Security News Digest
Information Security Branch

OCIO Office of the Chief Information Officer

October 22nd, 2019

October is "Cybersecurity awareness" Month

Try our October quiz – Fake or Not

Security Day, "The Humans of Security", Nov 20, 2019

This week's stories:

- **Canadian credit reporting agency compromised through third party**
- **Canadian Indigenous youth robotics team to compete in Dubai**
- **Researchers find huge database of fingerprints and facial recognition images on the Net**
- **Alexa and Google Home used to eavesdrop and phish passwords**
- **MedusaLocker Ransomware Wants Its Share of Your Money**
- **AWS chief says facial recognition should be regulated**
- **Top 10 technology trends for 2020 include hyperautomation, human augmentation and distributed cloud**
- **The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History**

Canadian credit reporting agency compromised through third party

https://www.itworldcanada.com/article/canadian-credit-reporting-agency-compromised-through-third-party/422576

A hacker was able to access financial information on 37,000 Canadians or businesses held by credit reporting agency TransUnion Canada for two weeks over the summer by going through one of the company's business customers.

The news site Bleeping Computer said Monday it had learned that TransUnion Canada began mailing notification letters to affected customers, saying someone stole the access code of equipment leasing firm CWB National Leasing, and with it entered a TransUnion business portal to do credit file lookups between June 28th and July 11th.

Click link above to read more

Canadian Indigenous youth robotics team to compete in Dubai

https://globalnews.ca/news/6023167/canadian-indigesteam-robotics/

Several Alberta students are preparing for an opportunity for a lifetime — this October, the IndigeSTEAM team will head to Dubai to compete on behalf of Canada in an international robotics competition.

The First Global event will be a chance for the team to show off their skills on a world stage, and the team is hoping to show off their culture as well.

Click link above to read more

Researchers find huge database of fingerprints and facial recognition images on the Net

https://www.itworldcanada.com/article/researchers-find-huge-database-of-fingerprints-and-facial-recognition-images-on-the-internet/420881

Biometric authentication — the use of facial recognition, iris recognition or fingerprints — is seen by many experts as the savior of security by allowing organizations to do away with passwords.

However, privacy researchers on Wednesday discovered a large bank of unprotected biometric, password and other personal data open on the internet. The data, which belong to the BioStar 2 identity and access control platform, serve as a reminder of the basic rule of cybersecurity: if highly-sensitive identity data isn't adequately protected, then the system is worthless

Click link above to read more

Alexa and Google Home abused to eavesdrop and phish passwords

https://arstechnica.com/information-technology/2019/10/alexa-and-google-home-abused-to-eavesdrop-and-phish-passwords/

Amazon- and Google-approved apps turned both voice-controlled devices into "smart spies."

By now, the privacy threats posed by Amazon Alexa and Google Home are common knowledge. Workers for both companies routinely listen to audio of users—recordings of which can be kept forever—and the sounds the devices capture can be used in criminal trials.

Click link above to read more

MedusaLocker Ransomware Wants Its Share of Your Money

https://www.bleepingcomputer.com/news/security/medusalocker-ransomware-wants-its-share-of-your-money/

A new ransomware called MedusaLocker is being actively distributed and victims have been seen from all over the world. It is not known at this time, how the attacker is distributing the ransomware.

This new ransomware was found by MalwareHunterTeam around October 17th, 2019, and while it is not currently known how the ransomware is being distributed, there has been a steady amount of submissions to the ID Ransomware site since then.

When the ransomware is installed, it will perform various startup routines in order to prep the computer for encryption.

Click link above to read more

AWS chief says facial recognition should be regulated

https://www.cnet.com/news/aws-chief-says-facial-recognition-should-be-regulated/

The chief of Amazon Web Services defended his company's use of facial recognition technology but said he believes it should be subject to government regulation.

Andy Jassy, the CEO of Amazon's cloud computing services, speaking Monday at the Code Conference in Scottsdale, Arizona, acknowledged that concerns about technologies like its controversial Rekognition program are valid but maintained the technologies still have value.

Click link above to read more

Top 10 technology trends for 2020 include hyperautomation, human augmentation and distributed cloud

https://www.techrepublic.com/article/hyperautomation-human-augmentation-and-distributed-cloud-among-top-10-technology-trends-for-2020/

Gartner identified the top strategic technology trends likely to reach tipping points in the near future.

The top 10 technology trends for 2020 presented at the Gartner IT Symposium/Xpo included hyperautomation, multiexperience, human augmentation and distributed cloud.

The key trends have a people-centric approach, explained David Cearley, vice president and Gartner Fellow, during a conference session today. The Orlando, FL conference runs through October 24, with more than 9,000 CIOs and IT leaders in attendance.

Click link above to read more

The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History

https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/#intcid=recommendations_wired-right-rail-popular_6819e63f-34aa-4f91-af2a-62b135580541_cral-top3-1

How digital detectives unraveled the mystery of Olympic Destroyer—and why the next big attack will be even harder to crack.

Just before 8 pm on February 9, 2018, high in the northeastern mountains of South Korea, Sang-jin Oh was sitting on a plastic chair a few dozen rows up from the floor of Pyeongchang's vast, pentagonal Olympic Stadium. He wore a gray and red official Olympics jacket that kept him warm despite the near-freezing weather, and his seat, behind the press section, had a clear view of the raised, circular stage a few hundred feet in front of him. The 2018 Winter Olympics opening ceremony was about to start.

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.