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

October 11, 2022

Challenge yourself with our Cyber Security Awareness Month Quiz!

Take the Cyber Security Awareness Month Challenges!

This past week's stories:

🍁 **Canadian ransomware hacker sentenced to 20 years in U.S. prison**

🍁 **Rural Saskatchewan needs to address cyber security threats: expert**

Former Uber Security Chief found guilty of data breach coverup

US hospital chain CommonSpirit Health says 'IT security issue' is disrupting services

FBI warns of disinformation threats before 2022 midterm elections

Pro-Russian hackers claim responsibility for knocking U.S. airport websites offline

Hackers can use 'App Mode' in Chromium Browsers' for stealth phishing attacks

Toyota discloses data leak after access key exposed on GitHub

Optus cyber attack: Man arrested for alleged data breach scam

Protests in Iran: State-run live TV hacked by protesters

Meta says it detected more than 400 malware apps targeting users' Facebook login information

Lloyd's, after proactively taking systems offline, finds no evidence of compromise

---

Canadian ransomware hacker sentenced to 20 years in U.S. prison

A former Canadian government employee turned ransomware hacker has been sentenced to a 20-year prison term in the United States in what a federal court judge called "the worst case he's ever seen."

Visibly outraged, Justice William F. Jung described Sébastien Vachon-Desjardins of Gatineau, Que., as "Jesse James meets the 21st century," referring to the notorious 19th century American outlaw as he handed down his decision in Tampa, Fla., on Tuesday.

https://www.cbc.ca/news/canada/ottawa/ransomeware-hacker-vachon-desjardins-sentenced-1.6606274

Click above link to read more.

Back to top

Rural Saskatchewan needs to address cyber security threats: expert

In 2022, it is nearly impossible to not have a digital footprint. Work, school and social media have all been brought into the digital age, and with it comes a focus on cyber security.

October marks cyber security awareness month in Canada, and one expert believes local governments need to take the time to review their defenses, especially in rural areas.

https://globalnews.ca/news/9188241/rural-saskatchewan-needs-to-address-cyber-security-threats-expert/

Click above link to read more.

Back to top

Former Uber Security Chief found guilty of data breach coverup

A U.S. federal court jury has found former Uber Chief Security Officer Joseph Sullivan guilty of not disclosing a 2016 breach of customer and driver records to regulators and attempting to cover up the incident.

Sullivan has been convicted on two counts: One for obstructing justice by not reporting the incident and another for misprision. He faces a maximum of five years in prison for the obstruction charge, and a maximum of three years for the latter.

https://thehackernews.com/2022/10/former-uber-security-chief-found-guilty.html

Click above link to read more.

Back to top

US hospital chain CommonSpirit Health says ‘IT security issue’ is disrupting services

CommonSpirit, the second-largest nonprofit hospital chain in the U.S., has confirmed a cybersecurity incident that is disrupting medical services across the country.

In a brief statement, Chicago-based CommonSpirit said the “IT security issue” is impacting some of CommonSpirit’s facilities and some patient appointments have been rescheduled as a result.

https://techcrunch.com/2022/10/05/us-hospital-chain-commonspirit-health-says-it-security-issue-is-disrupting-services/

Click above link to read more.

Back to top

FBI warns of disinformation threats before 2022 midterm elections

The Federal Bureau of Investigation (FBI) warned today of foreign influence operations that might spread disinformation to affect the results of this year's midterm elections.

The federal law enforcement agency warned that foreign actors are actively spreading election infrastructure disinformation to manipulate public opinion, discredit the electoral process, sow discord, and encourage a lack of trust in democratic processes and institutions.

https://www.bleepingcomputer.com/news/security/fbi-warns-of-disinformation-threats-before-2022-midterm-elections/

Click above link to read more.

Back to top

Pro-Russian hackers claim responsibility for knocking U.S. airport websites offline

A pro-Russian hacker group is taking credit for temporarily taking down several U.S. airport websites on Monday, though there appeared to be no impact on flight operations.

The cyberattacks claimed by Killnet impacted the websites for Los Angeles International, Chicago O'Hare, and Hartsfield-Jackson International in Atlanta, among others.

https://www.npr.org/2022/10/10/1127902795/airport-killnet-cyberattack-hacker-russia

Click above link to read more.

Back to top

Hackers can use 'App Mode' in Chromium Browsers' for stealth phishing attacks

In what's a new phishing technique, it has been demonstrated that the Application Mode feature in Chromium-based web browsers can be abused to create "realistic desktop phishing applications."

Application Mode is designed to offer native-like experiences in a manner that causes the website to be launched in a separate browser window, while also displaying the website's favicon and hiding the address bar.

https://thehackernews.com/2022/10/hackers-can-use-app-mode-in-chromium.html

Click above link to read more.

Back to top

Toyota discloses data leak after access key exposed on GitHub

Toyota Motor Corporation is warning that customers' personal information may have been exposed after an access key was publicly available on GitHub for almost five years.

Toyota T-Connect is the automaker's official connectivity app that allows owners of Toyota cars to link their smartphone with the vehicle's infotainment system for phone calls, music, navigation, notifications integration, driving data, engine status, fuel consumption, and more.

https://www.bleepingcomputer.com/news/security/toyota-discloses-data-leak-after-access-key-exposed-on-github/

Click above link to read more.

Back to top

Optus cyber attack: Man arrested for alleged data breach scam

A Sydney man has been charged for allegedly attempting to use stolen Optus customer data in a text message blackmail scam.

The Australian Federal Police said the man was not suspected of being the individual responsible for the Optus breach, but allegedly tried to financially benefit from stolen data uploaded to an online forum.

https://www.sbs.com.au/news/article/optus-cyber-attack-man-arrested-for-alleged-data-breach-scam/gepdxq7s9

Click above link to read more.

Back to top

Protests in Iran: State-run live TV hacked by protesters

Iran's state-run broadcaster was apparently hacked on air Saturday, with a news bulletin interrupted by a protest against the country's leader.

A mask appeared on the screen, followed by an image of Supreme Leader Ali Khamenei with flames around him.

https://www.bbc.com/news/world-middle-east-63188795

Click above link to read more.

Back to top

Meta says it detected more than 400 malware apps targeting users' Facebook login information

Facebook's parent company Meta said on Friday that it has detected more than 400 malware apps this year designed to steal users' Facebook login information.

The apps, which were listed on the Google Play Store and Apple App Store, were disguised to look like fun or useful apps, from photo editors to VPNs to fitness trackers, Meta said in a press release.

https://thehill.com/policy/technology/3679651-meta-says-it-detected-more-than-400-malware-apps-targeting-users-facebook-login-information/

Click above link to read more.

Back to top

Lloyd's, after proactively taking systems offline, finds no evidence of compromise

Lloyd's of London will restore full network service by Wednesday after an investigation into a security incident last week found no evidence of compromise.

"The investigation has concluded that no evidence of any compromise was found and as such Lloyd's has been advised that its network services can now be restored," a Lloyd's spokesperson said in an emailed statement to Cybersecurity Dive.

https://www.cybersecuritydive.com/news/lloyds-security-incident/633720/

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

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer