October 19, 2021

Challenge yourself with our Cyber Security Awareness Month quiz!

Join Cyber Security Awareness Month!

Register for Security Day!

This week's stories:

Playing digital defence: Small businesses are stepping up their cyber security efforts - but gap in preparedness remains: RBC poll

As the economy becomes increasingly digitized, cyber security concerns are rising to the top of business risks as ranked by Canadian small business owners – and for good reason. In a recent survey commissioned by RBC[1], nearly half of Canada's small business owners report that they anticipate becoming a victim of a cybercrime in the next 12 months – a percentage significantly higher than seen

among the general population (34%). Forty per cent of small businesses identified that having devices infected by a virus or malware is now perceived as their biggest threat, ranking higher than falling victim to an online scam or fraud (24%), or property damage (24%).

https://stockhouse.com/news/press-releases/2021/10/18/playing-digital-defence-small-businesses-are-stepping-up-their-cyber-security

Click above link to read more.

Back to top

Google gives security keys to 10,000 high-risk users

Google is giving free physical USB security keys to 10,000 users at high risk of being hacked - such as politicians and human rights activists.

The USB keys provide two-factor authentication - an additional layer of security beyond a password.

Google says it wants to encourage people to join its "advanced protection programme" for high-profile users.

https://www.bbc.com/news/technology-58844502

Click above link to read more.

Back to top

New Australian ransomware plan could freeze or seize cryptocurrencies

Australian authorities are laying the groundwork to seize or freeze cryptocurrencies linked to cybercrimes regardless from where the attacks originated, according to a new Ransomware Action Plan released by the Australian government.

The 12-page document aims to set out a comprehensive government strategy to target cyber criminals. Among other things, the plan proposes new criminal charges against adversaries who target critical infrastructure with ransomware and suggests new criminal statutes for those who knowingly buy or sell stolen data or malware.

https://therecord.media/new-australian-ransomware-plan-could-freeze-or-seize-cryptocurrencies/

Click above link to read more.

Back to top

Flaws in GitHub Actions bypass code review mechanism

Researchers at Cider Security have uncovered a security loophole in GitHub Actions that allows adversaries to bypass the required reviews mechanism and push non-reviewed code to a protected branch, allowing it into the pipeline to production.

Lead security researcher Omer Gil and his team of researchers at Cider Security, a start-up focusing on continuous integration/continuous delivery security, found the vulnerability as part of their research for novel attacks in DevOps according to a blog post on Medium.

https://www.bankinfosecurity.com/flaws-in-github-actions-bypass-code-review-mechanism-a-17733

Click above link to read more.

Back to top

Critical flaw in OpenSea could have let hackers steal cryptocurrency from wallets

A now-patched critical vulnerability in OpenSea, the world's largest non-fungible token (NFT) marketplace, could've been abused by malicious actors to drain cryptocurrency funds from a victim by sending a specially-crafted token, opening a new attack vector for exploitation.

The findings come from cybersecurity firm Check Point Research, which began an investigation into the platform following public reports of stolen cryptocurrency wallets triggered by free airdropped NFTs. The issues were fixed in less than one hour of responsible disclosure on September 26, 2021.

https://thehackernews.com/2021/10/critical-flaw-in-opensea-could-have-let.html

Click above link to read more.

Back to top

Best practices to detect and mitigate deepfake attacks

As public engagement with digital content continues to rise, consumers and businesses are increasingly more reliant on technology platforms.

The anonymity of our digital world makes it difficult to know who is behind the screen. This gray space gives would-be fraudsters an opening to threaten both businesses and consumers directly, especially in the realm of deepfakes -- artificially created images, video and audio designed to emulate real human characteristics. In recent years, deepfakes have garnered widespread attention. They are an area of growing concern due to their involvement in fraudulent activities.

https://searchsecurity.techtarget.com/post/Best-practices-to-detect-and-mitigate-deepfake-attacks

Click above link to read more.

Back to top

If your apps or gadgets break down on Sunday, this may be why: Gpsd bug to roll back clocks to 2002

Come Sunday, October 24, 2021, those using applications that rely on gpsd for handling time data may find that they're living 1,024 weeks – 19.6 years – in the past.

A bug in gpsd that rolls clocks back to March, 2002, is set to strike this coming weekend.

The programming blunder was identified on July 24, 2021, and the errant code commit, written two years ago, has since been fixed. Now it's just a matter of making sure that every application and device deploying gpsd has applied the patch.

https://www.theregister.com/2021/10/19/gpsd_bug_reset/

Click above link to read more.

Back to top

CryptoRom Scam Rakes in $1.4M by Exploiting Apple Enterprise Features

Pyramid-scheme cryptocurrency scammers are exploiting Apple's Enterprise Developer Program to get bogus trading apps onto their marks' iPhones. So far, so good: They've made off with at least $1.4 million in ill-gotten gains so far.

That's according to Sophos Labs, which observed the scam making the rounds on dating sites.

https://threatpost.com/cryptorom-scammers-apple-enterprise-features/175474/

Click above link to read more.

Back to top

October is high season for cyberattacks, Infosec Institute study shows

There has been an exponential increase in cyberattacks around the globe in the last five years and a major chunk of it happened in October each year, according to a study by Infosec Institute.

A similar offensive appears to be building up this month, judging from the study's projections for an "October surprise" as well as observations of cyberattacks that have occurred so far.

https://www.csoonline.com/article/3636161/october-is-high-season-for-cyberattacks-infosec-institute-study-shows.html

Click above link to read more.

Back to top

Math symbols used for spoofing purposes in phishing campaigns

Phishing is a malicious technique used by cybercriminals to gather sensitive information from users.

Phishing attacks happen when the attackers pretend to be a trustworthy entity so they can bait the victims into trusting them and revealing their confidential data, later to be used for financial theft, identity theft, and to gain unauthorized access to the victim's accounts.

https://heimdalsecurity.com/blog/math-symbols-used-for-spoofing-purposes-in-phishing-campaigns/

Click above link to read more.

Back to top

How AI can stop zero-day ransomware

Over the past year, the sheer number of ransomware attacks have increased dramatically, with organizations of all stripes being affected: government entities, educational institutions, healthcare facilities, retailers, and even agricultural groups.

While the bulk of the media attention has been on critical infrastructure and large organizations, attackers are not limiting themselves to just those types of victims.

https://www.darkreading.com/dr-tech/how-ai-can-stop-zero-day-ransomware

Click above link to read more.

Back to top

WhatsApp announces end-to-end backup to protect 100 million users every day

The CEO of Facebook Mark Zuckerberg has recently announced on Thursday that WhatsApp will start rolling out the end-to-end encrypted chat backups for iOS and Android users globally.

This end-to-end encryption has put a lot of importance on security, and that's why it is one of the USPs of the app. It's was being stated that five years ago WhatsApp has added end-to-end encryption by default, and today it guards over 100 billion messages daily.

https://cybersecuritynews.com/whatsapp-announces-end-to-end-backup/

Click above link to read more.

Back to top

Microsoft's very bad year for security: A timeline

So far, 2021 has proved to be somewhat of a security *annus horribilis* for tech giant Microsoft, with numerous vulnerabilities impacting several of its leading services, including Active Directory, Exchange, and Azure. Microsoft is no stranger to being targeted by attackers seeking to exploit known and zero-day vulnerabilities, but the rate and scale of the incidents it has faced since early March has put the tech giant on its back foot for at least a moment or two.

What follows is a timeline of the significant security events that have afflicted Microsoft in 2021, why it remains susceptible to serious vulnerabilities and attacks, and an assessment of its response according to experts from across the cybersecurity sector.

https://www.csoonline.com/article/3635849/microsofts-very-bad-year-for-security-a-timeline.html

Click above link to read more.

Back to top

DocuSign phishing campaign targets low-ranking employees

Phishing actors are following a new trend of targeting non-executive employees but who still have access to valuable areas within an organization.

As reported by Avanan researchers, half of all phishing emails they analyzed in recent months impersonated non-executives, and 77% of them targeted employees on the same level.

https://www.bleepingcomputer.com/news/security/docusign-phishing-campaign-targets-low-ranking-employees/

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.