Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

August 21st, 2018

August is "Wi-Fi" Month

This week's stories:

- Rising sea levels could knock out the internet within 15 years — here's how
- Sensitive Canadian, UK government info exposed from cloud project management service
- How Hacked Water Heaters Could Trigger Mass Blackouts
- Former Microsoft engineer sent behind bars for role in ransomware extortion scheme
- Australian teenager hacked Apple's network multiple times, accessed 90GB worth of files
- U.S. wants Facebook to let law enforcement wiretap a suspect's Messenger: sources
- Workers protest Google's censored search engine plans for China
- Trump Pulls Gloves Off on Offensive Cyber Actions
- Judge Approves Final $115 Million Anthem Settlement
- Instagram Hack: Hundreds Affected, Russia Suspected
- Here's What Happens When We Allow Facial Recognition Technology in Our Schools

---

Rising sea levels could knock out the internet within 15 years — here's how

https://globalnews.ca/news/4378627/rising-sea-levels-destroy-internet-15-years/

Thousands of miles of internet cables zigzagging under coastal cities in the United States could be completely submerged underwater within the next 15 years, a team of researchers has found.

Cities like New York, Miami, Seattle and even coastal regions in Canada, could see rising sea levels destroy a network of cables and data centres that bolsters so much of modern life.

Scientists at the University of Oregan and the University of Wisconsin-Madison, presented their study last month in Montreal, saying climate change is causing sea levels to rise rapidly, which in turn can lead to widespread flooding and cause massive internet outages.

Click link above to read more

Sensitive Canadian, UK government info exposed from cloud project management service

https://www.itworldcanada.com/article/sensitive-canadian-uk-government-info-exposed-from-cloud-project-management-service/408104

In another example of how employees can defeat the best security strategies, a researcher has discovered Canadian and British government staffers misconfigured some of their web-based Trello

project management software and exposed details of software bugs and security plans, as well as passwords for servers and other sensitive information.

Trello allows users to create cards of lists for managing projects. The cards can also include messages for team members. Normally Trello is configured to private by default, says the service provider. However, security researcher Kushagra Pathak found that 25 Canadian government boards exposed to the public Internet.

Click link above to read more

How Hacked Water Heaters Could Trigger Mass Blackouts

https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

When the cybersecurity industry warns about the nightmare of hackers causing blackouts, the scenario they describe typically entails an elite team of hackers breaking into the inner sanctum of a power utility to start flipping switches. But one group of researchers has imagined how an entire power grid could be taken down by hacking a less centralized and protected class of targets: home air conditioners and water heaters. Lots of them.

Click link above to read more

Former Microsoft engineer sent behind bars for role in ransomware extortion scheme

https://www.zdnet.com/article/former-microsoft-engineer-sent-behind-bars-for-role-in-ransomware-extortion-scheme/

A former Microsoft engineer has been given an 18-month prison sentence after being found guilty of laundering money acquired from Reveton ransomware victims.

The US Department of Justice (DoJ) said on Tuesday that Raymond Odigie Uadiale, 41, of Maple Valley, Washington, pleaded guilty to "cashing out" payments made by victims of Reveton.

The ransomware in question executes on PCs and encrypts system files. A message is then shown on the home screen which claims that the user has violated federal law and downloaded illegal content.

As the message utilizes the FBI logo, users may be frightened enough to pay the "fine" in order to regain access to their PC.

Click link above to read more

Australian teenager hacked Apple’s network multiple times, accessed 90GB worth of files

https://globalnews.ca/news/4395278/australian-teenager-hacked-apple/

Court documents reveal that a 16-year-old hacker from Australia allegedly broke into tech giant Apple’s computer systems and may have downloaded internal files.

The Age newspaper reports that the teenager’s actions were driven by an admiration for the company, and that the boy stored the stolen files in a folder entitled “hacky hack hack.” The teen reportedly downloaded over 90 gigabytes of data and accessed customer accounts without exposing his identity.

Click link above to read more

U.S. wants Facebook to let law enforcement wiretap a suspect’s Messenger: sources

https://globalnews.ca/news/4394990/facebook-messenger-us-government/

The U.S. government is trying to force Facebook Inc to break the encryption in its popular Messenger app so law enforcement may listen to a suspect’s voice conversations in a criminal probe, three people

briefed on the case said, resurrecting the issue of whether companies can be compelled to alter their products to enable surveillance.

The previously unreported case in a federal court in California is proceeding under seal, so no filings are publicly available, but the three people told Reuters that Facebook is contesting the U.S. Department of Justice's demand.

Click link above to read more

Workers protest Google's censored search engine plans for China

https://globalnews.ca/news/4393283/google-china-search-engine/

More than a thousand Google employees have signed a letter protesting the company's secretive plan to build a search engine that would comply with Chinese censorship.

The letter calls on executives to review ethics and transparency at the company.

The letter's contents were confirmed by a Google employee who helped organize it but who requested anonymity because of the sensitive nature of the debate.

Click link above to read more

Here's how to turn off Google's other tracking feature that you didn't know about

https://globalnews.ca/news/4386516/turn-off-google-tracking-feature/

A while back, we told you about Google Maps Timeline, a little-known feature that provides a minute-by-minute record of your physical movements available to you — and anyone else with access to your account.

Like many of these features, it's easy enough to turn off — once you know about it.

We had yet another reminder of this on Monday when the Associated Press reported that Google was tracking users' movements through a completely separate process, much less transparent than Google Timeline, that still works even if you turn Google Timeline off.

Click link above to read more

Trump Pulls Gloves Off on Offensive Cyber Actions

https://www.databreachtoday.com/trump-pulls-gloves-off-on-offensive-cyber-actions-a-11374

U.S. President Donald Trump signed a presidential order on Wednesday that revokes a set of Obama-era guidelines for offensive cyber operations, the Wall Street Journal reports.

The move was made without fanfare and was described by anonymous administration officials speaking to the publication. It's intended to loosen restrictions on U.S. use of cyber weapons against adversaries, the Journal reports.

The policy change may satisfy critics who contend the U.S. should be able to move faster and more aggressively in response to cyber attacks. But it also could raise questions as to whether such actions could further aggravate adversaries and cause an escalation of activity.

Click link above to read more

Judge Approves Final $115 Million Anthem Settlement

https://www.databreachtoday.com/judge-approves-final-115-million-anthem-settlement-a-11399

A federal judge in California has given final approval to a $115 million settlement involving health insurer Anthem over its 2015 data breach. The settlement is the largest ever recorded for a class-action lawsuit filed over a data breach. But most victims will receive no money.

The class-action suit has been winding its way through federal court in San Jose since mid-2015 and is the result of a consolidation of more than 100 lawsuits filed against Anthem.

Most of the settlement fund will be used to fund two more years of credit monitoring and fraud resolution services for victims. About 13 percent of the fund has been reserved for cash reimbursements for any victims who paid out of pocket for security monitoring services.

Click link above to read more

Instagram Hack: Hundreds Affected, Russia Suspected

http://www.darkreading.com/attacks-breaches/instagram-hack-hundreds-affected-russia-suspected/d/d-id/1332558?elq_mid=86322&elq_cid=5677080

A growing number of Instagram users have been hit in a hacking campaign leaving hundreds logged out of their accounts and struggling to reverse their profile content back to normal.

Users affected by the hack, first reported by Mashable, are logged out of their accounts. When they attempt to log back in, they learn their username, profile photos, password, and linked Facebook account have been changed. Email addresses linked to Instagram accounts have been switched to .ru domains, a sign the threat may originate from Russia or a Russian impersonator.

Click link above to read more

Here's What Happens When We Allow Facial Recognition Technology in Our Schools

https://medium.com/aclu/heres-what-happens-when-we-allow-facial-recognition-technology-in-our-schools-8502c116bc4a

The idea of facial recognition technology conjures up scenes from books and films set in dystopian futures in which freedom and liberty have been forfeited in exchange for the illusion of security. From "1984" to "Minority Report," these are worlds where everyone is suspect, and no one is safe.

Today, you don't need to look to fiction to imagine these consequences. Facial recognition technology—unregulated, prone to error, and poorly understood—is being rapidly rolled out in the institutions where we should place the most trust: our schools.

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