October 29th, 2019

October is "Cybersecurity awareness" Month

Try our October quiz – Fake or Not

Don't miss Security Day! - "The Humans of Security", Nov 20, 2019

This week's stories:

- **Unpacking the cybersecurity gap**
- **Bank of Canada exploring digital currency that would replace cash, track how people spend money**
- **Not all fun and memes: What's the trouble with TikTok?**
- **Tracking down the developer of Android adware affecting millions of users**
- **TrialWorks Ransomware Attack Disrupts Court Cases and Deadlines**
- **Hackers finding ways to exploit automotive software to overtake cars**
- **Ransomware with a difference as hackers threaten to release city data**
- **Steam-powered scammers**
- **These watchdogs track secret online censorship across the globe**
- **Is Voting by Mobile App a Better Security Option or Just 'A Bad Idea'?**

Unpacking the cybersecurity gap

https://www.theglobeandmail.com/business/adv/article-unpacking-the-cybersecurity-gap/

In 2019, it seems that barely a week goes by without news of a company being hacked. In July, financial giant Capital One was the victim of a huge breach, with a hacker stealing the personal data of six million Canadians, including one million social insurance numbers. In May, it was graphic design site Canva. Popular encrypted messaging app WhatsApp was hit just days before.

But these well-publicised incidents are only the tip of the iceberg. According to the most recent data from Statistics Canada, more than a fifth of Canadian businesses experienced a cybersecurity breach that affected their operations. And it's not just the big players: A 2019 Verizon report from the U.S. found that 43 per cent of attacks involve small businesses.

Click link above to read more

Bank of Canada exploring digital currency that would replace cash, track how people spend money

https://business.financialpost.com/technology/blockchain/bank-of-canada-exploring-digital-currency-that-would-replace-cash-track-how-people-spend-money

An internal Bank of Canada presentation says benefits of a digital currency include the sharing of personal information with police or tax authorities.

The Bank of Canada is considering launching a digital currency that would help it combat the “direct threat” of cryptocurrencies and collect more information on how people spend their money, The Logic has learned.

Click link above to read more

Not all fun and memes: What’s the trouble with TikTok?

https://www.cbc.ca/news/technology/tiktok-criticism-expansion-in-canada-1.5336375

Chinese video-sharing app plans Canadian expansion, faces allegations of censorship and intelligence-gathering.

It's been a bad week for TikTok. The Chinese-owned video-sharing app, wildly popular with teens, was forced to issue a rare public statement about its data security practices and whether it censors content on behalf of Beijing.

Click link above to read more

Tracking down the developer of Android adware affecting millions of users

https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

We detected a large adware campaign running for about a year, with the involved apps installed eight million times from Google Play alone.

We identified 42 apps on Google Play as belonging to the campaign, which had been running since July 2018. Of those, 21 were still available at the time of discovery. We reported the apps to the Google security team and they were swiftly removed. However, the apps are still available in third-party app stores. ESET detects this adware, collectively, as Android/AdDisplay.Ashas.

Click link above to read more

TrialWorks Ransomware Attack Disrupts Court Cases and Deadlines

https://www.bleepingcomputer.com/news/security/trialworks-ransomware-attack-disrupts-court-cases-and-deadlines/

TrialWorks, one of the top-rated providers of legal case management software for law firms and attorneys, became the victim of a ransomware attack earlier this month.

The ripples of disruption from this incident made it impossible for lawyers to access the legal documents hosted on TrialWorks’ platform.

Click link above to read more

Hackers finding ways to exploit automotive software to overtake cars

https://www.techrepublic.com/article/hackers-finding-ways-to-exploit-automotive-software-to-overtake-cars/

Over the last ten years cars have become packed full of new technology that makes it easier to play music and movies, take calls, or get directions all from your dashboard. But this digitization has come at a cost, giving cybercriminals a seemingly endless amount of access points to take over vehicles.

Cybersecurity firm IntSights recently released, "Under The Hood: Cybercriminals Exploit Automotive Industry's Software Features," a study on how hackers are managing to get into cars and do damage.

Click link above to read more

Ransomware with a difference as hackers threaten to release city data

https://nakedsecurity.sophos.com/2019/10/28/johannesburg-hit-by-second-malware-attack/

Johannesburg spent the weekend struggling to recover from its second cyberattack this year as it took key services systems offline.

The cyberattack came from a group calling itself the Shadow Kill Hackers. Some media outlets are reporting it as a ransomware attack, but according to a note reportedly sent to city employees and shared on Twitter, the hackers didn't encrypt data. Instead, they stole it and threatened to upload it to the internet if the City didn't pay up.

Click link above to read more

Steam-powered scammers

https://securelist.com/steam-powered-scammers/94553/

Digital game distribution services have not only simplified the sale of games themselves, but provided developers with additional monetization levers. For example, in-game items, such as skins, equipment, and other character-enhancing elements as well as those that help one show up, can be sold for real money. Users themselves can also sell items to each other, with the rarest fetching several thousand dollars. And where there's money, there's fraud. Scammers try to get hold of login details to "strip" the victim's characters and sell off their hard-earned items for a juicy sum.

One of the most popular platforms among users (and hence cybercriminals) is Steam, and we've been observing money-making schemes to defraud its users for quite some time. Since June, however, such attacks have become more frequent and, compared to previous attempts, far more sophisticated.

Click link above to read more

These watchdogs track secret online censorship across the globe

https://www.cnet.com/features/the-watchdogs-tracking-secret-online-censorship-across-the-globe-ooni/

Shortly after leaving Ethiopia's Bole Addis Ababa International Airport in a ride-hail car earlier this year, Moses Karanja faced an awkward situation: He couldn't pay his driver. While he was riding into town, the state-controlled telecom shuttered internet access, rendering the app useless. Neither Karanja nor the driver knew how much his trip should cost.

Karanja, a University of Toronto Ph.D. student, fished out some cash and came to an agreement with the driver. But the outage, which followed a series of assassinations in the country in June, prompted Karanja to look at how deep and long the shutdown was. He suspected some services, like WhatsApp, remained down even when other parts of the web came back up several days after the killings.

Click link above to read more

Is Voting by Mobile App Better Security Option or Just 'A Bad Idea'?

https://www.darkreading.com/edge/theedge/is-voting-by-mobile-app-a-better-security-option-or-just-a-bad-idea/b/d-id/1336152

Security experts say voting by app adds another level of risk, as mobile-voting pilots expand for overseas military and voters with disabilities.

Paper ballots and risk-limiting audits – the manual sampling of votes – have become the new best practices for protecting US elections in the aftermath of Russia's election meddling and hacking of voter registration databases during the 2016 presidential campaign.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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