March 5th, 2019

March is Fraud Awareness Month

This week’s stories:

- **Facebook Pressured Canadian Officials To Skirt Privacy Rules: U.K. Media Reports**
  
  [https://www.huffingtonpost.ca/2019/03/04/facebook-pressured-canadian-officials-to-skirt-privacy-laws-u-k-media-reports_a_23684253/?utm_hp_ref=ca-homepage](https://www.huffingtonpost.ca/2019/03/04/facebook-pressured-canadian-officials-to-skirt-privacy-laws-u-k-media-reports_a_23684253/?utm_hp_ref=ca-homepage)

  TORONTO — NDP MP Charlie Angus is calling for an investigation into Facebook's conduct following U.K. media reports that alleged a former federal infrastructure minister was pressured into making privacy commitments in order to land a Facebook data centre in Canada.

  In a letter to the federal lobbying commissioner Nancy Belanger, Angus said he would like the government to look into reports from The Observer and Computer Weekly that allege former Conservative minister Christian Paradis assured Facebook Canada the government would not seek jurisdiction over non-Canada data if a data centre was constructed in Canada.

  **Click link above to read more**

- **Comcast set mobile pins to “0000,” helping attackers steal phone numbers**
  

  A bad security decision by Comcast on the company's mobile phone service made it easier for attackers to port victims’ cell phone numbers to different carriers.

  Comcast in 2017 launched Xfinity Mobile, a cellular service that uses the Verizon Wireless network and Comcast Wi-Fi hotspots. Comcast has signed up 1.2 million mobile subscribers but took a shortcut in the system that lets users switch from Comcast to other carriers.
Formjacking: The newest way hackers are stealing credit card information
https://globalnews.ca/news/5017232/formjacking-hack-steal-credit-card-information/

2018 was the year of ransomware, phishing scams and the cryptocurrency hack known as cryptojacking. Come 2019 however, hackers have a new weapon in their arsenal — formjacking.

According to the Symantec Internet Security Threat Report, as security companies get better at preventing common scams, instances of formjacking have skyrocketed, with an average of almost 5,000 websites per month becoming victim to a formjacking attack during 2018.

Facebook sues 3 people, 4 companies in China for pushing sale of fake likes, followers, accounts

Facebook and Instagram have sued three people and four companies based in the People’s Republic of China, alleging that they promoted the sale of fake likes, followers and accounts on both sites.

The lawsuit, filed in U.S. Federal Court, alleges that this also happened on other online service providers including Google, Apple, Amazon, LinkedIn and Twitter.

What’s the issue with securing the 5G future?
https://globalnews.ca/news/5008787/issue-securing-5g-future/

The security of next-generation 5G networks has dominated this year’s Mobile World Congress in Barcelona, with conflicting views on the risks of moving to the new technology being debated on stage and in backroom meetings.

5G promises super-fast connections which evangelists say will transform the way we live our lives, enabling everything from self-driving cars to augmented-reality glasses and downloading a feature-length film to your phone in seconds.

How to avoid Fortnite V-bucks scams and cyber-criminal schemes

Mar. 4—Inside the super-popular online game Fortnite players must evade gunfire and rocket launcher attacks to be among the last ones standing in the multiplayer free-for-all.

But even bigger dangers involving the game await players in the real world.

Online profiteers hawking enhanced abilities for players’ Fortnite characters in exchange for their account login information could take over the account or, worse, steal credit card information in the account for fraud.

Alphabet’s Chronicle Startup Finally Launches—It’s Like Google Photos For Cybersecurity
It’s been a year since Alphabet, Google’s parent company, announced a moonshot cybersecurity company called Chronicle. No products have arrived until now, as Alphabet’s Chronicle announces Backstory.

It’s like Google Photos but for business’ network security, says Stephen Gillett, Chronicle’s CEO. “You dump everything in Google Photos, they structure it, they recognize faces, they give you themes, they store it in the cloud and allow you to understand it,” he told Forbes.

The Feds’ Favorite iPhone Hacking Tool Is Selling On eBay For $100—And It’s Leaking Data

When eBay merchant Mr. Balaj was looking through a pile of hi-fi junk at an auction in the U.K., he came across an odd-looking device. Easily mistaken for a child’s tablet, it had the word “Cellebrite” written on it. To Mr. Balaj, it appeared to be a worthless piece of electronic flotsam, so he left it in his garage to gather dust for eight months.

But recently he’s learned just what he had his hands on: a valuable, Israeli-made piece of technology called the Cellebrite UFED. It’s used by police around the world to break open iPhones, Androids and other modern mobiles to extract data. The U.S. federal government, from the FBI to Immigration and Customs Enforcement, has been handing millions to Cellebrite to break into Apple and Google smartphones. Mr. Balaj (Forbes agreed not to publish his first name at his request) and others on eBay are now acquiring and trading Cellebrite systems for between $100 and $1,000 a unit. Comparable, brand-new Cellebrite tools start at $6,000.

Microsoft Sees 250% Phishing Increase, Malware Decline by 34%

Phishing attacks have seen an impressive 250% increase between January and December 2018, with attackers moving to multiple points of attacks during the same campaign, switching between URLs, domains, and servers when sending e-mails and hosting phishing forms.

Threat actors have also begun to diversify the infrastructure they use to run phishing campaigns, with Microsoft observing as part of its Security Intelligence Report (SIR) Volume 24 that hosted servers and public cloud tools were adopted to make it easier to camouflage as legitimate services or products.
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.