January 26th, 2021

Try our January "Resolutions" Quiz

This week's stories:

The pandemic and the 'spamdemic': More cybersecurity tips from an Ottawa expert

https://ottawa.ctvnews.ca/mobile/the-pandemic-and-the-spamdemic-more-cybersecurity-tips-from-an-ottawa-expert-1.5279979

Sure, maybe it was hard on your arteries but it didn't compromise your identity, your privacy, your devices or your finances.

Ottawa cybersecurity expert John Robinson, President and CEO of Intega IT, a company specializing in protecting small and medium-sized businesses, says he has seen a noticeable increase in spam during the COVID-19 pandemic, causing him to encourage people to protect themselves against more than germs, but a "spamdemic".

"Everybody's been bombarded with spam emails and cyber criminals are out there looking for opportunities and preying on people's cyber fatigue," Robinson says.

According to Robinson, our vulnerabilities and naïveté are open to exploitation, especially when we are busy multi-tasking and working from home.

Click link above to read more

North Korean hackers have targeted security researchers via social media

https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/

Google said today that a North Korean government hacking group has targeted members of the cyber-security community engaging in vulnerability research.

The attacks have been spotted by the Google Threat Analysis Group (TAG), a Google security team specialized in hunting advanced persistent threat (APT) groups.

In a report published earlier today, Google said North Korean hackers used multiple profiles on various social networks, such as Twitter, LinkedIn, Telegram, Discord, and Keybase, to reach out to security researchers using fake personas.

Click link above to read more

Cloud Jacking: The Bold New World of Enterprise

https://www.darkreading.com/cloud/cloud-jacking-the-bold-new-world-of-enterprise-cybersecurity/a/d-id/1339896
Those with their finger on the pulse of emerging cybersecurity threats are already aware that there's a new danger in town: cloud jacking. The increased reliance of individuals and businesses on cloud computing has led inevitably to this form of cybercrime primarily driven by misconfiguration and that looks to dominate a multitude of online security concerns in the near future.

Click link above to read more

SonicWall says it was hacked using zero-days in its own products

https://www.zdnet.com/article/sonicwall-says-it-was-hacked-using-zero-days-in-its-own-products/

The networking device vendor has published a series of mitigations as it's investigating the incident and preparing patches. Networking device maker SonicWall said on Friday night that it is investigating a security breach of its internal network after detecting what it described as a "coordinated attack."

In a short statement posted on its knowledgebase portal, the company said that "highly sophisticated threat actors" targeted its internal systems by "exploiting probable zero-day vulnerabilities on certain SonicWall secure remote access products."

Click link above to read more

Australia's securities regulator says server hit by cyber security breach

https://www.reuters.com/article/us-australia-cyber-asic/australias-securities-regulator-says-server-hit-by-cyber-security-breach-idUSKBN29U0S7?il=0

Australia’s securities regulator said on Monday there was a cyber security breach at a server it used to transfer files including credit licence applications where some information may have been viewed.

The Australian Securities and Investment Commission (ASIC) said it became aware of the incident on Jan. 15 although it does not appear the credit licence forms or attachments were downloaded.

Click link above to read more

2.28M MeetMindful Daters Compromised in Data Breach

https://threatpost.com/meetmindful-daters-compromised-data-breach/163313/
The ShinyHunters hacking group offer a raft of information, from location and contact info to dating preferences and bodily descriptions, as a free download. More than 2.28 million members of the online dating site MeetMindful have reportedly been caught up in a wide-ranging data breach that exposes everything from Facebook tokens to physical characteristics.

Click link above to read more

FBI warns of voice phishing attacks targeting employees at large companies

https://www.techrepublic.com/article/fbi-warns-of-voice-phishing-attacks-targeting-employees-at-large-companies/?ftag=TREa988f1c&bhid=42420269&mid=13241219&cid=2176068089
Using VoIP calls, the attackers trick people into logging into phishing sites as a way to steal their usernames and passwords. The FBI is cautioning companies to beware of a slew of voice phishing attacks aimed at capturing the login credentials of employees.

Click link above to read more

The aftermath of the SolarWinds breach: Organizations need to be more vigilant

https://www.techrepublic.com/article/the-aftermath-of-the-solarwinds-breach-organizations-need-to-be-more-vigilant/?ftag=TREa988f1c&bhid=42420269&mid=13241219&cid=2176068089
Security experts say organizations are, and should, implement a number of changes ranging from how they vet vendors to handling application updates. The way Nick Fuchs sees it, in the aftermath of the massive SolarWinds breach, there has been one silver lining: A greater understanding of the important role security needs to play in any organization. Not only is there an "obvious opportunity to learn from the event," but also an awareness "around the importance of prioritizing security fundamentals that penetrates all levels of the organization," said Fuchs, senior director of infrastructure, security, support, and controls at Springfield Clinic.

Click link above to read more

Suspicious Vaccine-Related Domains Triple

https://www.infosecurity-magazine.com/news/suspicious-vaccine-related-domains/#at_pco=smlrebh-1.0&at_si=6009af3c3ffa3d45&at_ab=per-2&at_pos=1&at_tot=4
The number of suspicious domains that feature the word "vaccine" in their title increased by almost 100% in the month after the first Pfizer COVID-19 vaccine was given outside of a clinical trial.

British grandmother Margaret Keenan became the first person in the world to receive the vaccine on December 8, 2020, a week before her 91st birthday.

New research by American cybersecurity software company Webroot observed that December 8 through January 6, there was an 94.8% increase in suspicious domain names using "vaccine" compared with the previous 30 days.

Click link above to read more

---

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