April 9th, 2019

Try our April Quiz - Spotting a Fake

This week's stories:

- **Canada 'very likely' will be hit by foreign cyber threats before October election**
- **Ottawa city treasurer transfers $130K of taxpayer funds to email fraudsters**
- **New RCMP cyber co-ordination unit won't be fully operational until 2023**
- **Two of Canada's AI gurus warn of war by algorithm as they win tech 'Nobel Prize'**
- **Arizona Beverages knocked offline by ransomware attack**
- **Think you're using AI effectively in security? You're probably not says security expert**
- **Facebook are 'morally bankrupt liars' says New Zealand's privacy commissioner**
- **Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days**
- **Students Hack High School WiFi to Get Out of Tests**
- **Sextortion Scams Now Using Password Protected Evidence Files**
- **Genesee County, Michigan Recovering from Ransomware Attack**
- **Commercial drones pose cybersecurity threats, study finds**

Canada 'very likely' will be hit by foreign cyber threats before October election

https://www.itworldcanada.com/article/canada-very-likely-will-hit-by-foreign-cyber-threats-before-october-election-federal-report/416759

Despite widespread publicity, finger-pointing and the laying of criminal indictments, some countries continue trying to interfere online with democratic processes around the world.

As a result, Canada's electronic spy agency believes it is now "very likely" Canadians voters will encounter some form of foreign cyber interference during the run-up to October's federal election, most likely through disinformation — commonly called fake news.

Click link above to read more

Ottawa city treasurer transfers $130K of taxpayer funds to email fraudsters

https://www.ctvnews.ca/canada/ottawa-city-treasurer-transfers-130k-of-taxpayer-funds-to-email-fraudsters-1.4371900

Ottawa's city treasurer was scammed into wire-transferring more than $100,000 of taxpayer funds to a fraudster after she fell for an email scam, according to the city's auditor general's office.

Last July, Ottawa city treasurer Marian Simulik received an email from an address she thought belonged to city manager Steve Kanellakos.

Click link above to read more

New RCMP cyber co-ordination unit won't be fully operational until 2023

https://www.itworldcanada.com/article/new-rcmp-cyber-co-ordination-unit-wont-be-fully-operational-until-2023/416561

Just over a year ago the federal government announced it would beef up the RCMP's e-crime capabilities with the creation of a National Cyber Crime Co-ordination Unit (NC3).

The budget set aside $116 million over five years to create the unit, sought after for several years by the Mounties and police forces across the country who want a hub for cybercrime investigations, as well as a prominent place where residents and businesses can report cyber crime.

Click link above to read more

Two of Canada's AI gurus warn of war by algorithm as they win tech 'Nobel Prize'

https://www.canadiansecuritymag.com/news/industry-news/two-of-canadas-ai-gurus-warn-of-war-by-algorithm-as-they-win-tech-nobel-prize

MONTREAL — Two of Canada's artificial intelligence pioneers are warning about the consequences of AI in robotic weapons and outsourcing lethal decisions to machines, calling for an international agreement on its deployment as Canada marches toward the binary battlefield.

Geoffrey Hinton and Yoshua Bengio, who along with computer scientist Yann LeCun won the Turing Award on Wednesday — known as the Nobel Prize of the technology industry — say so-called weaponized AI and killer robots could spell danger for civilians.

Click link above to read more

Arizona Beverages knocked offline by ransomware attack

https://techcrunch.com/2019/04/02/arizona-beverages-ransomware/

Arizona Beverages, one of the largest beverage suppliers in the U.S., is recovering after a massive ransomware attack last month, TechCrunch has learned.

The company, famous for its iced tea beverages, is still rebuilding its network almost two weeks after the attack hit, wiping hundreds of Windows computers and servers and effectively shutting down sales operations for days until incident response was called in, according to a person familiar with the matter.

Click link above to read more.

Think you're using AI effectively in security? You're probably not says security expert

https://www.itworldcanada.com/article/think-youre-using-ai-effectively-in-security-youre-probably-not-says-security-expert/416728

Nearly 60 per cent of businesses have automated their security and incident response tools, but only at a very minimal level, according to a new SANS Institute study.

The D3 Security sponsored study on automation and integration indicates that while most respondents agree automation isn't killing jobs in the security field, few have gone past automating the most basic and repetitive tasks. But the low hanging fruit yields quick, measurable results, says Stan Engelbrecht, D3 Security partner and president, and gives skilled staff more time to focus on bigger picture items.

Click link above to read more

Facebook are 'morally bankrupt liars' says New Zealand's privacy commissioner

https://www.theguardian.com/technology/2019/apr/08/facebook-are-morally-bankrupt-liars-says-new-zealands-privacy-commissioner

New Zealand's privacy commissioner has lashed out at social media giant Facebook in the wake of the Christchurch attacks, calling the company "morally bankrupt pathological liars".

The commissioner used his personal Twitter page to lambast the social network, which has also drawn the ire of prime minister Jacinda Ardern for hosting a livestream of the attacks that left 50 dead, which was then copied and shared all over the internet.

Click link above to read more

Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days

https://www.bleepingcomputer.com/news/security/cyber-attack-shuts-down-hoya-corps-thailand-plant-for-three-days/

Japanese optical products manufacturer HOYA Corporation was hit by a cyber attack at the end of February which led to a partial shutdown of its production lines from Thailand for three days.

The company disclosed that around 100 computers were infected with a malware strain designed to steal user credentials from the machines it compromises and to drop a cryptocurrency miner during the infection process' second stage.

Click link above to read more

Students Hack High School WiFi to Get Out of Tests

https://www.bleepingcomputer.com/news/security/students-hack-high-school-wifi-to-get-out-of-tests/

To get out of taking tests and doing school work, two New Jersey Secuacus High School students came up with the innovative approach of bringing down their school's WiFi signal so students could not access the online curriculum.

As much of the Secuacus High School's classwork is done via the Internet, when the two 14 year old freshmen took down the WiFi, students were unable to access their work and classes were interrupted.

Click link above to read more

Sextortion Scams Now Using Password Protected Evidence Files

https://www.bleepingcomputer.com/news/security/sextortion-scams-now-using-password-protected-evidence-files/

New variants of the sextortion scams are now attaching password protected zip files that contain alleged proof that the sender has a video recording of the recipient. While you cannot view the individual files in the archive, you can see what they are named, which can cause recipients to become scared enough to make a payment.

The main goal of a sextortion scam is to scare the recipient of the email into making a payment in order to avoid the embarrassment of an alleged video being sent to their friends and family.

Click link above to read more

Genesee County, Michigan Recovering from Ransomware Attack

https://www.bleepingcomputer.com/news/security/genesee-county-michigan-recovering-from-ransomware-attack/

Tenesee County, Michigan was hit with a ransomware attack on Tuesday and the county has been working non-stop to get their systems back online. Unfortunately, this process turned out to be more difficult than expected and system are still down.

It is not known what ransomware they were affected by, but officials stated that their email was hacked and that the only way to contact the county was via phone.

Click link above to read more

Commercial drones pose cybersecurity threats, study finds

https://enterpriseiotinsights.com/20190401/channels/news/commercial-drones-pose-cyber-security-threats-study-finds

The growing popularity of personal and commercial drone use in populated areas poses significant risks both for society and drones due to the lack in additional technology that is required to secure both parties from one another, researchers found.

According to a new research report by Ben-Gurion University of the Negev (BGU) researchers and Fujitsu System Integration Laboratories, the lack of supporting technology could be exploited by malicious entities for cyberattacks, terrorism, crime and threats to privacy and also to attack drones while flying for a legitimate purpose.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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