July 12, 2022

Challenge yourself with our Travel Security quiz!

This past week's stories:

Northern college first school to adopt national cybersecurity standard
China's cabinet urges greater cybersecurity after mass data leak
The age of collaborative security: what tens of thousands of machines witness
Construction one of most at risk for cyber attacks, says report
Apple's coming security features an answer to government-backed spyware
Latest Marriott breach shows a human error pattern
Swiss Post boots its cybersecurity expertise
Over 70% of small businesses fail to prioritize cybersecurity
Email scams are getting more personal – they even fool cybersecurity experts
Brit cyber security heroes beat Russian hackers' attempts to wreak havoc at Wimbledon
Hospital ransomware concerns rise after payment vendor breach, North Korea threats
Hackers Exploiting Follina Bug to Deploy Rozena Backdoor

Northern college first school to adopt national cybersecurity standard

Many post-secondary institutions are vulnerable to cyber attacks, according to CyberCatch, a firm tasked with getting small- to medium-sized organizations up to date with Canada's new standard for cybersecurity.

Northern College is the first in Canada to sign up for the firm's program, which scans for vulnerabilities, fixes them and teaches staff how to be safer online.

https://northernontario.ctvnews.ca/northern-college-first-school-to-adopt-national-cybersecurity-standard-1.5977426

Click above link to read more.

Back to top

China's cabinet urges greater cybersecurity after mass data leak

China's cabinet stressed the need to bolster information security, following a huge leak of personal data that could be the largest cyber-attack in the country's history.

A State Council meeting led by Premier Li Keqiang emphasized the need "to improve security management provisions, raise protection abilities, protect personal information, privacy and commercial confidentiality in accordance with the law," according to the official Xinhua News Agency. The report didn't directly reference the hack, and other state media agencies have so far been silent about the incident.

https://www.bnnbloomberg.ca/china-s-cabinet-urges-greater-cybersecurity-after-mass-data-leak-1.1788745

Click above link to read more.

Back to top

The age of collaborative security: what tens of thousands of machines witness

What can tens of thousands of machines tell us about illegal hacker activities?

Do you remember that scene in Batman - The Dark Knight, where Batman uses a system that aggregates active sound data from countless mobile phones to create a meta sonar feed of what is going on at any given place?

https://thehackernews.com/2022/07/the-age-of-collaborative-security-what.html

Click above link to read more.

Back to top

Construction one of most at risk for cyber attacks, says report

Construction has been named the fifth most at-risk industry for a cyber attack and is still not doing enough to prevent being hit in the future.

The sector was given a risk score of 39, higher than financial services, energy and government, according to the latest Cyber Readiness Report from insurer Hiscox.

https://www.building.co.uk/news/construction-one-of-most-at-risk-for-cyber-attacks-says-report/5118295.article

Click above link to read more.

Back to top

Apple's coming security features an answer to government-backed spyware

Apple will introduce a new security capability, called Lockdown Mode, based on technology it developed to protect highly vulnerable targets like political activists, journalists and other users who may be the targets of government surveillance.

Apple plans to roll out Lockdown Mode features this fall as part of the iOS 16, iPadOS 16 and macOS Ventura operating system upgrade launches, the company said Wednesday. The feature will limit certain functionalities within the Apple computer and mobile device operating systems to reduce the attack surface that can be targeted.

https://www.cybersecuritydive.com/news/apple-security-Lockdown-Mode-spyware/626761/

Click above link to read more.

Back to top

Latest Marriott breach shows a human error pattern

Marriott International last month suffered its third publicly acknowledged data breach in four years. The hotel chain disclosed the incident after DataBreaches.net reported an unnamed threat actor claimed to have stolen 20 gigabytes of sensitive data.

A previous data breach that began in 2014 and went undetected for four years ultimately impacted 500 million guests. That breach hit the reservation system for Starwood Hotels and Resorts Worldwide two years before Marriott completed its acquisition of the company, forming the largest hotel chain globally.

https://www.cybersecuritydive.com/news/marriott-breach-human-error-pattern/626751/

Click above link to read more.

Back to top

Swiss Post boots its cybersecurity expertise

Swiss Post has acquired a majority shareholding in computer security company Hacknowledge.

According to the company, Swiss Post is constantly under attack from online criminals because it houses critical national infrastructure in partnership with the Swiss economy and its SMEs. Approximately 70 Swiss Post employees currently work in the information security unit to ensure that sensitive customer data in Swiss Post's systems is exchanged safely and reliably with business and private customers. These cybersecurity specialists at Swiss Post identify threats, including persistent ones, and defend both the system and physical and digital services against them. Swiss Post's team successfully repels over 100 targeted hacker attacks every month, over 280 waves of phishing against customers and around 10 million spam and phishing emails each month.

https://www.parcelandpostaltechnologyinternational.com/news/it-systems/swiss-post-boosts-its-cybersecurity-expertise.html

Click above link to read more.

Back to top

Over 70% of small businesses fail to prioritize cybersecurity

Cybersecurity threats are a ticking timebomb for many companies, and yet small businesses don't see it as a main budget priority, an exclusive Tech.co report has revealed.

With cyberattacks on the rise and the average cost of an attack in the millions, safeguarding against issues such as data breaches and ransomware should be a number one concern for businesses of all sizes.

https://tech.co/news/small-businesses-fail-cybersecurity

Click above link to read more.

Back to top

Email scams are getting more personal – they even fool cybersecurity experts

We all like to think we're immune to scams. We scoff at emails from an unknown sender offering us £2 million, in exchange for our bank details. But the game has changed and con artists have developed new, chilling tactics. They are taking the personal approach and scouring the internet for all the details they can find about us.

Scammers are getting so good at it that even cybersecurity experts are taken in.

https://uk.news.yahoo.com/email-scams-getting-more-personal-142624194.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAD_firkIEGBGcozHd19XpJFmlr24t20Ta9oZ-UquHORZYr02eG30deKYnvFjGbxyIofl7tSF-rfQyn9wvsxiEsAtH3TKIqLIqnqmn-OYfV-JJ8T73Pzw-gKySKe6bxlh1lf3f_zzjdDp8PlLVVEdHNryLSSQEnESk1axhtG-mfgr

Click above link to read more.

Back to top

Brit cyber security heroes beat Russian hackers' attempts to wreak havoc at Wimbledon

Brit security experts have defeated Russian hackers' attempts to cause chaos at Wimbledon.

Putin-backed spies have tried disrupt the tournament after Russian players were banned following the invasion of Ukraine.

https://www.dailystar.co.uk/news/latest-news/brit-cyber-security-heroes-beat-27438128

Click above link to read more.

Back to top

Hospital ransomware concerns rise after payment vendor breach, North Korea threats

The threat of ransomware is rising for U.S. hospitals, their partners and the patients whose data they collect.

A recently disclosed ransomware attack at a payment vendor could have exposed patient data from more than 650 healthcare providers, including those at Arizona-based nonprofit Banner Health and Nevada physician network Renown Health.

https://www.cybersecuritydive.com/news/Personal-finance-company-breach-Maui-ransomware-healthcare/626792/

Click above link to read more.

Back to top

Hackers exploiting Follina bug to deploy Rozena backdoor

A newly observed phishing campaign is leveraging the recently disclosed Follina security vulnerability to distribute a previously undocumented backdoor on Windows systems. "Rozena is a backdoor malware that is capable of injecting a remote shell connection back to the attacker's machine," Fortinet FortiGuard Labs researcher Cara Lin said in a report this week.

https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html

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.