Security News Digest
Information Security Branch
British Columbia OCIO | Office of the Chief Information Officer

February 11th, 2020

Try our February Quiz – Love Information Security

This week's stories:

- Canada's military wants Ottawa to ban Huawei from 5G 🇨🇦
- Canada's Top Women in Cyber Security 🇨🇦
- Coding Flaw Exposes Voter Details for 6.5 Million Israelis?
- Europe Limits Government by Algorithm. The US, Not So Much
- How Big Companies Spy on Your Emails
- OPINION: Digital IDs Make Systemic Bias Worse
- U.S Charges Four Chinese Military Members Over Equifax Hack
- 13 tips to avoid Valentine's Day online romance scams
- White Hats Shine a Light on Philips Hue Hack

Canada's military wants Ottawa to ban Huawei from 5G 🇨🇦

https://www.theglobeandmail.com/politics/article-canadas-military-wants-ottawa-to-ban-huawei-from-5g/

Canada's military wants the federal government to ban Chinese telecommunications giant Huawei Technologies Co. Ltd. from supplying equipment for the next generation of wireless infrastructure, according to a senior Canadian official with knowledge of the matter.

National security agencies, the military and the Department of Innovation are conducting a cybersecurity review to determine whether Huawei's 5G technology would be a security risk to Canada. The review also examines the costs to consumers and major telecom carriers of restricting 5G equipment suppliers.

Click link above to read more

CANADA'S TOP WOMEN IN CYBER SECURITY

https://www.itworldcanada.com/canadas-top-women-in-cyber-security

This new initiative recognizes women in Canada who have made a significant contribution to the cyber security industry.

The inaugural call for submissions will launch on International Women's Day
March 8, 2020

Click link above to read more

Coding Flaw Exposes Voter Details for 6.5 Million Israelis

https://www.databreachtoday.asia/coding-flaw-exposes-voter-details-for-65-million-israelis-a-13708

Israel's entire voter registration database - comprising close to 6.5 million people - was exposed to the internet because of an elementary coding flaw in an election application, according to an Israeli developer.

The error exposed full names, addresses, phone numbers, ID card numbers, genders and other personal information, writes Ran Bar-Zik, a front-end developer for Verizon Media who's also a technology writer for Israeli publisher Haaretz.

Bar-Zik, who was tipped off to the vulnerability by a source, also wrote a separate blog post describing the coding error.

Click link above to read more

Europe Limits Government by Algorithm. The US, Not So Much

https://www.wired.com/story/europe-limits-government-algorithm-us-not-much/

One evening last June, residents from the Hillesluis and Bloemhof neighborhoods on the south side of Rotterdam, in the Netherlands, crowded into a community room at their local playground. Many wore headscarves and some arrived after a protest march from a local mosque. The residents had assembled to learn more about a government system called SyRI that had quietly flagged thousands of people in their low-income communities to investigators as more likely to commit benefits fraud. “People were very, very angry,” says Maureen van der Pligt, an official with union federation FNV, which helped organize the meeting.

On Wednesday, van der Pligt and the concerned residents were planning a party. The district court of the Hague shut down SyRI, citing European human rights and data privacy laws.

The case demonstrates how privacy regulations and human rights laws can rein in government use of automation. It’s among several recent examples of European regulations limiting government programs that turn algorithms and artificial intelligence on citizens. In the US, however, such guardrails generally are lacking.

Click link above to read more

How Big Companies Spy on Your Emails

https://www.vice.com/en_us/article/pkekmb/free-email-apps-spying-on-you-edison-slice-cleanfox

The popular Edison email app, which is in the top 100 productivity apps on the Apple app store, scrapes users' email inboxes and sells products based off that information to clients in the finance, travel, and e-Commerce sectors. The contents of Edison users' inboxes are of particular interest to companies who can buy the data to make better investment decisions, according to a J.P. Morgan document obtained by Motherboard.

On its website Edison says that it does "process" users' emails, but some users did not know that when using the Edison app the company scrapes their inbox for profit. Motherboard has also obtained documentation that provides more specifics about how two other popular apps—Cleanfox and Slice—sell products based on users' emails to corporate clients.

Click link above to read more

OPINION: Digital IDs Make Systemic Bias Worse

https://www.wired.com/story/opinion-digital-ids-make-systemic-bias-worse/

Last week, the Kenyan High Court blocked the country’s new digital ID initiative from moving forward in its current form. Other nations’ judiciaries have taken on similar biometric ID programs—the Indian Supreme Court set limits on the subcontinent’s massive Aadhaar program, which has scanned the irises of over a billion people. But never before has a court halted a digital ID scheme on the grounds that it could exclude a segment of the population.

It's high time. Kenya is one of many countries (including the Philippines, Nigeria, and Mexico) looking to digitize their national ID systems. The privacy concerns related to digital ID are well known; they were the focus of India's Supreme Court ruling, for example. Less known is the way these digital systems are often being built, as in Kenya, atop discriminatory regimes.

Click link above to read more

How Shadow IT could put your organization at risk

https://www.techrepublic.com/article/how-shadow-it-could-put-your-organization-at-risk/

The IT professionals at your organization likely put a lot of effort into making sure your internal accounts, logins, passwords, and systems are secure and protected.

But what happens when an employee creates an external account without the knowledge of IT? That's known as Shadow IT, and a blog post published Thursday by 1Password explains why it presents a security risk.

Click link above to read more

U.S Charges Four Chinese Military Members Over Equifax Hack

https://www.bloomberg.com/news/articles/2020-02-10/justice-department-indicted-4-chinese-hackers-in-equifax-breach

The Department of Justice announced charges Monday against four members of China's People's Liberation Army for the 2017 hack of Equifax Inc., a breach that exposed the personal information of about 145 million Americans.

The announcement by Attorney General William Barr follows an indictment in Atlanta accusing the Chinese military personnel of conspiring wilth each other to hack into Equifax's network and stealing sensitive data on nearly half of all U.S. citizens.

Click link above to read more

---

13 tips to avoid Valentine's Day online romance scams

https://www.techrepublic.com/article/13-tips-to-avoid-valentines-day-online-romance-scams/

Cybercriminals will often leverage certain holidays and other calendar events to target people with specific scams. Tax season will see an increase in tax-related scams. The summer months will trigger vacation and travel scams.

And Valentine's Day will give rise to romance scams, often directed toward people who use dating sites and apps. For users of such sites, there are ways you can protect yourself, courtesy of the FBI and security providers Vectra and Thycotic.

Click link above to read more

White Hats Shine a Light on Philips Hue Hack

https://www.infosecurity-magazine.com/news/white-hats-shine-a-light-on/

Security researchers have discovered a new exploit which could allow hackers to compromise home and corporate IT networks via smart light bulbs.

The CVE-2020-6007 flaw exists in the Zigbee wireless protocol used to communicate with IoT devices. Check Point white hats found a way to exploit the bug in popular Philips Hue smart bulbs to take control of the bulbs' control bridge and then attack the network.

However, to achieve the above, a hacker would first need to implant malicious firmware on the bulb itself. By doing so, they can tamper with the settings remotely to trick the user into thinking there is a fault.

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

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer