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

December 20, 2022

Challenge yourself with our Holiday Scam Security Quiz!

Here are the top Security News Digest stories from 2022.

This is the last Security News Digest of 2022. Happy Holidays - see you in 2023!

This past year's stories:

🍁 **Threat of Russian-backed cyber attacks growing amid Ukraine tensions, Canada's cybersecurity agency warns** (January)

🍁 **Don't forget your burner phone: Why cybersecurity in China is an Olympic event in itself** (February)

🍁 **Russia cyber warfare is a problem for everyone, experts warn** (March)

🍁 **Ransomware attacks target more than 4 in 5 Canadian businesses** (April)

State of Cybersecurity Report 2022 names ransomware and nation-state attacks as biggest threats (May)

45% of cybersecurity pros are considering quitting the industry due to stress (June)

Uber admits covering up 2016 hacking, avoids prosecution in U.S. settlement

(July)

Cyber attacks escalate in Ukraine-Russia conflict; attackers living-off-the-land

(August)

Australia phones cyber-attack exposes personal data (September)

EnergyAustralia hacked after data stolen from Medibank, Optus

(October)

🍁 **Beware of gift card fraud — don't let it hijack your perfect present** (November)

The biggest data breaches and leaks of 2022 (December)

Threat of Russian-backed cyber attacks growing amid Ukraine tensions, Canada's cybersecurity agency warns

Canada's digital cybersecurity agency is warning the country's "critical infrastructure" providers to be increasingly weary of attacks from Russia-backed hackers as tensions between the two countries increase over the threat of war in Ukraine.

Experts say those attacks could come in a range of forms, from a "widespread ransomware attack" to a "single, carefully focused" attempt to significantly impact core infrastructure.

https://nationalpost.com/news/politics/threat-of-russian-backed-cyber-attacks-growing-amid-ukraine-tensions-canadian-cybersecurity-agency-warns

Click above link to read more.

Back to top

Don't forget your burner phone: Why cybersecurity in China is an Olympic event in itself

For Canadian athletes, staff and media, and their counterparts around the world, braving a hostile cyber environment is the part of the price of admission to the 2022 Winter Olympics.

At the top of the packing list for these Olympics? A virtual private network, or VPN. From Switzerland to Great Britain, prominent National Olympic Committees have equipped team members with burner phones, and cybersecurity briefings have been part of their preparations for the Games.

https://nationalpost.com/sports/olympics/2022-winter-olympics-china-cybersecurity-burner-phones

Click above link to read more.

Back to top

Russia cyber warfare is a problem for everyone, experts warn

Canada is reviewing its cyber defences to make sure it's secured against potential cyberattacks from an increasingly aggressive Russia. Experts say you should do the same at home.

While cyberattacks are already pummelling Ukraine, they could affect the average Canadian in a number of ways, too. They could hit your pocketbook, permanently wipe important files or sentimental photos from your electronics. In severe instances, they could disrupt critical infrastructure we rely on.

https://globalnews.ca/news/8650575/russia-ukraine-canada-cyberattack-cyberspace-cybersecurity/

Click above link to read more.

Back to top

Ransomware attacks target more than 4 in 5 Canadian businesses

In March 2021, tech firm Acer was faced with paying one of the largest ransomware demands known to date: a price tag of US$50 million for the return of the global computer manufacturer's stolen data.

The dramatic extortion by cybercriminals captured headlines. But ransomware attacks happen every day to every size of company.

https://www.theglobeandmail.com/business/adv/article-ransomware-attacks-target-more-than-4-in-5-canadian-businesses/

Click above link to read more.

Back to top

State of Cybersecurity Report 2022 names ransomware and nation-state attacks as biggest threats

Ransomware is the biggest concern for cybersecurity professionals, according to results of the Infosecurity Group's 2022 State of Cybersecurity Report, produced by Infosecurity Europe and *Infosecurity* Magazine.

This attack vector was voted as the biggest cybersecurity trend (28%) by the survey respondents (including CISOs, CTOs, CIOs and academics), marking a significant change from the previous report in 2020, where ransomware did not break the top three. This follows surging ransomware incidents in 2021, with ransom demands and payments growing significantly last year. A number of these attacks have also impacted critical industries, for example, taking down the US' largest fuel pipeline.

https://www.infosecurity-magazine.com/news/2022-state-industry-report/

Click above link to read more.

[Back to top](#)

45% of cybersecurity pros are considering quitting the industry due to stress

Deep Instinct released the third edition of its annual Voice of SecOps Report, focused on the increasing and unsustainable stress levels among 1,000 C-suite and senior cybersecurity professionals across all industries and roles. The research found that 45% of respondents have considered quitting the industry due to stress, with the primary issues being an unrelenting threat from ransomware and the expectations to always be on call or available.

https://www.helpnetsecurity.com/2022/06/13/cybersecurity-professionals-stress-levels/

Click above link to read more.

[Back to top](#)

Uber admits covering up 2016 hacking, avoids prosecution in U.S. settlement

Uber Technologies Inc (UBER.N) on Friday accepted responsibility for covering up a 2016 data breach that affected 57 million passengers and drivers, as part of a settlement with U.S. prosecutors to avoid criminal charges.

In entering a non-prosecution agreement, Uber admitted that its personnel failed to report the November 2016 hacking to the U.S. Federal Trade Commission, even though the agency had been investigating the ride-sharing company's data security.

https://www.reuters.com/business/autos-transportation/uber-enters-non-prosecution-agreement-admits-covering-up-2016-data-breach-2022-07-22/

Click above link to read more.

[Back to top](#)

Cyber attacks escalate in Ukraine-Russia conflict; attackers living-off-the-land

Cyberwar or cyberattacks has been playing a crucial role in the Ukraine-Russia war. It is opening a new dimension of modern warfare.

The “special operation” in Ukraine continues to characterize the threat landscape from a Hacktivism and Cyber Espionage standpoint. Multiple targes in Lithuania and Latvia (and in the United States as well) were hit with DDos attacks launched by pro-Russia attackers, while on the opposite front, the IT Army of Ukraine launched a wave of attacks against at least 80 Russian cinemas. The Russian Space Institute was also hit by a separate operation.

https://autofintechs.com/cyberattacks-escalate-in-ukraine-russia-conflict-attackers-living-off-the-land/

Click above link to read more.

Back to top

Australia phones cyber-attack exposes personal data

Australia's second-largest telecommunications company, Optus, has reported a cyber-attack.

The breach exposed customers' names, dates of birth, phone numbers and email addresses.

https://www.bbc.com/news/technology-62996101

Click above link to read more.

Back to top

EnergyAustralia hacked after data stolen from Medibank, Optus

EnergyAustralia has become the latest company to fall victim to a cyber attack, with hundreds of people impacted.

The electricity company said the breach involved unauthorised access of the online platform My Account, exposing the data of 323 residential and small business customers.

https://www.news.com.au/technology/online/hacking/energy-australia-hacked-after-data-stolen-from-medibank-optus/news-story/7fd668f480e8ab0b8c227fd772ed530f

Click above link to read more.

Back to top

Beware of gift card fraud — don't let it hijack your perfect present

The past few years have been a wild ride for online shoppers, and the 2022 holiday season probably won't be much different. Experts are expecting aftershocks from the notorious supply chain crisis — namely inflation, understaffing and inventory uncertainties — to impact holiday shopping again.

Smart consumers are ahead of the game. A recent survey by RetailMeNot revealed that more than 50% of holiday shoppers plan on circumventing these issues by going the gift card route this year. The only problem? The very real dangers of gift card fraud.

https://ca.news.yahoo.com/gift-card-fraud-malwarebytes-154531275.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAB2pusM3fH8NXqtO6qt1IwWKfr3vAt3qDyi1R-CgqsCLt4MmLmGP4YWu944e-Eqykd2evZ3nsiAqjMipmWWulAsIFVp82mgUgJjcssPhw-R5yAoPe3ywtO53AkbXGiE0dArHbHbdiBUXjAFDAr4eDktulOH_9c1iZhh8vUg0juj4

Click above link to read more.

The biggest data breaches and leaks of 2022

More than 4,100 publicly disclosed data breaches occurred in 2022 equating to approximately 22 billion records being exposed. Cyber security publication Security Magazine reported that the figures for 2022 are expected to exceed this figure by as much as five percent.

In this article, we reveal which data breaches and leaks and the phishing, malware and cyber attacks ranked among our top ten most-read cyber security news stories of 2022.

https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022

Click above link to read more.

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer