Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

April 21, 2020

Try our April Quiz – Working Remotely

Save the Date for Security Day - http://www.gov.bc.ca/securityday

Cyber Safety for Mobile Workers Information Sheet

This week's stories:

- **Using COVID-19 Patient Data for Research: Sizing Up Risks**
- **Scammers exploiting stimulus payments with phishing attacks and malicious domains**
- **Understanding the dangers of social networking questionnaires**
- **Fraud guides a hot commodity on the dark web**
- **Zoom: A cheat sheet about the video conferencing solution**
- **Russian state hackers behind San Francisco airport hack**
- **Suspected cyber attack closes MSC's data centre**
- **Energy giant EDP hit with RagnarLocker ransomware**
- **Four Million Quidd User Credentials Found on the Dark Web**

Using COVID-19 Patient Data for Research: Sizing Up Risks

https://www.healthcareinfosecurity.com/using-covid-19-patient-data-for-research-sizing-up-risks-a-14111

In the effort to develop COVID-19 medical insights, some healthcare and technology firms are reportedly partnering to collect coronavirus patient information to assist government and academic researchers. But such efforts are raising significant security and privacy concerns.

Click link above to read more

Scammers exploiting stimulus payments with phishing attacks and malicious domains

https://www.techrepublic.com/article/scammers-exploiting-stimulus-payments-with-phishing-attacks-and-malicious-domains/

Since January, more than 4,000 domains related to coronavirus stimulus packages have been registered, many of them malicious or suspicious, according to Check Point Research.

Cybercriminals have been taking advantage of the coronavirus outbreak to target victims with malware in the guise of information relevant to the disease. These attacks typically take the form of malicious apps, phishing emails, and phony websites.

Click link above to read more

Understanding the dangers of social networking questionnaires

https://www.techrepublic.com/article/understanding-the-dangers-of-social-networking-questionnaires/?ftag=TREa988f1c&bhid=42420269&mid=12798383&cid=2176068089

With people spending more time on Facebook and Twitter, it's important to know what to watch out for. Jack Wallen addresses the social networking behaviors you should avoid at all costs.

This comes from the office of "I shouldn't have to say this," but in line with the idea of using a weak password, not employing a password manager or two-factor authentication, there are some things that simply bear repeating over and over Especially given our current climate.

Click link above to read more

Fraud guides a hot commodity on the dark web

https://www.techrepublic.com/article/fraud-guides-a-hot-commodity-on-the-dark-web/?ftag=TREa988f1c&bhid=42420269&mid=12798383&cid=2176068089

Such guides provide instructions so that even novices can learn how to become cybercriminals, says web intelligence company Terbium Labs.

The dark web is home to a large hive of shady online marketplaces where people can buy and sell all kinds of products and information. Beyond trading in physical items such as drugs and guns, these marketplaces offer stolen user credentials, credit card data, and hacking tools and templates. But one type of item in great demand are fraud guides.

Click link above to read more

Zoom: A cheat sheet about the video conferencing solution

https://www.techrepublic.com/article/zoom-a-cheat-sheet-about-the-video-conferencing-solution/?ftag=TREa988f1c&bhid=42420269&mid=12798383&cid=2176068089

Zoom is now a household name for work-from-home employees. Here is your guide to Zoom basics, including its security vulnerabilities and video conferencing alternatives such as Microsoft Teams.

Due to the COVID-19 pandemic, more people are working from home. With workforces scattered to the wind, many businesses have had to adapt to virtual meetings as the new normal, which has been a massive boon for the video chat and conferencing software Zoom.

Click link above to read more

Russian state hackers behind San Francisco airport hack

https://www.zdnet.com/article/russian-state-hackers-behind-san-francisco-airport-hack/

Hackers believed to be operating on behalf of the Russian government have hacked two websites operated by the San Francisco International Airport, cyber-security firm ESET said today.

The hacks took place last month, in March, according to a data breach notification [PDF] posted on the airport's website.

The attacks targeted SFOConnect.com, a website used by airport employees, and SFOConstruction.com, a portal used by airport construction contractors.

Click link above to read more

Suspected cyber attack closes MSC's data centre

https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-attack-closes-msc-headquarters-servers-58933

Mediterranean Shipping Co (MSC) is battling to resume operations from its headquarters after what appears to be a cyber attack on its Swiss data centre.

MSC said it closed down servers at its Geneva, Switzerland, head-office and was tackling outages that brought down its website and myMSC portal.

These outages have halted operation of self-service tools for making and managing bookings on MSC ships. This comes as self-servicing and online trading has increased as more companies are working remotely during the coronavirus Covid-19 pandemic.

Click link above to read more

Energy giant EDP hit with RagnarLocker ransomware

https://www.techradar.com/news/energy-giant-edp-hit-with-ragnarlocker-ransomware

Attackers demand a $10.9m ransom or they'll leak the company's sensitive files.

The Portugese multinational energy giant Energias de Portugal (EDP) is the latest company to fall victim to the RagnarLocker ransomware and the attackers are now asking for a $10.9m ransom to unlock its files.

According to BleepingComputer and MalwareHunterTeam, the attackers claim to have stolen over 10TB of sensitive company files which they are threatening to leak if their ransom demands are not met.

Click link above to read more

Four Million Quidd User Credentials Found on the Dark Web

https://www.infosecurity-magazine.com/news/four-million-quidd-user

Security researchers have discovered almost four million credentials linked to digital collectibles site Quidd, including a sizeable number of corporate email addresses.

Risk Based Security's Data Breach Research Team announced the discovery on Friday, revealing the data was available "on a prominent deep web hacking forum."

It apparently features the email addresses, usernames and bcrypt hashed passwords of 3,954,416 users.

Click link above to read more

****

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