





December 15th, 2020

Try our December - [“Shopping Online” Quiz](#)

This week's stories:

- [Desjardins at fault for huge data breach, say privacy commissioners](#) 
- [Canada assessing SolarWinds hack as U.S. agencies lock down](#) 
- [Millions of Cisco devices, plus other enterprise and industrial ones, still affected by two vulnerabilities, says new report](#)
- [Facebook says hackers backed by Vietnam's government are linked to IT firm](#)
- [Google outage caused by critical system running out of storage](#)
- [Twitter fined ~\\$550K over a data breach in Ireland's first major GDPR decision](#)
- [Ransomware attack causing billing delays for Missouri city](#)

Desjardins at fault for huge data breach, say privacy commissioners 

<https://www.itworldcanada.com/article/breaking-desjardins-at-fault-for-huge-data-breach-say-privacy-commissioners/439581>

Canada's largest financial services data breach was caused by a series of gaps in administrative and technological safeguards, federal and Quebec privacy commissioners said in a report issued this morning.

“[Desjardins Group] did not demonstrate the appropriate level of attention required to protect the sensitive personal information entrusted to its care,” said Daniel Therrien, Privacy Commissioner of Canada. “The organization’s customers and members, and all citizens, were justifiably shocked by the scale of this data breach. That being said, we are satisfied with the mitigation measures offered to those affected and the commitments made by Desjardins.”

[Click link above to read more](#)

Canada assessing SolarWinds hack as U.S. agencies lock down 

<https://globalnews.ca/news/7521584/solarwinds-hack-canadian-impact-russia/>

Canadian security officials are eyeing a significant hack south of the border that appears to have penetrated top U.S. government agencies and left officials there scrambling to limit the damage.

Reuters reported on Monday that the Department of Homeland Security, the Treasury Department, and the Department of Commerce were among thousands of business and government entities hit by the attack, which appears to have let the hackers monitor operations for nine months before being detected.

[Click link above to read more](#)

Millions of Cisco devices, plus other enterprise and industrial ones, still affected by two vulnerabilities, says new report

<https://www.itworldcanada.com/article/millions-of-cisco-devices-plus-other-enterprise-and-industrial-ones-still-affected-by-two-vulnerabilities-says-new-report/439634>

Information and operational network administrators aren't doing a good job of patching their internet-connected devices against two vulnerabilities it discovered, according to a new vendor survey.

In a blog published Tuesday, California-based Armis Inc., which makes a network visibility tool, says its research suggests huge numbers of devices affected by the Urgent/11 and CDPwn vulnerabilities still haven't been patched, although security updates were issued months ago.

[Click link above to read more](#)

Facebook says hackers backed by Vietnam's government are linked to IT firm

<https://arstechnica.com/information-technology/2020/12/facebook-says-hackers-backed-by-vietnams-government-are-linked-to-it-firm/>

Facebook said it has linked an advanced hacking group widely believed to be sponsored by the government of Vietnam to what's purported to be a legitimate IT company in that country.

The so-called advanced persistent threat group goes under the monikers APT32 and OceanLotus. It has been operating since at least 2014 and targets private sector companies in a range of industries along with foreign governments, dissidents, and journalists in South Asia and elsewhere. It uses a variety of tactics, including phishing, to infect targets with fully featured desktop and mobile malware that's developed from scratch. To win targets' confidence, the group goes to great lengths to create websites and online personas that masquerade as legitimate people and organizations.

[Click link above to read more](#)

Google outage caused by critical system running out of storage

<https://www.bleepingcomputer.com/news/google/google-outage-caused-by-critical-system-running-out-of-storage/>

The global Google services outage yesterday was caused by the company's Identity Management System failing after a bug restricted its storage space.

This system failure prevented users from accessing Gmail, YouTube, Google Drive, Google Maps, Google Calendar, and other Google services.

[Click link above to read more](#)

Twitter fined ~\$550K over a data breach in Ireland's first major GDPR decision

<https://techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/>

Ireland's Data Protection Commission (DPC) has issued Twitter with a fine of €450,000 (~\$547,000) for failing to promptly declare and properly document a data breach under Europe's General Data Protection Regulation (GDPR).

The decision is noteworthy as it's the first such cross-border GDPR decision by the Irish watchdog, which is the lead EU privacy supervisor for a number of tech giants — having a backlog of some 20+ ongoing cases at this point, including active probes of Facebook, WhatsApp, Google, Apple and LinkedIn, to name a few.

[Click link above to read more](#)

Ransomware attack causing billing delays for Missouri city

<https://www.bleepingcomputer.com/news/security/ransomware-attack-causing-billing-delays-for-missouri-city/>

The City of Independence, Missouri, suffered a ransomware attack last week that continues to disrupt the city's services.

At the beginning of the month, Independence suffered a ransomware attack that forced them to shut down their IT system as they recovered from the attack.

[Click link above 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.

