December 13, 2022

Challenge yourself with our Holiday Scam Security Quiz!

This past week's stories:

CFIB launches Cybersecurity Academy for small, medium businesses

An online cybersecurity training program aimed at Canadian small and medium businesses debuts today, months after it was supposed to launch Cybersecurity Academy, a gamification platform open to the 95,000 members of the Canadian Federation of Independent Business (CFIB), was first announced in March and promised to go live in either the spring or the summer.

"We spent a lot of time discerning the contents and making sure that it was the right tone and digestible for business owners," Mandy D'Autremont, the federation's vice-president of marketing partnerships, said in an interview. "We wanted to get it right."

https://www.itworldcanada.com/article/cfib-launches-cybersecurity-academy-for-small-medium-businesses/517529

Click above link to read more.

Back to top

ChatGPT shows promise of using AI to write malware

For even the most skilled hackers, it can take at least an hour to write a script to exploit a software vulnerability and infiltrate their target. Soon, a machine may be able to do it in mere seconds.

When OpenAI last week released its ChatGPT tool, allowing users to interact with an artificial intelligence chatbot, computer security researcher Brendan Dolan-Gavitt wondered whether he could instruct it to write malicious code. So, he asked the model to solve a simple capture-the-flag challenge.

https://www.cyberscoop.com/chatgpt-ai-malware/

Click above link to read more.

Back to top

Major cloud, email hosting provider blames ransomware attack for outage

Email hosting provider Rackspace Technology confirmed on Tuesday that a ransomware attack is behind an outage that has been disrupting its email service since Friday.

The company said it has retained a cyber defense firm to investigate the attack and has since discovered that the incident only impacted its Hosted Exchange business while its other products and services are fully operational.

https://thehill.com/policy/cybersecurity/3765398-major-cloud-email-hosting-provider-blames-ransomware-attack-for-outage/

Click above link to read more.

Back to top

CloudSEK claims it was hacked by another cybersecurity firm

Indian cybersecurity firm CloudSEK says a threat actor gained access to its Confluence server using stolen credentials for one of its employees' Jira accounts.

While some internal information, including screenshots of product dashboards and three customers' names and purchase orders, was exfiltrated from its Confluence wiki, CloudSEK says the attackers didn't compromise its databases.

https://www.bleepingcomputer.com/news/security/cloudsek-claims-it-was-hacked-by-another-cybersecurity-firm/

Click above link to read more.

Back to top

Vice Society ransomware attackers targeted dozens of schools in 2022

The Vice Society cybercrime group has disproportionately targeted educational institutions, accounting for 33 victims in 2022 and surpassing other ransomware families like LockBit, BlackCat, BianLian, and Hive.

Other prominent industry verticals targeted include healthcare, governments, manufacturing, retail, and legal services, according to an analysis of leak site data by Palo Alto Networks Unit 42.

https://thehackernews.com/2022/12/vice-society-ransomware-attackers.html

Click above link to read more.

Back to top

Apple boosts iPhone security with major new move

Apple is set to boost security by more widely allowing the use of hardware security keys as an extra layer of protection, the iPhone maker has confirmed in an announcement.

Starting next year, the iPhone maker will allow you to protect your Apple ID and iCloud account using security keys. This means that as well as a password, a physical key can be used as another layer of protection on your account.

https://www.forbes.com/sites/kateoflahertyuk/2022/12/09/apple-boosts-iphone-security-with-major-new-move/?sh=75e697e3cb5c

Click above link to read more.

Back to top

The biggest data breaches and leaks of 2022

More than 4,100 publicly disclosed data breaches occurred in 2022 equating to approximately 22 billion records being exposed. Cyber security publication Security Magazine reported that the figures for 2022 are expected to exceed this figure by as much as five percent.

In this article, we reveal which data breaches and leaks and the phishing, malware and cyber attacks ranked among our top ten most-read cyber security news stories of 2022.

https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022

Click above link to read more.

Back to top

UNLV grads, Las Vegas Strip resorts team up to tackle cyber-security risks

Graduate students at the University of Nevada Las Vegas (UNLV) are working with major resorts and casinos in the battle against cyber security attacks.

The students are competing in National Cyber League, a virtual training ground that challenges participants to solve real-world cyber security challenges, using a safe platform.

https://www.8newsnow.com/news/local-news/unlv-grads-las-vegas-strip-resorts-team-up-to-tackle-cyber-security-risks/

Click above link to read more.

Back to top

UK Gov introduces new security and privacy rules for apps

In a bid to protect consumers from malicious apps which can steal data and money, the UK Government has introduced new rules for app store operators and developers.

Millions of people across the UK use apps on their smartphones, game consoles and smart TVs for a wide range of everyday activities such as work, communication, entertainment and banking.

https://www.digit.fyi/uk-gov-introduces-new-security-and-privacy-rules-for-apps/

Click above link to read more.

Back to top

New dark web website allows hackers to embed malware to legitimate Android apps

ThreatFabric's researchers found 'Zombinder', a third-party darknet service that was used to bind malware payloads to legitimate Android applications.

In order to deceive users into installing a malicious payload, it is used to bind a malicious payload to a legitimate application.

https://cybersecuritynews.com/legitimate-android-apps/

Click above link to read more.

Back to top

Researchers detail new attack method to bypass popular web application firewalls

A new attack method can be used to circumvent web application firewalls (WAFs) of various vendors and infiltrate systems, potentially enabling attackers to gain access to sensitive business and customer information.

Web application firewalls are a key line of defense to help filter, monitor, and block HTTP(S) traffic to and from a web application, and safeguard against attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection (SQLi).

https://thehackernews.com/2022/12/researchers-detail-new-attack-method-to.html

Click above link to read more.

Back to top

War in Ukraine dominated cybersecurity in 2022

Russia's war against Ukraine and the worries about possible cyberattacks against the country's allies, like the US, dominated cybersecurity news throughout 2022.

Even before Russia's February invasion, cybersecurity experts were gearing up for online attacks that some of them thought could potentially cross the line into cyberwarfare. Russia did have some success early on, but Ukraine showed it could not only rebound and rebuild, but also control the message coming out of the war zones, neutralizing Russian disinformation campaigns.

https://www.cnet.com/tech/services-and-software/war-in-ukraine-dominated-cybersecurity-in-2022/

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