March 7, 2023

Challenge yourself with our Fraud Prevention Quiz!

This past week's stories:

- **B.C. joins growing number of governments with employee TikTok ban**
- **What does TikTok know about you? What should you know about it?**
- **Ransomware group behind Indigo hack says it released stolen employee data, but nothing has appeared yet**
- **Ransomware Attack Hits US Marshals Service**
- **Hackers exploit containerized environments to steals proprietary data and software**
- **WH Smith staff data hit by cyber-attack**
- **LastPass Reveals Second Attack Resulting in Breach of Encrypted Password Vaults**
- **BetterHelp absorbed sensitive user health data, then gave it to Facebook**
- **Acer confirms breach after 160GB of data for sale on hacking forum**
- **Cybercriminals Targeting Law Firms with GootLoader and FakeUpdates Malware**
- **Police arrest suspected members of prolific DoppelPaymer ransomware gang**
- **Nine in 10 enterprises fell victim to successful phishing in 2022**

B.C. joins growing number of governments with employee TikTok ban

The B.C. government has joined an international trend and banned the TikTok social media app from its employees' work phones "out of an abundance of caution" to avert possible cybersecurity threats.

“It’s not clear what is driving this (ban), is it fear, is it ideology or is it empirical evidence,” said Peter Chow-White, a communications professor at SFU.

https://vancouversun.com/news/local-news/bc-joins-growing-number-of-governments-with-employee-tiktok-ban

Click above link to read more.

Back to top

What does TikTok know about you? What should you know about it?

One of the hottest TikTok trends right now seemingly is Western governments banning the immensely popular app from their employees' phones and launching probes into its data collection practices.

This week, Canada joined the U.S. and the European Union in prohibiting the social media app on government-issued devices. Other Canadian jurisdictions and institutions are considering similar bans.
https://www.cbc.ca/news/canada/tiktok-data-collection-privacy-1.6763626

Click above link to read more.

Back to top

Ransomware group behind Indigo hack says it released stolen employee data, but nothing has appeared yet

A deadline for Indigo Books to pay a ransom or risk the public release of employee personal information has come and gone without the stolen data being made public, but a privacy advocate and cybersecurity analyst both say this doesn't mean there's any less risk for Canadians affected by the data breach.

On Wednesday night, Canada's largest bookstore chain said it would not agree to payment demands from an online group claiming affiliation with ransomware site LockBit, because it could not guarantee the money wouldn't "end up in the hands of terrorists."

https://www.cbc.ca/news/business/ransomware-indigo-data-release-1.6766328

Click above link to read more.

Back to top

Ransomware Attack Hits US Marshals Service

The US Marshals Service (USMS) has confirmed falling victim to a ransomware attack that resulted in the compromise of sensitive law enforcement information.

A federal law enforcement agency within the Department of Justice, USMS supports the federal justice system by tracking down fugitives, protecting government witnesses and their families, executing federal court orders, and more.

https://www.securityweek.com/ransomware-attack-hits-us-marshals-service/

Click above link to read more.

Back to top

Hackers exploit containerized environments to steals proprietary data and software

A sophisticated attack campaign dubbed SCARLETEEL is targeting containerized environments to perpetrate theft of proprietary data and software.

https://thehackernews.com/2023/03/hackers-exploit-containerized.html

Click above link to read more.

Back to top

WH Smith staff data hit by cyber-attack

High Street retailer WH Smith has been hit by a cyber-attack, with hackers accessing some of its workers' data.

https://www.bbc.com/news/business-64823923

Click above link to read more.

Back to top

LastPass Reveals Second Attack Resulting in Breach of Encrypted Password Vaults

LastPass, which in December 2022 disclosed a severe data breach that allowed threat actors to access encrypted password vaults, said it happened as a result of the same adversary launching a second attack on its systems.

The company said one of its DevOps engineers had their personal home computer hacked and infected with a keylogger as part of a sustained cyber attack that exfiltrated sensitive data from its Amazon AWS cloud storage servers.

https://thehackernews.com/2023/02/lastpass-reveals-second-attack.html

Click above link to read more.

Back to top

BetterHelp absorbed sensitive user health data, then gave it to Facebook

In the press release, the US Federal Trade Commission (FTC) says BetterHelp users were told by the company that their answers in the provided questionnaire "will stay private between you and your counselor."

This wasn't the case, though. The FTC alleges BetterHelp passed its users' mental health information to social media companies such as Facebook or Snapchat. The latter, of course, find such data useful in order to make money through targeted ads based on it.

https://cybernews.com/news/betterhelp-user-data-facebook/

Click above link to read more.

Back to top

Acer confirms breach after 160GB of data for sale on hacking forum

Taiwanese computer giant Acer confirmed that it suffered a data breach after threat actors hacked a server hosting private documents used by repair technicians.

However, the company says the results of its investigation so far do not indicate that this security incident has impacted customer data.

https://www.bleepingcomputer.com/news/security/acer-confirms-breach-after-160gb-of-data-for-sale-on-hacking-forum/

Click above link to read more.

Back to top

Cybercriminals Targeting Law Firms with GootLoader and FakeUpdates Malware

Six different law firms were targeted in January and February 2023 as part of two disparate threat campaigns distributing GootLoader and FakeUpdates (aka SocGholish) malware strains.

GootLoader, active since late 2020, is a first-stage downloader that's capable of delivering a wide range of secondary payloads such as Cobalt Strike and ransomware.

https://thehackernews.com/2023/03/cybercriminals-targeting-law-firms-with.html

Click above link to read more.

Back to top

Police arrest suspected members of prolific DoppelPaymer ransomware gang

An international law enforcement operation has led to the arrests of suspected core members of the prolific DoppelPaymer ransomware operation.

German and Ukrainian police, working with law enforcement partners including Europol and the U.S. Federal Bureau of Investigation (FBI), said they took action last month against the notorious group blamed for numerous large-scale attacks since 2019.

https://techcrunch.com/2023/03/06/police-arrest-suspected-members-of-prolific-doppelpaymer-ransomware-gang/

Click above link to read more.

Back to top

Nine in 10 enterprises fell victim to successful phishing in 2022

Email security company Egress finds that 92% of organisations have fallen victim to a successful phishing attack in their Microsoft 365 environments over the past year, with a further 98% of cyber security managers expressing frustration with secure email gateway (SEG) technologies.

According to Egress' Email security risks report 2023 – which investigated both inbound phishing attacks and outbound data loss and exfiltration – 58% of cyber security managers said traditional SEG technologies were not effective in stopping employees from accidentally emailing the wrong person or with the wrong attachment, while 53% conceded that too many phishing attacks bypass their gateway.

https://www.computerweekly.com/news/365532100/Nine-in-10-enterprises-fell-victim-to-successful-phishing-in-2022

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