This week’s stories:

Amazon, Microsoft, Apple pressured by lawmakers at Ottawa hearing on big data firms

Fredericton approves $100K in annual spending for cybersecurity upgrades

Facebook the target of international lawmakers at Ottawa hearing

Headhunting Firm Leaks Millions of Resumes, Client Private Data

Billing Details for 11.9M Quest Diagnostics Clients Exposed

New Phishing Scam Asks You to Manage Your Undelivered Email

GandCrab Ransomware Shutting Down After Claiming to Earn $2.5 Billion

Checkers, Rally’s Burger Joints Hit By POS Malware

Applicants Must Give Up Social Media Privacy for US Visa Approval

Google cuts Baltimore off Gmail as city officials struggle with RobinHood ransomware aftermath

Amazon’s Alexa could in your next apartment whether you like it or not

Amazon, Microsoft, Apple pressured by lawmakers at Ottawa hearing on big data firms


Fresh off squeezing Facebook earlier this week, an international panel of lawmakers meeting in Ottawa tried putting pressure on Amazon, Microsoft and Apple for topics ranging from alleged anti-competitive activity and their privacy practices.

And, like Facebook, their questions circled back to the fact that lower officials instead of CEOs of the companies subpoenaed didn’t show up.

Click link above to read more

Fredericton approves $100K in annual spending for cybersecurity upgrades


The City of Fredericton is boosting its cybersecurity system.
The city has agreed to pay $324,360 to local company Bulletproof Solutions to protect and improve the city's networks for the next three years.

Pricing for additional services including forensics, on-premise penetration testing and vulnerability assessments was redacted from the document that was made public for Monday night's city council meeting, when the agreement was approved.

Facebook the target of international lawmakers at Ottawa hearing


A testy group of international lawmakers peppered officials from Facebook, Google and Twitter at a parliamentary committee meeting Tuesday, trying to pin the social media giants down on how they will prevent fake news from disrupting democracy in their countries.

The session was a combined meeting of the House of Commons privacy and ethics committee and the International Grand Committee of lawmakers from a dozen countries on privacy, big data and democracy.

Headhunting Firm Leaks Millions of Resumes, Client Private Data


A misconfigured and publicly accessible ElasticSearch cluster owned by FMC Consulting, a Chinese headhunting company, leaked millions of resumes and company records, as well as customers and employees PII data.

The database containing hundreds of thousands of customer records, internal emails, as well as employees daily tasks and calls they made while contacting clients was left unprotected, exposing all the data to anyone who knew where and how to look for it.

Billing Details for 11.9M Quest Diagnostics Clients Exposed


Quest Diagnostics Incorporated, a Fortune 500 diagnostic services provider, says that approximately 12 million of its clients may have been impacted by a data breach reported by one of its billing providers.

The company reported to the U.S. Securities and Exchange Commission (SEC) that it received a notification from its billing collection provider American Medical Collection Agency (AMCA) that their web payment page was breached.

New Phishing Scam Asks You to Manage Your Undelivered Email


A new phishing campaign is underway that pretends to be a list undelivered email being held for you on your Outlook Web Mail service. Users are then prompted to decide what they wish to do with each mail, with the respective links leading to a fake login form.
Recently, we have seen quite a few interesting spam campaigns such as account cancellation notices and alerts about unusual volumes of file deletions.

**GandCrab Ransomware Shutting Down After Claiming to Earn $2.5 Billion**


After almost a year and a half, the operators behind the GandCrab Ransomware are shutting down their operation and affiliates are being told to stop distributing the ransomware.

Filling the gaps left behind by the shutdown of large scale ransomware operations such as TeslaCrypt, CryptoWall, and Spora, GandCrab exploded into the ransomware world on January 28th, 2018, when they started marketing their services on underground criminal sites.

**Checkers, Rally's Burger Joints Hit By POS Malware**


Checkers Drive-In Restaurants, which also runs Rally's, says 102 of its 900 U.S. locations were hit with point-of-sale malware, with one California restaurant infected over a more than two-year period starting in December 2015.

Checkers, which was acquired by private equity firm Oak Hill Capital Partners in 2017, says it "recently" became aware of the malware and is taking steps to remove it.

**Applicants Must Give Up Social Media Privacy for US Visa Approval**

[https://hotforsecurity.bitdefender.com/blog/applicants-must-give-up-social-media-privacy-for-us-visa-approval-21302.html](https://hotforsecurity.bitdefender.com/blog/applicants-must-give-up-social-media-privacy-for-us-visa-approval-21302.html)

Be cautious with your digital presence as you might now have to share it with the US State Department. As of Friday, millions of US immigrant and non-immigrant visa seekers will have to submit their social media history, email addresses and phone numbers dating back five years, including travel history and family affiliation with terrorism, as per a new State Department policy, writes The New York Times.

Providing all "social media identifiers" is part of the screening and vetting strategy advanced by the Trump administration in March of 2018. If any social channels are missing from the list, visa applicants are expected to volunteer account information.

**Google cuts Baltimore off Gmail as city officials struggle with RobinHood ransomware aftermath**


The city of Baltimore in the US State of Maryland continues to struggle with the aftermath of a cyber incident incurred earlier this month, when attackers held municipal systems at ransom.
The RobbinHood ransomware attack on May 7 froze administrative transactions, payments and communication, leaving the city struggling to recover after officials refused to pay attackers’ ransom demands.

Two weeks after the attack, the city still couldn’t send and receive emails, but officials said they were making extensive efforts to regain control of the systems.

Click link above to read more

Amazon’s Alexa could in your next apartment whether you like it or not
https://reclaimthenet.org/amazon-alexa-preinstalled-apartments/

Just as many other modern homes in the U.S., the apartments at the Brandon Place complex in Oklahoma City are highly automated. There are smart locks on doors and thermostats with touch-screens, and new tenants will be informed in the move-in briefing that these smart systems can be operated through Amazon’s Alexa-powered devices.

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.

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