Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO Office of the Chief Information Officer

April 23rd, 2019

Try our April quiz - Spotting a Fake

This week's stories:

- **Canadian cloud leaders may be among the least secure, report suggests** 🇨🇦
- **Canadian organizations still unprepared for a cyber incident, study suggests** 🇨🇦
- **Cyber Security Today: Beware of fake Notre Dame donation sites, protect domain name servers and iPhone users being tricked**
- **Britain proposes banning kids from liking social media posts**
- **Cybercrime's Total Earnings Skyrocketed to $2.7 Billion Says the FBI**
- **Medical Information of Almost 150K Rehab Patients Exposed**
- **Bodybuilding.com Security Breach, All Customer Passwords Reset**
- **The ransomware took The Weather Channel's live transmission offline for almost an hour.**
- **Facebook Marketplace Flaw Revealed Seller's Exact Location**
- **The FBI's RAT: Blocking Fraudulent Wire Transfers**

Canadian cloud leaders may be among the least secure, report suggests 🇨🇦

https://www.itworldcanada.com/article/canadian-cloud-leaders-may-be-among-the-least-secure-report-suggests/417174

Canadian organizations are increasingly moving data and workloads to the cloud. But if a recently-released study is representative, the leading firms in this movement are among the least secure.

"They think security is being taken care of soup-to-nuts, said David Senf, founder of the consulting firm Cyverity and author of the study. But, he added, "there is a shared responsibility between the organization and its cloud provider. That means I have to do something as well as you. And organizations have to understand what their side of the equation looks like. Because clearly there is an abdication of responsibility by organizations as they rush into the cloud."

Click link above to read more

Canadian organizations still unprepared for a cyber incident, study suggests 🇨🇦

https://www.itworldcanada.com/article/canadian-organizations-still-unprepared-for-a-cyber-incident-study-suggests/417196

May Canadian of organizations have cyber security incident response plans that are incomplete or untested, if responses to a new survey are representative.

In a global report issued earlier this month, 74 per cent of Canadian respondents said they do not have a response plan that is applied consistently across their entire enterprise.

Of those that do have a plan, 59 per cent said they do not test them regularly, or don't test at all.

Click link above to read more

Cyber Security Today: Beware of fake Notre Dame donation sites, protect domain name servers and iPhone users being tricked

https://www.itworldcanada.com/article/cyber-security-today-beware-of-fake-notre-dame-donation-sites-protect-domain-name-servers-and-iphone-users-being-tricked/417156

Criminals try to exploit whatever's hot in the news to sucker you into giving them money. Now there are fund-raising scams for the re-building of Notre Dame cathedral in Paris after this week's fire. According to security vendor ZeroFox. there are a number of fake donation sites. One of them on the JustGiving crowdfunding site is called 'Friends of Notre Dame de Paris.' You should also beware of social media messages with Notre Dame hashtags. There is a legitimate website called www.notredamedeparis.fr. Be cautious of unfamiliar individuals or organizations asking you to wire money or send money through a gift card. And check with these two websites that rate charities: Charity Watch, and Charity Navigator.

Click link above to read more

Britain proposes banning kids from liking social media posts

https://globalnews.ca/news/5167881/britain-kids-social-media-likes/

Britain's privacy regulator wants to stop kids from being able to "like" posts on Facebook and other social media sites as part of tough new rules it's proposing to protect children's online privacy.

Under the draft rules, which were released for consultation on Monday, tech companies would not be allowed to use "nudge techniques" that encourage children to keep using a site.

Click link above to read more.

Cybercrime's Total Earnings Skyrocketed to $2.7 Billion Says the FBI

https://www.bleepingcomputer.com/news/security/cybercrimes-total-earnings-skyrocketed-to-27-billion-says-the-fbi/

FBI's Internet Crime Complaint Center (IC3) published its 2018 Internet Crime Report which shows that cybercrime was behind $2,7 billion in total losses during 2018 as shown by 351,936 complaints received during the last year.

Since its inception in May 2000, IC3 says that it has received 4,415,870 complaints, with an average of around 300,000 complaints each year and roughly 900 per day. These resulted in a total loss of $7.45 billion over the last five years, between 2014 and 2018.

Click link above to read more

Medical Information of Almost 150K Rehab Patients Exposed

https://www.bleepingcomputer.com/news/security/medical-information-of-almost-150k-rehab-patients-exposed/

Over 4.91 million documents containing personally identifiable information (PII) of addiction rehab patients were exposed by a misconfigured ElasticSearch database publicly accessible for more than two years, from mid 2016 to late 2018.

The open database containing two indexes with 1.45 GB worth of data was found by Cloudflare Director of Trust and Safety Justin Paine while searching for exposed internet-enabled devices using Shodan.

Click link above to read more

Bodybuilding.com Security Breach, All Customer Passwords Reset

https://www.bleepingcomputer.com/news/security/bodybuildingcom-security-breach-all-customer-passwords-reset/

Bodybuilding.com fitness and bodybuilding fan website notified its customers of a security breach detected during February 2019 which was the direct result of a phishing email received back in July 2018.

As detailed in the data incident notification published on the company's help center, the security breach might "have affected certain customer information in our possession" and, as concluded after investigating the incident with the help of "external forensic consultants that specialize in cyber-attacks," Bodybuilding.com says that it "could not rule out that personal information may have been accessed."

Click link above to read more

The ransomware took The Weather Channel’s live transmission offline for almost an hour.

https://www.hackread.com/the-weather-channel-ransomware-attack-offline/

Another day, another ransomware attack; this time The Weather Channel suffered a powerful ransomware attack forcing its live TV telecast to go offline for 90 minutes.

The ransomware attack took place on April 18th at around 6:00 am, local time, when the channel was telecasting its live morning show “AMHQ.” The Weather Channel was then forced to replace its live transmission with advertisements and recorded footage of “Heavy Rescue: 401,” a Canadian reality TV show that follows the operations of multiple heavy vehicle rescue and recovery towing companies.

Click link above to read more

Facebook Marketplace Flaw Revealed Seller's Exact Location

https://www.databreachtoday.com/facebook-marketplace-flaw-revealed-sellers-exact-location-a-12402

Facebook has patched a flaw in its digital marketplace that could have been abused to identify the location of a seller, and by extension, their goods.

Facebook Marketplace, available via both the Facebook app and website, allows users to list items for sale.

Researcher John Moss was researching how he might scrape the Facebook Marketplace for information that could be useful for helping to recover stolen goods. But when researching the location data that the marketplace provided, he found that the JSON - JavaScript object notation - responses for advertisements that had been created with the Facebook mobile app were not approximate. Instead, Moss says in a blog post, the data included precise latitude and longitude coordinates.

Click link above to read more

The FBI's RAT: Blocking Fraudulent Wire Transfers

https://www.databreachtoday.com/blogs/fbis-rat-blocking-fraudulent-wire-transfers-p-2740

As much as it might seem like fighting internet crime is like pushing the tide with a broom, there is a bright spot in the gloom. In February 2018, the IC3 created what it terms the RAT, or Recovery Asset Team. Its goal is to contact financial institutions quickly to freeze suspicious pending wire transfers before they're final.

Much internet-enabled crime eventually intersects with banking systems. So while it may be difficult to prevent scams, there is a touch point where with industrywide cooperation, stolen funds can be recovered. But time is tight, and swiftly contacting financial institutions is key to stopping stolen funds from being withdrawn.

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer