August 31, 2021

Challenge yourself with our Safe Surfing quiz!

This week's stories:

Halting hackers: How to keep your home Wi-Fi router secure

When it comes to home cybersecurity, experts tell CTVNews.ca that too many Canadians are overlooking their Wi-Fi routers, leaving their networks vulnerable to cyber-attacks.

"The word 'router' for most casual users of technology is often somewhat intimidating," London, Ont.-based technology analyst Carmi Levy told CTVNews.ca over the phone on Friday.

https://www.ctvnews.ca/sci-tech/halting-hackers-how-to-keep-your-home-wi-fi-router-secure-1.5565815?cid=sm%3Atrueanthem%3A%7B%7Bcampaignname%7D%7D%3Atwitterpost%E2%80%8B&taid=612c42abfbb26300018c3e2e&utm_campaign=trueAnthem%3A+Trending+Content&utm_medium=trueAnthem&utm_source=twitter

Click above link to read more.

Back to top

Microsoft fixes cloud platform vulnerability after warning

Microsoft says it has fixed a flaw in its cloud computing platform that cybersecurity researchers warned could have enabled hackers to take over a cloud-based database product used by many big companies.

The company said Friday there's no evidence the potential opening was exploited by malicious actors or that any customer data was exposed.

https://www.canadiansecuritymag.com/microsoft-fixes-cloud-platform-vulnerability-after-warning/

Click above link to read more.

Back to top

The underground economy: Recon, weaponization & delivery for account takeovers

In part one of a two-part series, Akamai's director of security technology and strategy, Tony Lauro, lays out what orgs need to know to defend against account takeover attacks.

With account takeover (ATO) attacks on the rise, stopping threat actors in the early phases of the kill chain will help today's defenders gain an upper hand against direct fraud campaigns.

https://threatpost.com/underground-economy-account-takeovers/169032/

Click above link to read more.

Back to top

Malware analysis for beginners: Getting started

With the cybersecurity industry struggling to fill open positions, now is the time to start in the field. Infosec expert Dylan Barker shares what you should know to be a malware analyst.
Staying ahead of hackers and the latest malware requires a knowledgeable security team. Malware, especially ransomware, is constantly in the news, as hacker groups use it to attack companies and government agencies. More than 13 million attempted malware attacks on just Linux systems were detected during the first half of 2021.

https://searchsecurity.techtarget.com/feature/Malware-analysis-for-beginners-Getting-started

Click above link to read more.

Back to top

Financial execs say security a top cryptocurrency barrier

Although a majority of financial services executives predict that cryptocurrency will replace or rival fiat currency within the next five to 10 years, they say cybersecurity, regulatory and privacy issues are among the biggest obstacles to its adoption, according to a survey by Deloitte.

The professional services company's "2021 Global Blockchain Survey" of 1,280 executives worldwide found that 81% believe blockchain - the general ledger that supports cryptocurrency - is "broadly scalable" and already mainstream.

https://www.bankinfosecurity.com/financial-execs-say-security-top-cryptocurrency-barrier-a-17378

Click above link to read more.

Back to top

New vulnerability allow hackers to bypass PIN codes on contactless cards from Mastercard & Maestro

The cybersecurity researchers at the Swiss Higher Technical School of Zurich have recently identified a critical vulnerability that allows any threat actor to bypass PIN codes on contactless cards from Mastercard and Maestro.

The most interesting and impactful thing is that on successful exploitation of this security flaw, a threat actor can easily abuse the stolen Mastercard and Maestro cards for contactless payments without having to provide any PIN codes.

https://cybersecuritynews.com/new-vulnerability-in-mastercard-maestro/

Click above link to read more.

Back to top

---

4 emerging ransomware groups take center stage

A series of four emerging ransomware groups have caught the attention of researchers with Palo Alto Networks' Unit 42.

In research published Tuesday, the Unit 42 team profiled four ransomware packages, dubbed AvosLocker, Hive, HelloKitty and LockBit 2.0, that could potentially fill the voids left by the notorious and now-defunct DarkSide and REvil gangs. The emerging quartet is an equal mixture of cybercriminal groups that operate on their own and ransomware as a service (RaaS) operations that create the malware and outsource the actual hacking to others.

Unit 42 expects that all four of the operations will probably be menacing companies for some time.

https://searchsecurity.techtarget.com/news/252505816/Four-emerging-ransomware-groups-take-center-stage

Click above link to read more.

Back to top

ALTDOS hacking group wreaks havoc across Southeast Asia

For the past eight months, a cybercrime group calling itself ALTDOS has been wreaking havoc across Southeast Asia, hacking companies left and right, in order to pilfer their data and ransom it back or sell it on underground forums.

First spotted in December 2020, the group has been linked to intrusions at companies in Bangladesh, Singapore, and Thailand.

According to a series of government cybersecurity alerts and reporting done by *DataBreaches.net*, which has had extensive direct contact and conversations with the group, ALTDOS' modus operandi can only be described as chaotic.

https://therecord.media/altdos-hacking-group-wreaks-havoc-across-southeast-asia/

Click above link to read more.

Back to top

Microsoft may withhold security updates from unsupported Windows 11 PCs

MS would really, really like you to use an officially supported PC.

There are still a lot of question marks about running Windows 11 on unsupported hardware. We know that Microsoft won't go to extraordinary lengths to keep you from running it, we know that the new OS won't be offered to older PCs automatically using Windows Update, and we know that although Microsoft's preferred security settings can degrade performance on older hardware, those settings still won't be the defaults for new installs. But now, Microsoft has added another question to that list: Will unsupported PCs be able to get updates?

https://arstechnica.com/gadgets/2021/08/microsoft-may-withhold-security-updates-from-unsupported-windows-11-pcs/

Click above link to read more.

Back to top

The real victims of mass-crypto hacks that keep happening

Taxi driver Chris is obsessively checking his phone for updates.

"I'm set to lose almost 2,500 euros (£2,100) worth of cryptocurrency coins," he says.
Chris describes himself as "a small crypto-holder from Austria" and is one of many victims of a hack attack on cryptocurrency exchange Liquid Global last week.

The company has insisted it will pay all customers who lost out in the $100m (£72.8m) attack.

But until they get the money back, many customers are worried.

https://www.bbc.com/news/technology-58331959

Click above link to read more.

Back to top

Report: Cybercriminals increasingly targeting outpatient facilities

A report released Thursday by the cybersecurity firm Critical Insight found that bad actors have begun to shift their healthcare targets.

The report used cyberattack data from the first half of 2021 to show that the number of breaches in the beginning of 2021 was higher than any six-month period between 2018 and the first half of 2020.

"Examining breaches caused by hacking reveals something unexpected – attackers breached outpatient facilities and specialty clinics nearly as much as hospitals," read the report.

https://www.healthcareitnews.com/news/report-cyber-criminals-increasingly-targeting-outpatient-facilities

Click above link to read more.

Back to top

There's no escape from Facebook, even if you don't use it

Megan Borovicka joined Facebook in 2013 and then forgot she even had an account. But Facebook never forgot about her.

The 42-year-old Oakland, Calif., lawyer never picked any "friends," posted any status updates, liked any photos or even opened the Facebook app on her phone. Yet over the last decade, Facebook has used an invisible data vacuum to suction up very specific details about her life — from her brand of underwear to where she received her paycheck.

https://www.msn.com/en-us/news/technology/there-s-no-escape-from-facebook-even-if-you-don-t-use-it/ar-AANRTjr

Click above link to read more.

Back to top

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.