Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

December 18th, 2018

December is Mobile Month

This week's stories:

- Bomb threats demanding Bitcoin investigated across Canada, U.S. 🇨🇦
- The average Cyber Security salary in Canada is now between $80 – $150k🇨🇦
- Regulate social media, says Canadian parliamentary committee 🇨🇦
- Maria Butina: Cybersecurity charlatan, spy
- Six Cyber Security Essentials To Protect Your Organisation
- Marriott cyber breach shows industry's hospitality to hackers
- In Bengaluru cyber crime station, one Inspector for 5,000 cases
- STEP FORWARD FOR £9M CYBER SECURITY CENTRE
- US ballistic missile systems have very poor cyber-security
- Cyber Hacks Could Cost Auto Industry $24 Billion, New Upstream Security Study Reports
- The Death of Emails Could Eradicate Cyber Crime In Conveyancing
- Facebook admits photo API bug, Irish privacy commission adds to its investigation
- Phishing Attack Pretends to be a Office 365 Non-Delivery Email
- 123456 Is the Most Used Password for the 5th Year in a Row

Bomb threats demanding Bitcoin investigated across Canada, U.S. 🇨🇦

https://globalnews.ca/news/4760045/canada-united-states-bomb-threats/

The RCMP is telling Canadians not to comply with threatening emails demanding Bitcoin after a wave of bomb threats were received across Canada and the U.S.

The RCMP said in a statement Thursday evening that it is aware of threats sent via email in which the sender threatens to detonate a bomb if the cryptocurrency ransom is not paid.

Click link above to read more

The average Cyber Security salary in Canada is now between $80 – $150k🇨🇦

https://www.vancouverisawesome.com/2018/12/14/cyber-security-education-nyit-vancouver/

Cyber Security is arguably one of the fastest growing professional fields in Canada's tech industry and there is currently a huge demand for jobs. Fortunately, Vancouver is home to one of the country's leading programs for Cyber Security and digital risk management education.

At New York Institute of Technology – Vancouver (NYIT), you'll gain a comprehensive understanding of computer security and its impact on networks, web services, infrastructure, cybersecurity, databases, and software design, preparing you for the job market and whatever surprises the digital world holds.

Click link above to read more

Regulate social media, says Canadian parliamentary committee 🇨🇦

https://www.itworldcanada.com/article/regulate-social-media-says-canadian-parliamentary-committee/412940

Social media platforms based in Canada should regulated by a law forcing them to delete "manifestly illegal content in a timely fashion" including hate speech harassment and disinformation, a parliamentary committee has recommended.

That was one of the recommendations made Tuesday by the House of Commons access to information, privacy and ethics committee into the impact social media platforms can have on democracy. The committee's work started with investigating allegations that personal information of some 87 million Facebook users – including Canadians — wound up in the hands of U.K. political analysis firm Cambridge Analytica.

Click link above to read more

Maria Butina: Cybersecurity charlatan, spy

https://www.engadget.com/2018/12/14/maria-butina-cybersecurity-charlatan-spy/

Russian spy Maria Butina's cover story was her academic interest and expertise in cybersecurity. As cover stories go, this unfortunately wasn't a hard one to pull off.

Except anyone holding even the barest minimum of cybersecurity knowledge could've figured out in minutes that Butina's interest in cybersecurity was minimal.

Click link above to read more

Six Cyber Security Essentials To Protect Your Organisation

https://www.cbronline.com/opinion/mariana-peycheva-cyber-security-essentials

As businesses and customers become more connected and digital-first, the need to protect cyber assets and personal information has become paramount.

Analysts estimate that by 2020, 60% of enterprises will be victims of a major cyber security breach. Whilst 74% of these attacks will be due to careless or uneducated employees, according to EY's Global Information Security Survey 2017, the remaining 26% are often highly sophisticated attacks, which are difficult to predict, identify and defend against.

Click link above to read more

Marriott cyber breach shows industry's hospitality to hackers

https://www.thestar.com.my/tech/tech-news/2018/12/17/marriott-cyber-breach-shows-industrys-hospitality-to-hackers/#t5WIwTDeWLfXj3oK.99

Long before Marriott International Inc disclosed a massive security breach, the hotel industry had earned the dubious reputation as a hospitable place for hackers.

Thieves have skimmed credit cards, looted loyalty accounts, and mounted complex schemes to trick clerks into downloading malicious software. In one elaborate series of attacks known as DarkHotel, networks at individual properties were hijacked to spy on corporate executives and politicians. In a cruder ploy, crooks have even seized control of a keyless entry system, locking down rooms until the hotel owner paid a ransom.

Click link above to read more

In Bengaluru cybercrime station, one Inspector for 5,000 cases

https://indianexpress.com/article/india/in-bengaluru-cyber-crime-station-one-inspector-for-5000-cases-5496539/

As cyber frauds involving the theft of small amounts of money increase with the spread of technology, senior officers estimate that the total is likely to cross 5,000 cases by the year-end, involving the loss of over Rs 10 crore, and double by the end of 2019.

Click link above to read more

STEP FORWARD FOR £9M CYBER SECURITY CENTRE

https://www.insidermedia.com/insider/midlands/step-forward-for-9m-cyber-security-centre

Plans for a new £9m Centre for Cyber Security in Hereford have taken a major step forward.

Herefordshire Council's cabinet has approved the launch of a new joint venture company with the University of Wolverhampton to build the centre at Skylon Park, creating 190 jobs and helping lead the UK's fight against cybercrime.

The university and council will make a loan of £5m to the new company in return for a shareholding.

The new centre will offer research facilities through the university's Wolverhampton Cyber Research Institute (WCRI) as well as providing office space for cyber businesses and advanced training facilities designed specifically to tackle threats in cyberspace.

As well as creating jobs, the centre will help attract inward investment and form part of a 'Cyber Triangle' with GCHQ in Cheltenham, the Government Cyber Centre in Newport, South Wales, and Qinetiq in Worcestershire.

The university has already secured grant funding of £4m from the Marches LEP Local Growth Fund and the European Regional Development Fund (ERDF).

Click link above to read more

US ballistic missile systems have very poor cyber-security

https://www.zdnet.com/article/us-ballistic-missile-systems-have-very-poor-cyber-security/

No data encryption, no antivirus programs, no multifactor authentication mechanisms, and 28-year-old unpatched vulnerabilities are just some of the cyber-security failings described in a security audit of the US' ballistic missile system released on Friday by the US Department of Defense Inspector General (DOD IG).

The report was put together earlier this year, in April, after DOD IG officials inspected five random locations where the Missile Defense Agency (MDA) had placed ballistic missiles part of the Ballistic Missile Defense System (BMDS) --a DOD program developed to protect US territories by launching ballistic missiles to intercept enemy nuclear rockets.

Click link above to read more

Cyber Hacks Could Cost Auto Industry $24 Billion, New Upstream Security Study Reports

https://www.prnewswire.com/news-releases/cyber-hacks-could-cost-auto-industry-24-billion-new-upstream-security-study-reports-815998175.html

Cyber hacks might cost the auto industry $24 billion within five years, according a new study released by Upstream Security, the first and only cloud-based Smart Mobility Cybersecurity provider.

Upstream issued its first comprehensive report studying the impact of more than 170 documented, Smart Mobility, cyber incidents reported between 2010-2018 and projects future trends based on that eight-year history.

Click link above to read more

The Death of Emails Could Eradicate Cyber Crime In Conveyancing

https://www.todaysconveyancer.co.uk/main-news/death-emails-eradicate-cyber-crime-conveyancing/

An expert has predicted that in only five years law firms will stop using emails to be replaced with a more secure means of communication.

Cybercrime is happening all the time and becoming more and more sophisticated. Law firms are particularly targeted due to a lot of sensitive information held on clients and their money – which provides for an extra juicy opportunity for fraudsters.

Conveyancing and probate are predominantly vulnerable to email fraud attacks as they deal with large amounts of money which are often being moved during transactions and administration of estates.

Click link above to read more

Facebook admits photo API bug, Irish privacy commission adds to its investigation

https://www.itworldcanada.com/article/facebook-admits-photo-api-bug-irish-privacy-commission-adds-to-its-investigation/413023

Under the microscope for a major data breach discovered in October and for allowing third party developers to access user information without sufficient consent, Facebook has found itself in hot water again.

After acknowledging on Friday that a bug in its photo API may have allowed third-party apps to access user's photos for 12 days in September, the Irish Data Protection Commission (DPC) said it is investigating the incident as part of a broader inquiry into the company.

The DPC has European jurisdiction over Facebook because the company's international headquarters is in Dublin.

Click link above to read more

Phishing Attack Pretends to be a Office 365 Non-Delivery Email

https://www.bleepingcomputer.com/news/security/phishing-attack-pretends-to-be-a-office-365-non-delivery-email/

A phishing campaign has been discovered that pretends to be a non-delivery notification from Office 365 that leads you to a page attempting to steal your login credentials.

This new campaign was discovered by ISC Handler Xavier Mertens and states that "Microsoft found Several Undelivered Messages". It then prompts you to click on the "Send Again" link in order to try sending the emails again. An example of this phishing email can be seen below.

Click link above to read more

123456 Is the Most Used Password for the 5th Year in a Row

https://www.bleepingcomputer.com/news/security/123456-is-the-most-used-password-for-the-5th-year-in-a-row/

For the 5th year in a row, "123456" is most used password, with "password" coming in at second place. Even in the wake of a constant stream of data breaches, hacks, and ransomware attack reports people continue to utilize weak passwords that not only put their information at jeopardy, but also their organization's data.

In SplashData's 8th annual worst passwords list, the password management company analyzed more than 5 million leaked passwords to come up with their list of most used passwords. According to their report, the top 10 most used passwords are:

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

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.

Information Security Branch
www.gov.bc.ca/informationsecurity
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer