been stolen from law firm HWL Ebsworth by a Russian ransomware gang and posted online, Australia's new cybersecurity chief says.

https://www.theguardian.com/technology/2023/jul/05/hwl-ebsworth-hack-russian-gang-released-sensitive-personal-and-government-information-australian-cybersecurity-chief-says

Click above link to read more.

Back to top

RedEnergy stealer-as-a-ransomware threat targeting energy and telecom sectors

A sophisticated stealer-as-a-ransomware threat dubbed RedEnergy has been spotted in the wild targeting energy utilities, oil, gas, telecom, and machinery sectors in Brazil and the Philippines through their LinkedIn pages.

https://thehackernews.com/2023/07/redenergy-stealer-as-ransomware-threat.html

Click above link to read more.

Back to top

Harvard University web flaw exposed it to remote attacks

A Harvard University subdomain vulnerability exposed the website to remote code execution (RCE) attacks, potentially allowing threat actors to steal and modify data stored on the website.

https://cybernews.com/security/harvard-university-remote-code-execution-attack/

Click above link to read more.

Back to top

ChatGPT to ThreatGPT: Generative AI impact in cybersecurity and privacy

OpenAI launched ChatGPT in November 2022, and the arrival of ChatGPT caused a significant disruption in the AI/ML community.

https://cybersecuritynews.com/chatgpt-to-threatgpt/

Click above link to read more.

Back to top

ISACA joins European Cyber Security Organisation (ECSO) to strengthen cybersecurity and digital skills in Europe

ISACA, a leading global association for digital trust professionals, is delighted to announce it is joining the European Cyber Security Organisation (ECSO). The membership will work to accelerate ECSO and ISACA's shared commitment to advancing cybersecurity, fostering collaboration and driving digital trust across Europe.

https://www.businesswire.com/news/home/20230706302434/en/ISACA-Joins-European-Cyber-Security-Organisation-ECSO-to-Strengthen-Cybersecurity-and-Digital-Skills-in-Europe

Click above link to read more.

Back to top

Most Fortinet FortiGate firewalls remain vulnerable to critical CVE

More than two-thirds of Fortinet's FortiGate firewalls remain at risk of exploits through a vulnerability the company disclosed on June 12, according to research Bishop Fox released Friday.

https://www.cybersecuritydive.com/news/fortinet-firewalls-vulnerability-exploits/685230/

Click above link to read more.

Back to top

UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach

The U.K.'s largest NHS trust has confirmed it's investigating a ransomware incident as the country's public sector continues to battle a rising wave of cyberattacks

https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/

Click above link to read more.

Back to top

Top Cybersecurity Jobs Available Now in 2023

Cybersecurity jobs are in high demand in today's increasingly digital environment interactions

https://www.analyticsinsight.net/top-cybersecurity-jobs-available-now-in-2023/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.