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

November 24th, 2020

Try our November - ‘Phishing’ Quiz

This week’s stories:

- 🇨🇦 Investigation finds ‘unauthorized access’ to B.C. legislature servers
- 🇨🇦 Canadian Centre for Cyber Security Releases the Canadian National Cyber Threat Assessment 2020
- 🇨🇦 Understanding Canadian cybersecurity laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)
- 🇨🇦 Cybersecurity agency calls out four countries as the 'greatest strategic threats' to Canada
- 🇨🇦 His bank raided his account to cover a payment made to scammers
- House approves bill to secure internet-connected federal devices against cyber threats
- When Growth Hackers Take It Too Far: The Fake Hair Story
- More Ransomware-as-a-Service Operations Seek Affiliates
- Microsoft warns Office 365 users of consent phishing dangers
- Cisco Webex ‘Ghost’ Flaw Opens Meetings to Snooping
- Why biometrics will not fix all your authentication woes
- Facebook Messenger Flaw Enabled Spying on Android Callee
- GoDaddy Employees Used in Attacks on Multiple Cryptocurrency Services

---

🇨🇦 Investigation finds ‘unauthorized access’ to B.C. legislature servers

https://globalnews.ca/news/7473203/bc-legislature-server-hack/

The British Columbia legislature confirms that someone recently gained “unauthorized access” to some of its servers.

In a statement posted Thursday, the legislature said there was “no evidence of unathorized access to or loss of legislative assembly or personal data.”

Click link above to read more

🇨🇦 Canadian Centre for Cyber Security Releases the Canadian National Cyber Threat Assessment 2020

https://www.canada.ca/en/communications-security/news/2020/11/canadian-centre-for-cyber-security-releases-the-canadian-national-cyber-threat-assessment-2020.html

Ottawa, Ontario, November 18 2020 – The Canadian Centre for Cyber Security (Cyber Centre) has released its National Cyber Threat Assessment 2020.

This public report, based on both classified and unclassified sources, identifies current trends in the cyber threat environment, the likelihood that these cyber threats will occur, and how Canadians could be affected.

Click link above to read more

🇨🇦 Understanding Canadian cybersecurity laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)

https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-deep-dark-and-undetectable-canadian-jurisdictional-considerations-in-global-encrypted-networks-article-7/438587

The rapid growth of encryption technology has revolutionized the online marketplace and helped to enable the creation of anonymous online networks, like the Dark Net — a hidden forum for which has attracted individuals who wish to engage in criminal activities while remaining anonymous and untraceable. Cybercriminal activity, unlike typical localized or neighbourhood crimes, is not confined by national or provincial borders or limited by physical geography. The fairly recent creation and development of cryptocurrencies, through the Dark Net, has created the possibility of full transactional anonymity for those involved in criminal activities both on- and offline. For the most part, crime hidden on the Dark Web (accessed via the Dark Net) or committing using the Dark Net is not a novel crime; it is an established crime the commission of which is being facilitated through the use of anonymous encrypted networks.

Click link above to read more

🇨🇦 Cybersecurity agency calls out four countries as the 'greatest strategic threats' to Canada

https://www.ctvnews.ca/politics/cybersecurity-agency-calls-out-four-countries-as-the-greatest-strategic-threats-to-canada-1.5194491

OTTAWA -- Canada’s top cybersecurity agency has named China, Russia, Iran, and North Korea’s state-sponsored cyber activity as posing the “greatest strategic threats” to Canada’s critical infrastructure, intellectual property, and political events like elections.

In its 2020 National Cyber Threat Assessment, the Canadian Centre for Cyber Security within the Communications Security Establishment warns that state-sponsored cyber activity is the most sophisticated and actors are “very likely” attempting to develop capabilities to disrupt critical systems; will “almost certainly” continue conducting commercial espionage against Canadian governments, businesses, and organizations; and are keeping up ongoing online foreign influence campaigns aimed at altering discourse around current events to divide Canadians.

.

Click link above to read more

🇨🇦 His bank raided his account to cover a payment made to scammers

https://www.cbc.ca/news/canada/tangerine-account-raided-job-scam-1.5806275

Justin Smith has been hit with a one-two punch of bad luck.

First, the Toronto man was duped by a job scam that made off with $3,000. Then his longtime bank, Tangerine, helped itself to money Smith had in his tax-free savings account to recoup what it had lost in the scam.

"You keep your money in the bank because you think it's safe," he said. "And they treat the money like it's theirs, and they just move it around to protect themselves. That's not fair."

Click link above to read more

House approves bill to secure internet-connected federal devices against cyber threats

https://thehill.com/policy/cybersecurity/516373-house-approves-bill-to-secure-internet-connected-federal-devices-against

The House on Monday passed legislation to improve the security of federal internet-connected devices, with the bill garnering bipartisan support.

The Internet of Things (IoT) Cybersecurity Improvement Act, passed unanimously by the House, would require all internet-connected devices purchased by the federal government — including computers, mobile devices and other products with the ability to connect to the internet — to comply with minimum security recommendations issued by the National Institute of Standards and Technology.

.

Click link above to read more

When Growth Hackers Take It Too Far: The Fake Hair Story

https://wersm.com/when-growth-hackers-take-it-too-far-the-fake-hair-story/

Clickbaiting is so 2017. The new fast-growth platforms are visual now. Take Instagram Stories for example, it is one of the most engaging, fun and interactive channels right now. There are no live links on Instagram, and the same applies to Stories. Except if you swipe up that is. And that’s not even a “natural” experience for users: we are used to click or tap – not swipe up.

Therefore, marketers have been keen to try all sorts of design tactics to make us swipe up more – from simple text instructions to “swipe up,” all the way to more elaborate visual callouts, often built out of emojis. And that is fine, right?

Click link above to read more

More Ransomware-as-a-Service Operations Seek Affiliates

https://www.bankinfosecurity.com/more-ransomware-as-a-service-operations-seek-affiliates-a-15378

Ransomware developers continue to put highly automated attack toolkits into the hands of criminals, allowing even individuals without advanced technical skills to amass victims.

"The prospect of large profits drives a lot of criminals towards ransomware," says John Fokker, head of cyber investigations and red teaming for McAfee Advanced Threat Research. "Everyone wants a piece of the pie."

Click link above to read more

Microsoft warns Office 365 users of consent phishing dangers

https://www.techradar.com/in/news/microsoft-warns-users-of-the-dangers-of-consent-phishing

Microsoft is warning users that the shift to remote working during the pandemic has exposed organizations to additional security threats including consent phishing.

Unlike traditional phishing attacks where cybercriminals try to steal user credentials, consent phishing is a technique where attackers trick users into granting a malicious app access to sensitive data or other resources.

Once an attacker has compromised a victim's Office 365 account, they can then obtain access to their mail, files, contacts, notes, profiles and other sensitive information and resources stored in their organization's SharePoint or OneDrive accounts.

Click link above to read more

Cisco Webex 'Ghost' Flaw Opens Meetings to Snooping

https://threatpost.com/cisco-webex-flaw-snooping/161355/

A vulnerability in Cisco's Webex conferencing application could allow an attendee to act as a "ghost" in the meeting – allowing them to spy in on potentially sensitive company secrets.

To exploit the flaw (CVE-2020-3419), attackers can be remote – however, they would need access to join the Webex meetings, including applicable meeting "join" links and passwords. For this reason, the flaw is only considered medium severity by Cisco, ranking 6.5 out of 10 on the CVSS scale. However, the practical implications are significant when considering information a "ghost" could obtain in a meeting that assumed he or she was absent from.

Click link above to read more

Why biometrics will not fix all your authentication woes

https://www.helpnetsecurity.com/2020/11/17/biometric-authentication/

As the number of data breaches shows no signs of decreasing, the clamor to replace passwords with biometric authentication continues to grow. Biometrics are becoming widely incorporated to secure organizations from unauthorized access and the growing appeal of these security solutions is expected to create a market worth $41.8 billion by 2023, according to MarketsandMarkets.

Click link above to read more

Facebook Messenger Flaw Enabled Spying on Android Callees

https://www.darkreading.com/threat-intelligence/facebook-messenger-flaw-enabled-spying-on-android-callees/d/d-id/1339509

Facebook has patched a critical vulnerability in the Facebook Messenger for Android mobile app, which could have let attackers spy on other Facebook users using audio and video calls.

Natalie Silvanovich, the researcher with Google's Project Zero who discovered the bug, says it existed in Facebook Messenger's implementation of a protocol called WebRTC, which the app uses to set up audio and video calls by exchanging "thrift messages" between callee and caller.

Click link above to read more

GoDaddy Employees Used in Attacks on Multiple Cryptocurrency Services

https://krebsonsecurity.com/2020/11/godaddy-employees-used-in-attacks-on-multiple-cryptocurrency-services/

Fraudsters redirected email and web traffic destined for several cryptocurrency trading platforms over the past week. The attacks were facilitated by scams targeting employees at **GoDaddy**, the world’s largest domain name registrar, KrebsOnSecurity has learned.

The incident is the latest incursion at GoDaddy that relied on tricking employees into transferring ownership and/or control over targeted domains to fraudsters. In March, a voice phishing scam targeting GoDaddy support employees allowed attackers to assume control over at least a half-dozen domain names, including transaction brokering site escrow.com.

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