Security Digest
Information Security Branch

BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer

July 31st, 2018

July is "Security while you travel" Month

This week's stories:

- **Canada Is Using DNA Ancestry Websites To Assist In Deporting People**
- **At least two malls are using facial recognition technology to track shoppers' ages and genders without telling**
- **Privacy commissioner and advocates warn Canadians to keep data secure when crossing the border**
- **Twitter's Plan to Clean Itself Up Involves Getting Rid of 143,000 Bad Apps**
- **Facebook Suspends Harvard Prof's Data Analytics Company Over User Privacy Concerns**
- **Dropbox still has questions to answer after claims of improper data sharing**
- **Here's why Twitter will lock your account if you change your display name to Elon Musk**
- **DOD to Move All Websites to HTTPS by the End of the Year**
- **Pentagon Creates 'Do Not Buy' List of Chinese and Russian Software Providers**
- **Florida High School Football Team Improperly Accessed Rivals' Training Videos**
- **Biggest Pediatric Hospital Breach Reported**

Canada Is Using DNA Ancestry Websites To Assist In Deporting People

https://socialnewsdaily.com/73399/canada-deporting-via-ancestry-sites/

The Canada Border Services Agency has been assembling their DNA and utilizing ancestry websites to locate and contact their distant relatives and establish their nationality, in another example of the exceptional lengths Canadian immigration officials go to deport migrants.

"I think it is a matter of public interest that border service agencies like the CBSA are able to obtain access to DNA results from sites like Familytreedna.com and Ancestry.com," said Subodh Bharati, an attorney who is representing a man who says he's Liberian, but who the government is now attempting to prove is actually Nigerian.

"There are clear privacy concerns. How is the CBSA able to access this information and what measures are being put in place to ensure this information remains confidential?"

Click link above to read more

At least two malls are using facial recognition technology to track shoppers' ages and genders without telling

https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964

At least two Calgary malls are using facial recognition technology to track shoppers' ages and genders without first notifying them or obtaining their explicit consent.

Click link above to read more

Privacy commissioner and advocates warn Canadians to keep data secure when crossing the border

https://www.thestar.com/vancouver/2018/07/24/leave-the-phone-at-home-privacy-commissioner-and-advocates-warn-canadians-to-keep-data-secure-when-crossing-the-border.html

VANCOUVER—Crossing the border into the United States is routine for many Canadians, but the Privacy Commissioner of Canada is warning citizens to be aware that their digital devices can be searched — and civil liberties advocates say every precaution must be taken.

The commissioner's updated guidelines on privacy at airports and borders advises that officers on both sides of the border can search your devices and ask for passwords.

Tobi Cohen, spokesperson for the Office of the Privacy Commissioner of Canada, said the guidelines include new advice on searches conducted at "preclearance" sites, where U.S. border officials can do searches on Canadian ground, part of an act passed in late 2017.

The commissioner's updates also come following the release of a new U.S. Customs and Border Protection directive on searches of electronic devices, which clarifies previous search rules. It also includes updates on electronic searches for people going back through Canadian customs.

Click link above to read more

Twitter's Plan to Clean Itself Up Involves Getting Rid of 143,000 Bad Apps

http://fortune.com/2018/07/24/twitter-apps-data-privacy/

Twitter's plans to clean itself up from bad behavior that plagues the service involves removing more than 143,000 malicious apps from its service.

The online messaging company said Tuesday that it removed the bad apps between April and June 2018, citing in a blog post that it does "not tolerate the use of our APIs to produce spam, manipulate conversations, or invade the privacy of people using Twitter." Third-party developers can access Twitter's APIs, or application programming interface, to build their own apps on Twitter's platform.

Twitter's purge of bad apps comes amid controversy facing social media giant Facebook and its Cambridge Anlaytica scandal. Facebook has weathered fierce criticism from lawmakers that it failed to prevent an academic researcher from building an app on its platform that siphoned user data, which was ultimately sold to a political consulting firm that used the information to allegedly influence the 2016 U.S. presidential election.

Click link above to read more

Facebook Suspends Harvard Prof's Data Analytics Company Over User Privacy Concerns

https://www.thecrimson.com/article/2018/7/27/facebook-suspends-crimson-hexagon/

Facebook suspended Crimson Hexagon — a data analytics company founded by University professor Gary King— last week, claiming the group may have violated Facebook policies in its analysis of site data for the U.S. government and for a Russian nonprofit linked to the Kremlin.

During the suspension, Facebook will investigate how Crimson Hexagon collects, shares, and stores user data. The suspension and investigation were first reported by the Wall Street Journal.

Crimson Hexagon, located in Boston, pulls and analyzes public Facebook data for third-party clients. Russian non-profit Civil Society Development Foundation paid the company to study Russians' opinions of the regime of Vladimir Putin — and, last month, Crimson Hexagon forged a contract with the U.S. State Department for more than $240,000, the Journal reported.

Click link above to read more

Dropbox still has questions to answer after claims of improper data sharing

https://www.zdnet.com/article/dropbox-faces-questions-over-claims-of-improper-data-sharing/#ftag=RSSbaffb68

Confusion swirled after a report claimed last week that file storage service Dropbox had given away data on thousands of academics.

The researchers claimed they could see "every Dropbox folder associated with a given researcher."

In case you missed it, the highlights of a research study by Northwestern University published on Harvard Business Review revealed Dropbox had given them "access to project-folder-related data" over a two-year period from about 400,000 users across 1,000 universities.

The researchers initially claimed Dropbox gave them raw data, which they anonymized, but their report was updated after *ZDNet* reported last Monday that Dropbox said it anonymized the data before handing it over.

Dropbox said in a statement that its anonymization process prevented the researchers from seeing any personal information, but it allowed them to analyze the anonymized data for patterns and insights.

It's a confusing situation -- and one that has academics rightfully angry any of their data, even anonymized, was shared in the first place. Given that academics often work on highly sensitive projects, keeping data in the cloud can be risky.

Click link above to read more

Here's why Twitter will lock your account if you change your display name to Elon Musk

https://hotforsecurity.bitdefender.com/blog/heres-why-twitter-will-lock-your-account-if-you-change-your-display-name-to-elon-musk-20138.html

There's bad news if your name really is "Elon Musk".

You're going to jump over some additional hurdles to convince Twitter that you should be allowed to change your display name to the one you share with the boss of Tesla and SpaceX.

For months scammers have been creating Twitter profiles which pose as tech billionaire, in an attempt to defraud unwary users out of cryptocurrency.

The scam works like this.

The real Elon Musk (@elonmusk) posts a message to his 22 million followers. Some of his followers reply. Perhaps even the real Elon Musk responds to some of the comments he receives.

But what also happens is, with alarming regularity, a fake Elon Musk profile using the same avatar jumps into the threaded conversation and steers it towards a webpage under their control.

Click link above to read more

DOD to Move All Websites to HTTPS by the End of the Year

https://www.bleepingcomputer.com/news/government/dod-to-move-all-websites-to-https-by-the-end-of-the-year/

The US Department of Defense plans to implement HTTPS and HSTS (HTTP Strict Transport Security) for all its public-facing websites by the end of the year.

Issues about DOD websites using insecure HTTP connections or problematic SSL certificates have been raised in a letter sent earlier this year, in May, by Oregon Democrat Senator Ron Wyden.

Click link above to read more

Pentagon Creates 'Do Not Buy' List of Chinese and Russian Software Providers

https://www.bleepingcomputer.com/news/government/pentagon-creates-do-not-buy-list-of-chinese-and-russian-software-providers/

The Department of Defense (DOD) acquisition chief confirmed on Friday in a press conference that they've been silently working on a "Do Not Buy" list of companies known to use Chinese and Russian software in their products.

Ellen Lord, defense undersecretary for acquisition and sustainment, said the Pentagon started compiling the list about six months ago. She said the Department shared the list with DOD agencies but have not enforced or made it obligatory.

Click link above to read more

Florida High School Football Team Improperly Accessed Rivals' Training Videos

https://www.bleepingcomputer.com/news/security/florida-high-school-football-team-improperly-accessed-rivals-training-videos/

The Braden River High School football program is in trouble after it was caught accessing the training videos of four of its rivals.

The incident happened during last year's high school football season, but it only recently came to light after a representative of the Manatee County School District announced the results of an investigation they started back in May.

Team coaches accessed a college's HUDL account

District officials say that Braden River coaching staff had accessed the HUDL account of a college and used it to view training videos recorded by its rivals.

HUDL is an online service used by Florida high schools to upload and store videos of players, practices, and games. HUDL grants access to these videos to colleges across the country for recruitment purposes.

District officials didn't say what college's account Braden River coaches used to view practices from rival teams. They also didn't specify if this was a case of a malicious, intrusive hack or a college representative willingly giving access to the Braden River coaching staff.

Click link above to read more

Biggest Pediatric Hospital Breach Reported

https://www.databreachtoday.com/biggest-pediatric-hospital-breach-reported-a-11257

A recent hacking incident at Boys Town National Research Hospital is the largest ever reported by a pediatric care provider or children's hospital, according to the federal health data breach tally. A wide variety of data on some 105,000 individuals, including young patients as well as employees, was exposed, opening the door to potential fraud.

The U.S. Department of Health and Human Services' HIPAA Breach Reporting Tool website, commonly called the "wall of shame," lists breaches reported since 2009 that affected 500 or more individuals. The tally now includes about 35 major breaches at children's hospitals or pediatric healthcare providers impacting a total of more than 434,000 individuals.

As of Thursday, the Boys Town Hospital incident also ranked as the eighth largest health data breach posted so far this year.

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