June 18th, 2019

Try our June quiz – Smart Cities

This week's stories:

- **Open Elasticsearch instance had data on Canadian immigrant applicants**
- **Ontario city stung for $503,000 in switched bank account fraud**
- **Ryerson, Rogers, RBC back new Brampton cyber security innovation centre**
- **In new guide, spy agency warns campaign teams 'more likely' targets of cyber attacks**
- **New York Times: US ramping up cyber attacks on Russia**
- **Samsung's Smart TV Malware Scan Reminder Met by User Criticism**
- **Some BD Infusion Pumps Vulnerable to Remote Attacks**
- **Instagram Shows Kids' Contact Details in Plain Sight**
- **Google Researcher Details Windows Cryptographic Library Bug**

Open Elasticsearch instance had data on Canadian immigrant applicants

https://www.itworldcanada.com/article/open-elasticsearch-instance-had-data-on-canadian-immigrant-applicants-researcher/418962

Finding exposed Elasticsearch servers has become great sport among some security pros. Canadian researcher and consultant Darryl Burke recently came across two more, one of which held sensitive personal information of Middle East residents looking to immigrate to Canada.

Using a research tool he created for finding unsecured databases, last month Burke found an exposed Elasticsearch database belonging to an immigration consulting company in the United Arab Emirates (UAE), where a knowledgable person could have found data of applicants including their names, passwords, emails, photocopies of passports and other material.

Click link above to read more

Ontario city stung for $503,000 in switched bank account fraud

https://www.itworldcanada.com/article/ontario-city-stung-for-503000-in-switched-bank-account-fraud/419007

Creating trust is vital for any organization. It's also one of the factors criminals rely on.

The City of Burlington, Ont. found that out the hard way last month when an employee fell for an increasingly common scam: An email supposedly from what it calls a "trusted vendor" requesting to change the bank account where the municipality normally transfers money to.

Agreeing to the change, the $503,000 payment went to an account controlled by an unknown person.

The incident took place May 16. The city only learned about it five business days later. It made the incident public in a news release Thursday.

Click link above to read more

Ryerson, Rogers, RBC back new Brampton cyber security innovation centre

https://www.itworldcanada.com/article/ryerson-rogers-rbc-back-new-brampton-cyber-security-innovation-centre/419025

Canada's biggest telco, the biggest bank and the federal government are among the backers contributing a combined $30 million to fund Ryerson Univesity's new cyber security innovation and collaboration centre west of Toronto.

Rogers Communications, the Royal Bank and Ottawa's FedDev Ontario agency said Friday they are helping to fund what will be called the Rogers Cybersecure Catalyst centre in downtown Brampton. Located in city hall, it's scheduled to open in November.

Click link above to read more

In new guide, spy agency warns campaign teams 'more likely' targets of cyber attacks

https://www.ctvnews.ca/politics/in-new-guide-spy-agency-warns-campaign-teams-more-likely-targets-of-cyber-attacks-1.4470357

OTTAWA – If you are working on a political campaign, are a candidate, or political volunteer, you are poised to be a prime target for attempted foreign interference and cyber attacks in the coming federal election.

That's the message from the Communications Security Establishment (CSE) in a newly released cyber guide for political campaigns.

Click link above to read more

New York Times: US ramping up cyber-attacks on Russia

https://www.cnn.com/2019/06/15/politics/us-ramping-up-cyberattacks-russia/index.html

The US is escalating cyber attacks on Russia's electric power grid and has placed potentially crippling malware inside the Russian system, The New York Times reported Saturday.

The placement of the malware that deep within the Russian grid had never previously been attempted, the Times reports, and is intended partly as a warning and also to put the US in a position to conduct cyber-attacks should a significant conflict arise with Russia.

Click link above to read more

Samsung's Smart TV Malware Scan Reminder Met by User Criticism

https://www.bleepingcomputer.com/news/security/samsungs-smart-tv-malware-scan-reminder-met-by-user-criticism/

Samsung issued a reminder for customers to scan their Internet-connected Smart QLED TVs for malware to prevent malicious campaigns from targeting their devices and use them as part of cyber attacks.

As the company said today on Twitter, "Scanning your computer for malware viruses is important to keep it running smoothly. This also is true for your QLED TV if it's connected to Wi-Fi!"

Smart Samsung TVs should be scanned for malware infections every few weeks using the built-in Smart Security solution that is designed to inspect the TVs and all connected storage devices for viruses.

Click link above to read more

Some BD Infusion Pumps Vulnerable to Remote Attacks

https://www.govinfosecurity.com/alerts-some-bd-infusion-pumps-vulnerable-to-remote-attacks-a-12634

Medical device vendor Becton Dickinson and U.S. federal regulators have issued security alerts about vulnerabilities that potentially put certain infusion pump products from the manufacturer at risk for remote hacker attacks.

Click link above to read more

Instagram Shows Kids' Contact Details in Plain Sight

https://www.govinfosecurity.com/instagram-shows-kids-contact-details-in-plain-sight-a-12631

Tens of thousands of minors on Instagram expose their email addresses and phone numbers to the public, a situation that child-safety and privacy experts say could be exploited by scammers or predators.

David Stier, a San Francisco-based data scientist and business adviser who recently brought a data exposure issue to Instagram's attention, uncovered the situation.

Click link above to read more

Google Researcher Details Windows Cryptographic Library Bug

https://www.govinfosecurity.com/google-researcher-details-windows-cryptographic-library-bug-a-12622

A Google security researcher has disclosed what he calls an unpatched bug in the main cryptographic library used in newer versions of the Windows operating system that he claims could affect an entire fleet of Windows-based devices.

Tavis Ormandy, a researcher with Google Project Zero, says he first took notice in March of the bug in Microsoft's SymCrypt, an open source project that forms the core cryptographic function library currently included in newer version of Windows, including Windows 8 and Window 10.

Click link above to read more.

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