






February 4th, 2020

Try our February Quiz – [Love Information Security](#)

Save the date - February 5th to 7th is the [Privacy and Security Conference](#)

This week's stories:

- [Beware of coronavirus email scams, Instagram password worries, threats to Ashley Madison users and more](#) 
- [Federal IT systems at risk of 'critical failure,' Trudeau warned in memo](#) 
- [Ransomware attack on company raises questions about federal contracts](#) 
- [Researchers Find 'Anonymized' Data Is Even Less Anonymous Than We Thought](#)
- [Twitter Warns API Flaw Abuse May Have Unmasked Users](#)
- [The next battleground for facial recognition: The Pacific Northwest](#)
- [UN hacked: Attackers got in via SharePoint vulnerability](#)
- [97 of the world's 100 largest airports have massive cybersecurity risks](#)
- [Google researchers find serious privacy risks in Safari's anti-tracking protections](#)

Beware of coronavirus email scams, Instagram password worries, threats to Ashley Madison users and more

<https://www.itworldcanada.com/article/cyber-security-today-beware-of-coronavirus-email-scams-instagram-password-worries-threats-to-ashley-madison-users-and-more/426740>

Hackers often use news headlines as a hook to spread malware. They find a hot topic, craft an email with an eye-catching subject line and insert a malicious attachment. That attachment infects a computer if it's opened. Fears about the spread of the coronavirus is the latest event to be exploited. Beware of email with documents that supposedly have information about protecting yourself from the virus, even if the sender appears to be a health centre. IBM and security firm Kaspersky have seen evidence of these campaigns.

[Click link above to read more](#)

Federal IT systems at risk of 'critical failure,' Trudeau warned in memo

<https://www.canadiansecuritymag.com/federal-it-systems-at-risk-of-critical-failure-trudeau-warned-in-memo/>

OTTAWA — Newly released briefing notes for Prime Minister Justin Trudeau describe the dire state of federal computer systems, which deliver billions in benefits and are on the precipice of collapse.

Officials briefing Trudeau after his party's re-election noted "mission-critical" systems and applications are "rusting out and at risk of failure," requiring immediate attention from his government.

[Click link above to read more](#)

Ransomware attack on construction company raises questions about federal contracts

<https://www.cbc.ca/news/politics/ransomware-bird-construction-military-1.5434308>

RCMP has reported an uptick in ransomware attacks

A construction company that's won millions of dollars worth of contracts with the military and other federal departments has been hit by a ransomware attack — raising questions about how the federal government does business with outside firms open to cyberattacks.

Ransomware attacks involve malicious software used to cripple a target's computer system to solicit a cash payment. Last month, a group known as Maze — infamous for publicly shaming victims until they pay up — claimed to have run a successful strike against the Toronto-based company Bird Construction, stealing 60 GBs of data.

[Click link above to read more](#)

Researchers Find 'Anonymized' Data Is Even Less Anonymous Than We Thought

https://www.vice.com/en_us/article/dygy8k/researchers-find-anonymized-data-is-even-less-anonymous-than-we-thought

Corporations love to pretend that 'anonymization' of the data they collect protects consumers. Studies keep showing that's not really true.

Last fall, Adblock Plus creator Wladimir Palant revealed that Avast was using its popular antivirus software to collect and sell user data. While the effort was eventually shuttered, Avast CEO Ondrej Vitek first downplayed the scandal, assuring the public the collected data had been “anonymized”—or stripped of any obvious identifiers like names or phone numbers.

[Click link above to read more](#)

Twitter Warns API Flaw Abuse May Have Unmasked Users

<https://www.healthcareinfosecurity.com/twitter-warns-api-flaw-abuse-may-have-unmasked-users-a-13680>

A Twitter API could have enabled outsiders to match users' phone numbers to their corresponding accounts and potentially unmask anonymous users of the social media site.

Twitter says the flaw has now been fixed, but not before at least one large-scale effort exploited it. Any resulting impact on users remains unclear.

[Click link above to read more](#)

The next battleground for facial recognition: the Pacific Northwest

<https://www.biometricupdate.com/202002/the-next-battleground-for-facial-recognition-the-pacific-northwest>

A regional chain of convenience stores in the Pacific Northwest is expanding its use of facial recognition systems designed to keep out people it does not want to patronize its businesses.

Idaho-based Jacksons Food Stores has put Blue Line Technology biometric face-scanning technology in three Portland, Oregon, locations and one in Tacoma, Washington. The first one, in southeast Portland, went live in November 2018. Another Jacksons, also in Tacoma, reportedly plans to install software and cameras.

Jacksons executives have said the system captures the faces of all people before they enter the stores. It will not unlock a door for someone whose face matches a database image linked to a crime, presumably committed on the premises.

[Click link above to read more](#)

UN hacked: Attackers got in via SharePoint vulnerability

<https://www.helpnetsecurity.com/2020/01/30/un-hacked/>

In summer 2019, hackers broke into over 40 (and possibly more) UN servers in offices in Geneva and Vienna and downloaded “sensitive data that could have far-reaching repercussions for staff, individuals, and organizations communicating with and doing business with the UN,” The New Humanitarian reported on Wednesday.

The UN, unfortunately, did not share that discovery with the authorities, the public, or even the potentially affected staff, and we now know about it only because TNH reporters got their hands on a confidential report by the UN.

[Click link above to read more](#)

97 of the world's 100 largest airports have massive cybersecurity risks

<https://www.techrepublic.com/article/97-of-the-worlds-100-largest-airports-have-massive-cybersecurity-risks/>

Swiss web security company ImmuniWeb has released an in-depth report on the cybersecurity posture of the world's biggest airports, finding that almost all of them had an alarming lack of systems in place to protect their websites, mobile applications and public clouds.

The company's researchers compiled their findings in the "State of Cybersecurity at Top 100 Global Airports" report, which said only three airports -- Amsterdam Airport Schiphol, Helsinki-Vantaa Airport and Dublin Airport -- passed all of their tests without a single major issue being detected.

[Click link above to read more](#)

Google researchers find serious privacy risks in Safari's anti-tracking protections

https://arstechnica.com/information-technology/2020/01/safaris-anti-tracking-protections-can-leak-browsing-and-search-histories/?utm_source=The%20Parallax%20View&utm_campaign=2f0bb0d041-EMAIL_CAMPAIGN_2019_11_22_COPY_01&utm_medium=email&utm_term=0_7d4de369d8-2f0bb0d041-223502857

When Apple introduced powerful anti-tracking protections to Safari in 2017, advertisers banded together to say they were “deeply concerned” it would sabotage ad-supported content. Now, there’s new information showing that Safari users had good reason for unease as well.

Known as Intelligent Tracking Prevention, the mechanism uses machine learning to classify which websites are allowed to use browser cookies or scripts hosted on third-party domains to track users.

[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:

Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8

<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.

