April 2nd, 2019

This week's stories:

- How a Halifax cafe endured a Facebook page hi-jacking
- Get meaningful consent when collecting voter data, federal parties told
- Government issues cyber security guide for SMBs
- Prague airport to get more facial recognition cameras
- Saudis hacked Amazon chief Jeff Bezos's phone, says company's security adviser
- New York Albany Capital Hit by Ransomware Attack
- IoT Attacks Escalating with a 217.5% Increase in Volume
- Ironically, Phishing Kit Hosted on Nigerian Government Site
- Toyota Security Breach Exposes Personal Info of 3.1 Million Clients
- Huawei Security Shortcomings Cited by British Intelligence

How a Halifax cafe endured a Facebook page hi-jacking

https://www.itworldcanada.com/article/how-a-halifax-cafe-endured-a-facebook-page-hi-jacking/416417

Halifax's Humani-T Cafe had its Facebook page revived this week after a lengthy take-over of the site during which the vegan restaurant suffered the indignity of having an attacker place odd videos of a half-naked person eating steak.

Now company co-owner Kiyan Sobhani has to begin rebuilding the hundreds of thousands of followers he said the page had before it was taken over.

For Sobhani there are two questions: How was the page hacked, and why did it take Facebook so long to help him?

Click link above to read more

Get meaningful consent when collecting voter data, federal parties told

https://www.itworldcanada.com/article/get-meaningful-consent-when-collecting-voter-data-federal-parties-told/416504

Canada's federal political parties are being encouraged to play it straight with the personal information of voters they hold.

The advice came Monday from federal privacy commissioner Daniel Therrien and chief electoral officer Stéphane Perrault ahead of October's national election.

Click link above to read more

Government issues cyber security guide for SMBs

https://www.itworldcanada.com/article/government-issues-cyber-security-guide-for-smbs/416464

Small and mid-sized companies face a dilemma when it comes to cyber security: If they can't afford full-time infosec experts to effectively defend themselves, what and how much can they afford to do?

To answer, the government hopes, is in a new guide issued by the Canadian Centre for Cyber Security. The Centre is the recently-established federal advisory agency on security. It's a unit of the Communications Security Establishment, responsible for securing federal departments.

Click link above to read more.

Prague airport to get more facial recognition cameras

https://www.canadiansecuritymag.com/news/transportation/prague-airport-to-get-more-facial-recognition-cameras

PRAGUE, Czech Republic — The Czech government says it has approved a plan to expand use of facial recognition cameras at Prague's international airport. The government agreed to deploy the cameras across Prague's Vaclav Havel airport, having previously approved their installation for the transit areas.

The move will increase the total numbers of cameras from 100 to 145. The government boosted security at the airport more than a year ago by deploying 200 more officers. The government is also planning to boost security measures at the country's remaining international airports.

Click link above to read more

Saudis hacked Amazon chief Jeff Bezos's phone, says company's security adviser

https://www.theguardian.com/technology/2019/mar/31/saudis-hacked-amazons-jeff-bezos-phone-claims-security-chief-jamal-khashoggi-mohammed-bin-salman

The security chief for Jeff Bezos, chief executive of Amazon, says the Saudi government had access to Bezos's phone and gained private information from it.

Gavin de Becker, Bezos's longtime security consultant, said he had concluded his investigation into the publication in January of leaked text messages between Bezos and Lauren Sánchez, a former television anchor whom the US National Enquirer tabloid newspaper said Bezos was dating.

Click link above to read more

New York Albany Capital Hit by Ransomware Attack

https://www.bleepingcomputer.com/news/security/new-york-albany-capital-hit-by-ransomware-attack/

The City of Albany, the capital of the U.S. state of New York, was hit by a ransomware attack on March 30, with city officials working over the weekend to respond to the incident.

At the time, the extent of the damages suffered by the city's computing systems is not yet known but, according to a press release available on the official site of the New York's Capital City, all city services will be available to the public except "Birth Certificates, Death Certificates, or Marriage Certificates."

Click link above to read more

IoT Attacks Escalating with a 217.5% Increase in Volume

https://www.bleepingcomputer.com/news/security/iot-attacks-escalating-with-a-2175-percent-increase-in-volume/

Attacks against Internet of Things (IoT) devices and networks have been escalating throughout 2018 with 32.7 million IoT attacks having been detected during last year by SonicWall, while phishing saw a decrease in volume with most of the attacks being targeted.

While everyone wants to have their devices interconnected and connected to the Internet, many of the estimated 31 billion IoT devices that will be installed by 2020 according to Statista will also come with easy to abuse or no security controls.

Click link above to read more

Ironically, Phishing Kit Hosted on Nigerian Government Site

https://www.bleepingcomputer.com/news/security/ironically-phishing-kit-hosted-on-nigerian-government-site/

Those who remember earlier days of the internet are familiar with the “Nigerian Prince letter,” also known as the 419 scam. While that fraud typically runs from personal email accounts, another one uses an official Nigerian government website to host a phishing page for the DHL international courier service.

Click link above to read more

Toyota Security Breach Exposes Personal Info of 3.1 Million Clients

https://www.bleepingcomputer.com/news/security/toyota-security-breach-exposes-personal-info-of-31-million-clients/

The personal information of roughly 3.1 million Toyota customers may have been leaked following a security breach of multiple Toyota and Lexus sales subsidiaries, as detailed in a breach notification issued by the car maker today.

As detailed in a press release published on Toyota'a global newsroom, unauthorized access was detected on the computing systems of Tokyo Sales Holdings, Tokyo Tokyo Motor, Tokyo Toyopet, Toyota Tokyo Corolla, Nets Toyota Tokyo, Lexus Koishikawa Sales, Jamil Shoji (Lexus Nerima), and Toyota West Tokyo Corolla.

Click link above to read more

Huawei Security Shortcomings Cited by British Intelligence

https://www.databreachtoday.com/huawei-security-shortcomings-cited-by-british-intelligence-a-12279

Britain's intelligence establishment has concluded that Chinese networking giant Huawei's "software engineering and cybersecurity processes" continue to be beset by unresolved "defects." In addition, engineering and risk management improvements that the U.K. government has demanded of Huawei, which it has promised to make, have yet to be put in place.

Click link above to read more

---

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