March 29, 2022

Challenge yourself with our Fraud Prevention quiz!

This past week's stories:

- A majority of small businesses want to improve their cybersecurity within the next year
- Making ransom payment no assurance of getting data back: Telus
- Experts call for better IT security after MLA admits he hacked Alberta vaccine records website
- Hundreds of companies potentially hit by Okta hack
- Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal
- Google issues emergency security update for 3.2 billion Chrome users—attacks underway
- Four Russian government employees charged for hacking critical infrastructure worldwide
- Email phishing scams prey on tax season, crisis in Ukraine
- Health data breaches swell in 2021 amid hacking surge, POLITICO analysis finds
- FCC warns that Kaspersky poses national security risk
- Ukraine war: Major internet provider suffers cyber attack

A majority of small businesses want to improve their cybersecurity within the next year

Seven in ten (72%) small business owners are more concerned than ever about cyberattacks on their business, according to a new joint survey from the Canadian Federation of Independent Business (CFIB) and Mastercard. One in four (24%) small business owners report an increase in cyberattack attempts against their business in the last year.

"The last two years saw a huge number of small businesses increase the amount of business they are doing online, which has many benefits but also introduces new risks," said Laura Jones, CFIB executive vice-president. "It's critical to make it easy for business owners to protect themselves in this new environment."

https://www.newswire.ca/news-releases/a-majority-of-small-businesses-want-to-improve-their-cybersecurity-within-the-next-year-870505869.html

Click above link to read more.

Back to top

Making ransom payment no assurance of getting data back: Telus

Almost half of surveyed Canadian organizations that suffered a recent ransomware attack paid in the hopes of getting get access of their data back, according to a study by one of the country's biggest telcos. That hope, however, was only realized for just under half of them.

The message, suggests the study by Telus, is that the odds of getting your data back from a ransomware attack are less than 50/50.

It found that 67 per cent of the 463 respondents to the survey said their organization had been hit by ransomware. Of that number, 44 per cent said their organization had paid a ransom. And of them, fewer than half – 42 per cent, said they got full access to their data back. Forty-nine per cent said they only got partial access back. Seven per cent who paid said they never got their data back.

https://www.itbusiness.ca/news/making-ransom-payment-no-assurance-of-getting-data-back-telus/120933

Click above link to read more.

Back to top

Experts call for better IT security after MLA admits he hacked Alberta vaccine records website

An Edmonton MLA's intentional breach of Alberta's COVID-19 vaccine records website should motivate the province to better safeguard its IT systems against hackers, cybersecurity experts say.

Thomas Dang described his hack last September in a report he posted to his website Tuesday.

He said he used Premier Jason Kenney's birthdate and a simple coding program to access a stranger's vaccine record.

https://www.cbc.ca/news/canada/edmonton/thomas-dang-hack-breach-cybersecurity-alberta-1.6396428

Click above link to read more.

Back to top

Hundreds of companies potentially hit by Okta hack

Hundreds of organisations that rely on Okta to provide access to their networks may have been affected by a cyber-attack on the company.

Okta said the "worst case" was 366 of its clients had been affected and their "data may have been viewed or acted upon" - its shares fell 9% on the news.

https://www.bbc.com/news/technology-60849687

Click above link to read more.

Back to top

Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal

A 16-year-old from Oxford has been accused of being one of the leaders of cyber-crime gang Lapsus$. The teenager, who is alleged to have amassed a $14m (£10.6m) fortune from hacking, has been named by rival hackers and researchers.

https://www.bbc.com/news/technology-60864283

Click above link to read more.

Back to top

Google issues emergency security update for 3.2 billion Chrome users—attacks underway

Google has issued an emergency security update for all Chrome users as it confirms that attackers are already exploiting a high severity zero-day vulnerability.

The emergency update to version 99.0.4844.84 of Chrome is highly unusual in that it addresses just a single security vulnerability. A fact that only goes to emphasize how serious this one is.

https://www.forbes.com/sites/daveywinder/2022/03/26/google-confirms-emergency-security-update-for-32-billion-chrome-users-attacks-underway/?sh=7e223752aaa2

Click above link to read more.

Back to top

Four Russian government employees charged for hacking critical infrastructure worldwide

Two indictments were unsealed today by the Department of Justice, accusing four defendants belonging to Russian nationals who operated for the Russian government. They were charged for attempting, supporting, and carrying out computer intrusions that specifically aimed at the global energy sector in two separate conspiracies between 2012 and 2018. In total, thousands of computers in hundreds of firms and organizations in approximately 135 countries were targeted in these hacking efforts.

https://cybersecuritynews.com/four-russian-government-employees-charged/

Click above link to read more.

Back to top

Email phishing scams prey on tax season, crisis in Ukraine

Researchers on Wednesday reported on phishing emails tied to current events, especially the Russia-Ukraine conflict and the upcoming tax season deadline next month.

In a blog post, FortiGuard researchers detailed two recent tax season scams and pleas to send money to help Ukrainian refugees.

https://www.scmagazine.com/news/email-security/email-phishing-scams-prey-on-tax-season-crisis-in-ukraine

Click above link to read more.

Back to top

Health data breaches swell in 2021 amid hacking surge, POLITICO analysis finds

Nearly 50 million people in the U.S. had their sensitive health data breached in 2021, a threefold increase in three years, according to a POLITICO analysis of the latest HHS data.

Health care organizations including providers and insurers in every state except South Dakota reported such incidents last year. About half of states and Washington, D.C., saw more than 1 in 10 of their residents directly impacted by unauthorized access to their health information, according to the analysis. And hacking accounted for nearly 75 percent of all such breaches — up from 35 percent in 2016.

https://www.politico.com/news/2022/03/23/health-data-breaches-2021-hacking-surge-politico-00019283

Click above link to read more.

Back to top

FCC warns that Kaspersky poses national security risk

The FCC has added Kaspersky, China Mobile, and China Telecom to the list of companies affected by the Secure and Trusted Communications Networks Act of 2019.

The so-called Covered List includes companies "that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons," the commission explains, typically because of their connections to foreign governments.

https://www.pcmag.com/news/fcc-warns-that-kaspersky-poses-national-security-risk

Click above link to read more.

Back to top

Ukraine war: Major internet provider suffers cyber-attack

Ukraine's national telecoms operator Ukrtelecom is restoring internet services after driving back a major cyber-attack.

The company said it restricted customer access to protect military users and critical infrastructure.

https://www.bbc.com/news/60854881

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