July 19, 2022

Challenge yourself with our Travel Security quiz!

This past week's stories:

- **Exclusive: Northern Credit Union target of cybersecurity breach**
- **University of Windsor restores 'vast majority' of systems after security breach**
- **Microsoft Teams security vulnerability left users open to XSS via flawed stickers feature**
- **Hackers impersonate cybersecurity firms in callback phishing attacks**
- **Ransomware attacks surge in education sector**
- **Cyberinsurers looking for new risk assessment models**
- **Disaster recovery planning: A successful framework for strategy and execution**
- **1.9m patient records exposed in healthcare debt collector ransomware attack**
- **NFT artist DeeKay Twitter hacked, phishing attack steals $150k**
- **FBI warns fake cryptocurrency apps are defrauding investors**
- **The Nigerian Prince has evolved: email scams now even fool cybersecurity experts**
- **Huge phishing campaign evades MFA, leads to business email fraud: Microsoft**

Exclusive: Northern Credit Union target of cybersecurity breach

The largest credit union in Northern Ontario was hit by a major cybersecurity incident that exposed personal information about an undisclosed number of customers, Village Media has learned.

In a prepared statement issued Monday night, Northern Credit Union confirmed that a recent “online security incident” at a third-party contractor targeted confidential client information—and that “impacted members will be receiving written notice” in the coming days.

https://www.sootoday.com/local-news/exclusive-northern-credit-union-target-of-cybersecurity-breach-5597248

Click above link to read more.

Back to top

University of Windsor restores 'vast majority' of systems after security breach

The University of Windsor confirms it has restored the "vast majority" of its systems following a cyber security breach that temporarily shut down its website last month.

On June 22, the university issued a notice that its website and other services were temporarily unavailable. On Thursday, a spokesperson said in an emailed statement to CBC News that a full investigation is underway with a team of external cyber security experts to better understand what happened.

https://www.cbc.ca/news/canada/windsor/uwindsor-restores-systems-1.6521329

Click above link to read more.

Back to top

Microsoft Teams security vulnerability left users open to XSS via flawed stickers feature

A security researcher has found that attackers could abuse the popular sticker feature in Microsoft Teams to conduct cross-site scripting (XSS) attacks.

Microsoft Teams, alongside comparable teleconferencing services including Zoom, have experienced a surge in popularity over the past few years.

https://portswigger.net/daily-swig/microsoft-teams-security-vulnerability-left-users-open-to-xss-via-flawed-stickers-feature

Click above link to read more.

Back to top

Hackers impersonate cybersecurity firms in callback phishing attacks

Hackers are impersonating well-known cybersecurity companies, such as CrowdStrike, in callback phishing emails to gain initial access to corporate networks.

Most phishing campaigns embed links to landing pages that steal login credentials or emails that include malicious attachments to install malware.

https://www.bleepingcomputer.com/news/security/hackers-impersonate-cybersecurity-firms-in-callback-phishing-attacks/

Click above link to read more.

Back to top

Ransomware attacks surge in education sector

The education sector got hit with even more ransomware attacks in 2021, impacting almost two-thirds of higher education organizations, Sophos concluded in a new survey.

Ransomware attacks hit more than half of the lower-education organizations surveyed and almost two-thirds of higher education institutions.

https://www.cybersecuritydive.com/news/ransomware-surge-education/627234/

Click above link to read more.

Back to top

Cyberinsurers looking for new risk assessment models

The ever-increasing number of ransomware attacks has created a quandary for those in the cyberinsurance industry. With premiums skyrocketing, coverage being limited and insurers struggling to earn revenue because of the cost and growing number of claims, something has to give. Due to these factors, organizations are searching for new methods of risk assessment to better evaluate the market for cyberinsurance, per Panaseer's "2022 Cyber Insurance Market Trends Report".

Four hundred global insurers were surveyed as part of the report, in order to discover what issues the market is facing and potential solutions to achieve a healthy cyberinsurance market.

https://www.techrepublic.com/article/cyberinsurers-looking-for-new-risk-assessment-models/

Click above link to read more.

Back to top

Disaster recovery planning: A successful framework for strategy and execution

The rise in cyber incidents is set to continue on its meteoric trajectory over the next decade. Ransomware attacks on a business, consumer, or a device are anticipated to take place every two seconds by 2031 -- a worrying escalation from every 11 seconds in 2021. And by 2025, damages are projected to reach a staggering $15 trillion annually, up from $3 trillion in 2015, according to Cybersecurity Ventures.

At the same time, users demand better performance and user experience year-after-year, and the subsequently increased threat landscape poses real challenges in connectivity and data security. 'Insider threat' also poses a considerable risk, with 80 percent of breaches involving privileged credentials misuse or abuse and malicious insider activity from recent employees.

https://betanews.com/2022/07/14/disaster-recovery-planning/

Click above link to read more.

Back to top

1.9m patient records exposed in healthcare debt collector ransomware attack

Professional Finance Company, a Colorado-based debt collector whose customers include hundreds of US hospitals, medical clinics, and dental groups, recently disclosed that private data – including names, addresses, social security numbers, and health records – for more than 1.9 million people was exposed during a ransomware infection.

In a notice [PDF] posted on its website, PFC said it "detected and stopped a sophisticated ransomware attack" on February 26 this year, during which criminals accessed files containing data from more than 650 healthcare providers [PDF]. The company said it notified the affected medical centers around May 5, and is mailing letters to individuals whose data may have been stolen during the intrusion.

https://www.theregister.com/2022/07/13/19m_patients_medical_data_exposed/

Click above link to read more.

Back to top

NFT artist DeeKay Twitter hacked, phishing attack steals $150k

Non-fungible tokens (NFTs) have exploded in popularity over the past year. However, amid this popularity, there has also been a rising streak of hacking attacks where NFT investors have suffered massive losses.

DeeKay Kwon, a renowned NFT animator, has suffered an exploit of their Twitter account. The hacked account was used to conduct a phishing campaign on Friday.

https://www.business2community.com/nft-news/nft-artist-deekay-twitter-hacked-phishing-attack-steals-150k-02524455

Click above link to read more.

Back to top

FBI warns fake cryptocurrency apps are defrauding investors

Cybercriminals are creating fake cryptocurrency apps in an effort to defraud investors, according to a Monday warning from the FBI. The bureau's cyber division identified 244 victims that have been swindled by fraudulent apps, accounting for an estimated loss of $42.7 million.

The fake cryptocurrency apps have used the names, logos and other identifying information of legitimate apps, said the FBI. These fake apps have been seen contacting crypto investors and falsely claiming to offer real services to push people to download them.

https://www.cnet.com/personal-finance/crypto/fbi-warns-fake-cryptocurrency-apps-are-defrauding-investors/

Click above link to read more.

Back to top

The Nigerian Prince has evolved: email scams now 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://thenextweb.com/news/the-nigerian-prince-has-evolved-email-scams-now-even-fool-cybersecurity-experts

Click above link to read more.

Back to top

Huge phishing campaign evades MFA, leads to business email fraud: Microsoft

A large phishing campaign is focusing on organizations using Microsoft Office 365, tricking victims into logging into a spoofed Office online authentication page to steal their credentials and ultimately conduct business email compromise (BEC) scams.

The warning comes from Microsoft, which says the heart of the attack are what it calls adversary-in-the-middle (AiTM) phishing sites. These are impersonated websites that deploy a proxy server between a target user and the website the user wants to visit.

https://financialpost.com/technology/huge-phishing-campaign-evades-mfa-leads-to-business-email-fraud-microsoft

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer