Security News Digest
Information Security Branch
British Columbia OCIO Office of the Chief Information Officer

August 10th, 2020

Try our August - 'Summer social media' Quiz

This week's stories:

- **Understanding Canadian Cybersecurity Laws: "Insert Something Clever Here" — Canada's Anti-Spam Legislation (Article 5)**
- **'Remote access is here to stay,' healthcare webinar told**
- **Bugs in HDL Automation expose IoT devices to remote hijacking**
- **FBI: Iranian hackers trying to exploit critical F5 BIG-IP flaw**
- **Gamifying Password Training Shows Security Benefits**
- **Digital Clones Could Cause Problems for Identity Systems**
- **#DEFCON: How the International Space Station Enables Cybersecurity**
- **Attackers Horn in on MFA Bypass Options for Account Takeovers**
- **Assuring VPN Availability & Performance in a Pandemic World**
- **#DEFCON: Bypassing Biometric Scanners with 3D Printed Fingerprints**

Understanding Canadian Cybersecurity Laws: "Insert Something Clever Here" — Canada's Anti-Spam Legislation (Article 5)

https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-insert-something-clever-here-canadas-anti-spam-legislation-article-5/434004

As we continue to adapt to the changing demands to navigate the spread of COVID-19, an increasing number of workspaces and social interactions have had to rely much more heavily on email and other online forms of electronic forms communication. Our increased reliance on electronic messages, particularly in the context of doing business, exposes individuals and organizations to the increased risk of receiving unsolicited commercial electronic messages, which we call "spam". Only a mere six years ago, Canada was home to seven of the world's top 100 spamming organizations. This changed in 2014, with the implementation of Canada's Anti-Spam Legislation.

Click link above to read more

'Remote access is here to stay,' healthcare webinar told

https://www.itworldcanada.com/article/remote-access-is-here-to-stay-healthcare-webinar-told/434359

Many clinical and administrative staff will be treating patients and accessing data remotely after the COVID-19 crisis settles, experts said during a Canadian webinar on the effects of the pandemic on the healthcare sector.

“Remote access is here to stay. In a big way,” said Kashif Pervaiz, CISO of Toronto’s University Health Network (UHN), a group of three hospitals, rehabilitation centres and a clinician training school.

Click link above to read more

Bugs in HDL Automation expose IoT devices to remote hijacking

https://www.bleepingcomputer.com/news/security/bugs-in-hdl-automation-expose-iot-devices-to-remote-hijacking/

A security researcher discovered vulnerabilities in an automation system for smart homes and buildings that allowed taking over accounts belonging to other users and control associated devices.

In a presentation on Saturday at the IoT Village during the DEF CON hacker conference, Barak Sternberg shows how some weak spots in the HDL automation system could have been leveraged by attackers to fully compromise it.

Click link above to read more

FBI: Iranian hackers trying to exploit critical F5 BIG-IP flaw

https://www.bleepingcomputer.com/news/security/fbi-iranian-hackers-trying-to-exploit-critical-f5-big-ip-flaw/

The FBI warns of Iranian hackers actively attempting to exploit an unauthenticated remote code execution flaw affecting F5 Big-IP application delivery controller (ADC) devices used by Fortune 500 firms, government agencies, and banks.

Click link above to read more

Gamifying Password Training Shows Security Benefits

https://www.darkreading.com/operations/identity-and-access-management/gamifying-password-training-shows-security-benefits/d/d-id/1338628

Passwords continue to be problematic for many companies because users tend to pick predictable combinations of letters, numbers, and symbols. Using a game for training can reinforce the rules for picking stronger passwords, a group of researchers from the India-based Tata Consulting Services stated in a presentation at the USENIX Symposium on Usable Privacy and Security on August 10 and in a report.

Click link above to read more

Digital Clones Could Cause Problems for Identity Systems

https://www.darkreading.com/endpoint/digital-clones-could-cause-problems-for-identity-systems/d/d-id/1338615

The fundamental technologies for creating digital clones of people — text, audio, and video that sound and look like a specific person — have rapidly advanced and are within striking distance of a future in which digital avatars can sound and act like specific people, Tamaghna Basu, co-founder and chief

technology officer of neoEYED, a behavioral analytics firm, told attendees at the virtual Black Hat conference on Aug. 6.

Click link above to read more

#DEFCON: How the International Space Station Enables Cybersecurity

https://www.infosecurity-magazine.com/news/international-space-station/

Like any other IT environment, there are potential cyber-risks to the International Space Station (ISS), though the station is quite literally like no environment on Earth.

In a session on August 9 at the Aerospace Village within the DEFCON virtual security conference, former NASA astronaut Pamela Melroy outlined the cybersecurity lessons learned from human spaceflight and what still remains a risk. Melroy flew on two space shuttle missions during her tenure at NASA and visited ISS. Hurtling high above the Earth, ISS is loaded full of computing systems designed to control the station, conduct experiments and communicate with the ground.

Click link above to read more

Attackers Horn in on MFA Bypass Options for Account Takeovers

https://threatpost.com/attackers-mfa-bypass-account-takeovers/158189/

An uptick in business email compromise attacks is being attributed to successful compromises of multi-factor authentication (MFA) and conditional access controls, according to researchers. While brute-forcing and password spraying techniques are the most common way to mount account takeovers, more methodical cybercriminals are able to gain access to accounts even with more secure MFA protocols in place.

Click link above to read more

Assuring VPN Availability & Performance in a Pandemic World

https://www.darkreading.com/attacks-breaches/assuring-vpn-availability-and-performance-in-a-pandemic-world/d/d-id/1338479

The current pandemic has spurred a revolutionary shift to remote work environments and triggered a huge increase in Internet traffic. According to OpenVault's Q12020 Broadband Insights Report, average bandwidth consumption has jumped 47% since the same time last year, much of that traffic being outbound, signifying VPN usage.

Click link above to read more

#DEFCON: Bypassing Biometric Scanners with 3D Printed Fingerprints

https://www.infosecurity-magazine.com/news/defcon-bypassing-biometric-scanners/

Biometric authentication, including facial recognition and fingerprint scanners, is increasingly common, but that doesn't mean they are safe from hackers.

At the DEFCON virtual security conference on August 8, security researcher Yamila Levalle from Dreamlab Technologies outlined how she was able to bypass biometric authentication for a number of different types of fingerprint scanners. During her session, Levalle explained various methods of bypass including using a budget 3D printer, which yielded positive results.

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:

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