April 4, 2023

Challenge yourself with our Drop Shipping Scam Quiz!

This past week's stories:

Multilayered cybersecurity approach crucial for businesses - report
Only 10% of workers remember all their cyber security training
Microsoft puts ChatGPT to work on automating cybersecurity
Study reveals WiFi protocol vulnerability exposing network traffic
Winter Vivern APT targets European government entities with Zimbra vulnerability
Failed IT systems at Capita fuel fears of cyber-attack on crucial NHS provider
ChatGPT banned in Italy over privacy concerns
Cyber Police of Ukraine busted phishing gang responsible for $4.33 million scam
Ferrari disclosed a data breach impacting customer data but refused to pay ransom
NATO officially bans TikTok on devices of its staff
Novel social engineering attacks surge by 135 percent driven by generative AI
'Tactical Octopus' hackers using tax-related phishing scams to spread malware

---

Multilayered cybersecurity approach crucial for businesses – report

A new report has highlighted the importance of a multilayered cybersecurity approach for businesses of all sizes due to threat actors that have continued to "double down on longstanding tactics while demonstrating innovation with new techniques."

https://www.insurancebusinessmag.com/ca/news/cyber/multilayered-cybersecurity-approach-crucial-for-businesses--report-441235.aspx

Click above link to read more.

Back to top

Only 10% of workers remember all their cyber security training

New research by CybSafe found only 10% of workers remember all their cybersecurity training. This is exposing companies to cyber risk.

https://www.itsecurityguru.org/2023/03/30/only-10-of-workers-remember-all-their-cyber-security-training/

Click above link to read more.

Back to top

Microsoft puts ChatGPT to work on automating cybersecurity

Microsoft on Wednesday rolled out an AI-powered security analysis tool to automate incident response and threat hunting tasks, showcasing a security use-case for the popular chatbot developed by OpenAI.

https://www.securityweek.com/microsoft-puts-chatgpt-to-work-on-automating-cybersecurity/

Click above link to read more.

Back to top

Study reveals WiFi protocol vulnerability exposing network traffic

Researchers have discovered a major security vulnerability in the WiFi protocol that risks data exposure to snoopers. They demonstrated two attack strategies exploiting the flaw, which could allow an adversary to meddle with traffic, client connections, and more.

https://latesthackingnews.com/2023/03/31/study-reveals-wifi-protocol-vulnerability-exposing-network-traffic/

Click above link to read more.

Back to top

Winter Vivern APT targets European government entities with Zimbra vulnerability

The advanced persistent threat (APT) actor known as Winter Vivern is now targeting officials in Europe and the U.S. as part of an ongoing cyber espionage campaign.

https://thehackernews.com/2023/03/winter-vivern-apt-targets-european.html

Click above link to read more.

Back to top

Failed IT systems at Capita fuel fears of cyber-attack on crucial NHS provider

Computer systems have abruptly stopped working at the outsourcing group Capita, knocking out local council phone lines and triggering fears that the company that runs crucial operations for the NHS and the military could be under cyber-attack.

https://www.theguardian.com/business/2023/mar/31/capita-it-systems-fail-cyber-attack-nhs-fears

Click above link to read more.

Back to top

ChatGPT banned in Italy over privacy concerns

Italy has become the first Western country to block advanced chatbot ChatGPT.

https://www.bbc.com/news/technology-65139406

Click above link to read more.

Back to top

Cyber Police of Ukraine busted phishing gang responsible for $4.33 million scam

The Cyber Police of Ukraine, in collaboration with law enforcement officials from Czechia, has arrested several members of a cybercriminal gang that set up phishing sites to target European users.

https://thehackernews.com/2023/03/cyber-police-of-ukraine-busted-phishing.html

Click above link to read more.

Back to top

Ferrari disclosed a data breach impacting customer data but refused to pay ransom

Ferrari disclosed a data breach impacting the customer data of an undisclosed number of individuals after a threat actor made a ransom demand.

https://www.cpomagazine.com/cyber-security/ferrari-disclosed-a-data-breach-impacting-customer-data-but-refused-to-pay-ransom/

Click above link to read more.

Back to top

NATO officially bans TikTok on devices of its staff

Social media app TikTok has been officially banned by NATO from the devices it provides to its staffers, citing security concerns, as per two NATO officials who were familiar with the matter.

https://www.wionews.com/world/nato-officially-bans-tiktok-on-devices-of-its-staff-578456

Click above link to read more.

Back to top

Novel social engineering attacks surge by 135 percent driven by generative AI

New research from cybersecurity AI company Darktrace shows a 135 percent increase in social engineering attacks using sophisticated linguistic techniques, including increased text volume, punctuation, and sentence length, and with no links or attachments.

https://betanews.com/2023/04/03/novel-social-engineering-attacks-surge-by-135-percent-driven-by-generative-ai/

Click above link to read more.

Back to top

'Tactical Octopus' hackers using tax-related phishing scams to spread malware

Researchers are warning about a group of hackers that are using tax-related email lures to spread dangerous malware.

https://therecord.media/hackers-use-phishing-schemes-tax-scams

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