October 15th, 2019

October is "Cybersecurity awareness" Month

Try our October quiz – Fake or Not

This week's stories:

- **Former CIO warns that Canada lacks the 'building blocks' of digital economy**
- **2 Montrealers charged in connection with Bell Canada cyber attack**
- **New York Times: THE PRIVACY PROJECT**
- **Digital dystopia: how algorithms punish the poor**
- **Apple drops Hong Kong police-tracking app used by protesters**
- **A Deepfake Deep Dive into the Murky World of Digital Imitation**
- **Microsoft says Iranian hackers tried to hack a US presidential campaign**
- **Twitter 'accidentally' misused user data to sell targeted ads**

Former CIO warns that Canada lacks the 'building blocks' of digital economy

https://www.globalgovernmentforum.com/former-cio-warns-that-canada-lacks-the-building-blocks-of-digital-economy/

Alex Benay, Canada's former chief information officer, has warned that officials are not making sufficient progress on digital identity, which he argues is the cornerstone of a digital economy.

Speaking with Global Government Forum, Benay – who announced his departure from government in August, and has since joined Artificial Intelligence firm MindBridge Ai as chief client officer – noted that "most countries that have been successful in the industrial age have had a hard time pivoting to the digital reality, and a digital identity is part of that. In Canada we've got pockets of things going on on the identity piece, but it's on the corner of people's desks, off the radar and not supported politically."

Click link above to read more

---

2 Montrealers charged in connection with Bell Canada cyber attack

https://globalnews.ca/news/6008541/montrealers-charged-bell-cyber-attack/

The RCMP say charges have been laid against two Quebecers for their alleged involvement in a cyber attack of Bell Canada customer accounts.

Nana Koranteng and Jesiah Russell-Francis of Montreal are to appear on charges including unauthorized use of a computer, fraud over $5000, conspiracy to commit fraud, laundering proceeds of crime, identity theft, and identity fraud

The Mounties began the investigation, dubbed Project Abalone, in 2018 after it was notified that some Bell accounts were breached and personal information was stolen.

The RCMP say the suspects were identified after a number of stolen accounts were used to fraudulently purchase goods online.

Click link above to read more

New York Times: THE PRIVACY PROJECT

https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html

Companies and governments are gaining new powers to follow people across the internet and around the world, and even to peer into their genomes. The benefits of such advances have been apparent for years; the costs — in anonymity, even autonomy — are now becoming clearer.

The boundaries of privacy are in dispute, and its future is in doubt. Citizens, politicians and business leaders are asking if societies are making the wisest tradeoffs.

The Times is embarking on this months-long project to explore the technology and where it's taking us, and to convene debate about how it can best help realize human potential.

Click link above to read more

Digital dystopia: how algorithms punish the poor

https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor

All around the world, from small-town Illinois in the US to Rochdale in England, from Perth, Australia, to Dumka in northern India, a revolution is under way in how governments treat the poor.

You can't see it happening, and may have heard nothing about it. It's being planned by engineers and coders behind closed doors, in secure government locations far from public view.

Only mathematicians and computer scientists fully understand the sea change, powered as it is by artificial intelligence (AI), predictive algorithms, risk modeling and biometrics. But if you are one of the millions of vulnerable people at the receiving end of the radical reshaping of welfare benefits, you know it is real and that its consequences can be serious – even deadly.

Click link above to read more

Apple drops Hong Kong police-tracking app used by protesters

https://packetstormsecurity.com/news/view/30573/Apple-Drops-Hong-Kong-Police-Tracking-App-Used-By-Protesters.html

Apple has removed an app that protesters in Hong Kong have used to track police movements and tear gas use, saying the app violated its rules.

The company said the app, HKmap.live, had "been used in ways that endanger law enforcement and residents".

Apple initially rejected the app - which uses data from protesters on the ground - from its store.

Click link above to read more

A Deepfake Deep Dive into the Murky World of Digital Imitation

https://threatpost.com/a-deepfake-deep-dive-into-the-murky-world-of-digital-imitation/149131/

Deepfake technology is becoming easier to create – and that's opening the door for a new wave of malicious threats, from revenge porn to social-media misinformation.

About a year ago, top deepfake artist Hao Li came to a disturbing realization: Deepfakes, i.e. the technique of human-image synthesis based on artificial intelligence (AI) to create fake content, is rapidly evolving. In fact, Li believes that in as soon as six months, deepfake videos will be completely undetectable. And that's spurring security and privacy concerns as the AI behind the technology becomes commercialized – and gets in the hands of malicious actors.

Click link above to read more

Microsoft says Iranian hackers tried to hack a US presidential campaign

https://www.bleepingcomputer.com/news/security/muhstik-ransomware-victim-hacks-back-releases-decryption-keys/

Hackers backed by the Iranian government recently tried to hack email accounts used by the campaign of a US presidential candidate, a Microsoft official said on Friday.

The "Phosphorous" hackers, as Microsoft has named the group, targeted the unidentified campaign by attempting to access email accounts campaign staff received through Microsoft cloud services. Rather than relying on malware or exploiting software vulnerabilities, the attackers worked relentlessly to gather information that could be used to activate password resets and other account recovery services Microsoft provides.

Click link above to read more

Twitter 'accidentally' misused user data to sell targeted ads

https://www.techspot.com/news/82267-twitter-accidentally-misused-user-data-sell-targeted-ads.html

Twitter this week said it recently realized that some e-mail addresses and phone numbers submitted for account security purposes (two-factor authentication, for example) may have actually been used for targeted advertising purposes.

Specifically, Twitter's Tailored Audiences and Partner Audiences advertising systems may have been leveraged in the scheme. These programs allow advertisers to target ads to customers based on either their own custom contact lists or those provided by a third party.

Click link above to read more

4000 Seymour Place, Victoria, BC V8X 4S8

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca