Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer

# May 28th, 2019

**Try our May quiz - Security By The Numbers**

**Get Ready for Security Day - June 13, 2019**

**This week's stories:**

- **Nearly 100 malicious email campaigns aimed at Canadian organizations in Q1** 🇨🇦
- **Social media giants focus of three-day parliamentary hearing in Ottawa** 🇨🇦
- **Trudeau government unveils plans for digital overhaul** 🇨🇦
- **Google admits two password hash blunders, one dating back 14 years**
- **Huawei security and privacy chief calls for government collaboration**
- **Owner of Defunct Firm Fined in LeakedSource.com Case**
- **Misconfigured IT (Again) Leads to Big Health Data Breach**
- **Facebook removes 3 billion fake accounts — unclear if the problem is getting better**
- **Tech-savvy Estonia sets example of online voting as EU elections begin**
- **New Bitcoin Scam Leads to Ransomware and Info-Stealing Trojans**
- **Manufacturing spending billions on IoT, but still can't patch Windows or remember passwords**

## Nearly 100 malicious email campaigns aimed at Canadian organizations in Q1 🇨🇦

https://www.itworldcanada.com/article/nearly-100-malicious-email-campaigns-aimed-at-canadian-organizations-in-q1-report/418318

IT security experts say they still come across business leaders in Canada who don't believe their organization will be targeted for a cyber attack. A new report from security vendor Proofpoint should help dispell that.

Looking at data from customer devices, the company found that between January 1 and May 1, threat actors conducted thousands of malicious email campaigns, hundreds of which were sent to Canadian organizations.

**Click link above to read more**

## Social media giants focus of three-day parliamentary hearing in Ottawa

https://www.itworldcanada.com/article/social-media-giants-focus-of-three-day-parliamentary-hearing-in-ottawa/418387

The invitations have been sent to chief executives of some of the world's biggest social media platforms, but no one knows who will show up for the start tonight of a three-day parliamentary committee meeting in Ottawa before a group of elected representatives from 13 countries.

Subpoenas went out in February to Facebook, Twitter, Google, Microsoft, Amazon and Apple. Those subpoenas are only effective to people in Canada, and Mark Zuckerberg, Tim Cook, Jeff Bezos and others mainly live in the U.S. Whether companies will send their CEOs or lower-level executives will only be known at 8:30 a.m. when the House of Commons standing committee on access to information, privacy and ethics convenes.

**Click link above to read more**

---

## Trudeau government unveils plans for digital overhaul

https://www.cbc.ca/news/politics/digital-internet-canada-laws-1.5143522

Prime Minister Justin Trudeau's government set the stage Tuesday for an overhaul of Canada's laws governing the internet and digital privacy.

Innovation Minister Navdeep Bains today unveiled elements of the government's long-awaited digital strategy. Among other things, the strategy includes a digital charter that guarantees Canadians data portability — the ability of consumers to retain data when changing services.

Bains said the ten-point digital charter will lay out the government's basic principles for online governance, including universal access, safety and security, user control over personal data, transparency and portability and keeping digital platforms free from hate and violent extremism.

**Click link above to read more**

---

## Google admits two password hash blunders, one dating back 14 years

https://www.itworldcanada.com/article/google-admits-two-password-hash-blunders-one-dating-back-14-years/418254

Google likes to boast about its security, but on Tuesday it admitted making two password hash storage blunders. one of which dates back to 2005. For a number of unnamed organizations and users, passwords weren't hashed, making it possibly easier for them to be cracked.

As a result, an unknown number of G Suite administrators have been told all users have to reset their passwords.

The problems only affect the paid enterprise G Suite and not the free consumer Google accounts.

**Click link above to read more**

---

## Huawei security and privacy chief calls for government collaboration

https://www.itworldcanada.com/article/huawei-security-privacy-chief-calls-for-government-collaboration/418171

Amid the ongoing controversies about his employer, Huawei's global cyber security and privacy officer (GSPO) John Suffolk is frequently in the hot seat. He oversees 170 countries where Huawei equipment is deployed by 1,700 customers; Huawei says that one-third of the world's mobile traffic passes through its equipment.

**Click link above to read more**

---

## Owner of Defunct Firm Fined in LeakedSource.com Case

https://www.databreachtoday.com/owner-defunct-firm-fined-in-leakedsourcecom-case-a-12516

The former owner of the company behind the LeakedSource.com website, which trafficked in billions of stolen login credentials, will pay a fine equivalent to the money he made off the scam, according to the Royal Canadian Mounted Police.

Evan Bloom of Thornhill, Ontario, who owned Defiant Tech, had been charged with trafficking in identity information, unauthorized use of computer, mischief to data and possession of property obtained by crime, according to a 2018 police statement.

**Click link above to read more**

---

### Misconfigured IT (Again) Leads to Big Health Data Breach

https://www.databreachtoday.com/misconfigured-again-leads-to-big-health-data-breach-a-12511

An all-too-common type of data security mistake - a misconfigured IT setting - has landed a Puerto Rico-based clearinghouse and cloud software services provider at the top of federal regulators' list of largest health data breaches so far this year, in an incident impacting nearly 1.6 million individuals.

According to a posting added Tuesday onto the Department of Health and Human Services' HIPAA Breach Reporting Tool website, San Juan-based Immediate Health Group reported to HHS' Office for Civil Rights on April 24 a misconfiguration incident as an "unauthorized access/disclosure" breach involving a network server impacting 1.56 million individuals.

**Click link above to read more.**

---

### Facebook removes 3 billion fake accounts — unclear if the problem is getting better

https://globalnews.ca/news/5307160/facebook-3-billion-fake-profiles/

Facebook removed more than 3 billion fake accounts from October to March, twice as many as the previous six months, the company said Thursday.

Nearly all of them were caught before they had a chance to become “active” users of the social network.

Nonetheless, Facebook’s new report didn’t say how many fake accounts it also missed. As a result, it’s not clear whether Facebook is getting better at catching made-up accounts or if the problem itself is just getting worse — or both.

The increase in removals shows the challenges Facebook faces in removing accounts created by computers to spread spam, fake news and other objectionable material. Even as Facebook’s detection tools get better, so do the efforts by the creators of these fake accounts.

**Click link above to read more**

---

### Tech-savvy Estonia sets example of online voting as EU elections begin

https://globalnews.ca/news/5295587/estonia-online-voting/

Estonia was crippled by cyberattacks on government networks during a dispute with Russia in 2007. Today the tiny tech-savvy nation is so certain of its cyber defenses that it is the only country in the world to allow internet voting for the entire electorate, in every election, and thousands have already done so in the European Parliament elections.

Internet voting — or i-voting —has been available since 2005 in the nation that gave the world Skype, and the percentage of voters using the internet to cast ballots has increased with each election, reaching 44 per cent of voters in a national election in March.

**Click link above to read more**

---

## New Bitcoin Scam Leads to Ransomware and Info-Stealing Trojans

https://www.bleepingcomputer.com/news/security/new-bitcoin-scam-leads-to-ransomware-and-info-stealing-trojans/

A series of web sites are pushing a scam promising $5-30 worth of free bitcoins a day simply by running their Bitcoin Collector program. In reality, this program does nothing but install ransomware or password-stealing Trojans onto a victim's computer.

This scam was first discovered by a malware researcher going by the alias Frost who posted about it on Twitter and discussed it with BleepingComputer.com.

The scam is promoted through sites that promise to earn you Ethereum by referring other people to their site.  Their FAQ states that by referring 1,000 visits using your referral link you will earn 3 Ethereum, which is worth approximately $750 USD.

**Click link above to read more**

---

## Manufacturing spending billions on IoT, but still can't patch Windows or remember passwords

https://www.itworldcanada.com/article/manufacturing-spending-billions-on-iot-but-still-cant-patch-windows-or-remember-passwords/418175

When more than 200 business leaders and IT specialists were asked if they knew the password policies of the various systems running in their building, or in some cases, parts of the building itself, the silence at the recent Data Connectors event in Toronto was deafening. Two people raised their hand, says the man who posed the question – Tony Anscombe, global security evangelist at ESET. Even those two didn't seem very confident.

**Click link above to read more**

---

**Click Unsubscribe to stop receiving the Digest.**

**************************************************************************************************************************

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.