Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

October 30th, 2018

October is "Cybersecurity awareness" Month
Test yourself with the Cybersecurity Awareness Month Quiz: Cybersecurity by the Numbers

This week's stories:

- EXCLUSIVE: Stats Canada requesting banking information of 500,000 Canadians without their knowledge
- Government failing to protect Canadians from cyber threats, says Senate report
- Cyber Security Awareness Month: Tips from experts
- Android voice mail scam, bad apps in Google Store
- BankIslami Customers Lose Over $6 Million in Biggest Security Breach in Pakistan's History
- Chinese and Russian spies routinely eavesdrop on Trump's iPhone calls
- Russia was likely behind dangerous critical infrastructure attack, report says
- Gabon official websites hacked: Anonymous group
- Primer: 4 ways to protect your devices from botnets
- Iranian Hackers Hit U.K. Cybersecurity Universities

EXCLUSIVE: Stats Canada requesting banking information of 500,000 Canadians without their knowledge

https://globalnews.ca/news/4599953/exclusive-stats-canada-requesting-banking-information-of-500000-canadians-without-their-knowledge/?utm_source=Article&utm_medium=EditorsPick&utm_campaign=2015

Statistics Canada is asking banks across the country for financial transaction data and personal information of 500,000 Canadians without their knowledge, Global News has learned.

Documents obtained by Global News show the national statistical agency plans to collect "individual-level financial transactions data" and sensitive information, like social insurance numbers (SIN), from Canadian financial institutions to develop a "new institutional personal information bank."

Click link above to read more

Government failing to protect Canadians from cyber threats, says Senate report

https://www.itworldcanada.com/article/government-failing-to-protect-canadians-from-cyber-threats-says-senate-report/410906

The federal government is failing to protect Canadians from increasingly sophisticated cyber attacks that have already victimized millions, according to a scathing Senate committee report released this morning that calls for the creation of a minister of cyber security.

Click link above to read more

Cyber Security Awareness Month: Tips from experts

https://www.itworldcanada.com/article/cyber-security-awareness-month-tips-from-experts/410867

Making sure your employees are following best computer security practices and company policies is a daunting task.

As Cyber Security Awareness Month draws to a close we talked to a number experts about what they've learned. Here are their tips:

Click link above to read more

Android voice mail scam, bad apps in Google Store

https://www.itworldcanada.com/article/cyber-security-today-oct-26-2018-android-voice-mail-scam-bad-apps-in-google-store/410834

Hackers are increasingly targeting smart phones. According to McAfee the latest scam is sending Android device owners a text message saying they've got a voice mail, but they need to click on a link to download an app to hear it. The app is really malware that can open a backdoor from the phone or tablet to your home or business computer. This con has been running since at least March, with an estimated 5,000 victims in the U.S. so far. The best defence: Beware of text messages from strangers, and only download an app you know a lot about, and from a safe web site.

Click link above to read more

BankIslami Customers Lose Over $6 Million in Biggest Security Breach in Pakistan's History

https://propakistani.pk/2018/10/29/bankislami-customers-lose-over-6-million-in-biggest-security-breach-in-pakistans-history/

A Pakistani bank has reportedly come under what seems to be one of the biggest cyber attacks in the country's history. As per our sources, a group of hackers (or more) have breached the data center of Bank Islami and stolen the data of thousands of customers.

The alleged security breach first came to light on October 27 when customers of the bank received automated messages about their payment cards being used in different countries. The bank denied that any data theft took place.

Click link above to read more

Chinese and Russian spies routinely eavesdrop on Trump's iPhone calls

https://arstechnica.com/tech-policy/2018/10/nyt-chinese-and-russian-spies-routinely-eavesdrop-on-trumps-iphone-calls/

Chinese and Russian spies routinely eavesdrop on personal phone calls President Trump makes on his iPhones, one of which is no different from the smartphone millions of other people use. The US president's casual approach to electronic security has several current and former officials so frustrated they leaked the details to *The New York Times*, which reported on the phone interceptions Wednesday evening.

Click link above to read more

Russia was likely behind dangerous critical infrastructure attack, report says

https://arstechnica.com/information-technology/2018/10/russia-was-likely-behind-dangerous-critical-infrastructure-attack-report-says/

Malware that caused a dangerous operational failure inside a Middle Eastern critical infrastructure facility was most likely developed by a Russian government-backed research institute, researchers from US security firm FireEye said Tuesday.

The malware, alternately dubbed Triton and Trisis, was most likely designed to cause physical damage inside critical infrastructure sites, such as gas refineries and chemical plants, FireEye researchers said in a report published in December. The attack worked by tampering with a safety instrumented system, which the targeted facility and many other critical infrastructure sites use to prevent unsafe conditions from arising. FireEye's December report said a nation-state was most likely behind the attack but stopped short of identifying the country.

Click link above to read more

Gabon official websites hacked: Anonymous group

https://www.vanguardngr.com/2018/10/gabon-official-websites-hacked-anonymous-group/

The Anonymous hackers collective on Sunday claimed it hacked into the websites of more than 70 Gabon government sites, saying its action targeted dictatorships. Government sites including the ministries of communications and the civil service were inaccessible on Sunday, as were the websites of at least 30 other institutions, though there was no independent confirmation of the Anonymous claim.

Click link above to read more

Primer: 4 ways to protect your devices from botnets

https://www.the-parallax.com/2018/10/26/primer-4-ways-protect-devices-botnet

When a massive cyberattack took down many major websites in 2016—including those of Amazon.com, HBO, Netflix, The New York Times, and Spotify—authorities feared that it may have been the work of a hostile nation-state. But the culprits turned out to be less interesting than the way the attack was carried out: More than 600,000 hacked devices flooded the Internet with more than 1 terabyte per second of junk data, in what came to be known as the Mirai botnet.

A botnet, or robot network, is a string of infected computers that carries out a task. Often, that task is a distributed denial-of-service attack to block access to a site or service, says David London, senior director at security and risk management advisory company The Chertoff Group. The word "computers" is loosely used today, he says, as botnets can infect servers, mobile devices, laptops and, in the case of Mirai, Internet-connected devices such as DVRs, cameras, and "smart" light bulbs and meters, collectively known as the Internet of Things.

Click link above to read more

Iranian Hackers Hit U.K. Cybersecurity Universities

https://www.forbes.com/sites/geoffwhite/2018/10/29/iranian-hackers-hit-u-k-cybersecurity-universities/#2478074531c9

Iranian cybercriminals tried to hack into U.K. universities offering government-certified cybersecurity courses, successfully accessing at least one university's accounts during a campaign lasting months.

The hacking group has targeted at least 18 British universities, according to researchers. The list includes top-flight institutions. But it also includes less well-known destinations which are notable for being among

a select group certified by the National Cyber Security Centre (NCSC) to provide degrees in cybersecurity.

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