Security News Digest
Information Security Branch

OCIO | Office of the Chief Information Officer

July 21st, 2020

Try our July - 'Back to Basics' Quiz

This week's stories:

- Changing world of work: Citrix survey shows how Canadians imagine (home) office routine of tomorrow
- UK, US, Canada accuse Russia of hacking virus vaccine trials
- Cyber attacks have increased in past 12 months for 99 per cent of Canadian organizations: survey
- Who's Behind Wednesday's Epic Twitter Hack?
- How Nanotechnology Will Disrupt Cybersecurity
- Phishing attacks hiding in Google Cloud to steal Microsoft account credentials
- Facebook's NSO Group Lawsuit Over WhatsApp Spying Set to Proceed
- Paving the Path to Passwordless
- A New Flaw In Zoom Could Have Let Fraudsters Mimic Organisations
- Iranian Spies Accidentally Leaked Videos of Themselves Hacking

---

Changing world of work: Citrix survey shows how Canadians imagine (home) office routine of tomorrow

https://www.canadiansecuritymag.com/changing-world-of-work-citrix-survey-shows-how-canadians-imagine-home-office-routine-of-tomorrow/

Lockdown restrictions in Canada have begun to lift and companies are beginning to strategize on how they will create a secure return to work process. However, before companies can fully reopen their doors, there are some things they will need to amend or even rethink completely.

From the work models being offered, technology being used, or the overall company culture — the workplace will need to change, according to employee expectations.

Click link above to read more

UK, US, Canada accuse Russia of hacking virus vaccine trials

https://www.canadiansecuritymag.com/uk-us-canada-accuse-russia-of-hacking-virus-vaccine-trials/

LONDON — Britain, the United States and Canada accused Russia on Thursday of trying to steal information from researchers seeking a COVID-19 vaccine.

The three nations alleged that hacking group APT29, also known as Cozy Bear and said to be part of the Russian intelligence service, is attacking academic and pharmaceutical research institutions involved in coronavirus vaccine development.

Click link above to read more

Cyber attacks have increased in past 12 months for 99 per cent of Canadian organizations: survey

https://www.canadiansecuritymag.com/99-per-cent-of-canadian-organizations-said-cyber-attacks-have-increased-in-past-12-months-survey/

Twitter was thrown into chaos on Wednesday after accounts for some of the world's most recognizable public figures, executives and celebrities starting tweeting out links to bitcoin scams. Twitter says the attack happened because someone tricked or coerced an employee into providing access to internal Twitter administrative tools. This post is an attempt to lay out some of the timeline of the attack, and point to clues about who may have been behind it.

Click link above to read more

Who's Behind Wednesday's Epic Twitter Hack?

https://krebsonsecurity.com/2020/07/whos-behind-wednesdays-epic-twitter-hack/

The UK government has announced a series of measures to remove the Chinese phone-maker Huawei from the UK's 5G mobile networks.

It will ban UK mobile providers from buying new Huawei 5G equipment after the end of this year and they will have to remove all of its 5G kit from their networks by 2027.

The government had previously said Huawei could be involved in the project but it changed its mind following growing security concerns about China.

Click link above to read more

How Nanotechnology Will Disrupt Cybersecurity

https://www.darkreading.com/threat-intelligence/how-nanotechnology-will-disrupt-cybersecurity-/a/d-id/1338285

Tangible solutions related to cryptography, intelligent threat detection and consumer security are closer than you think.

It sometimes feels like nanotechnology is a solution looking for a problem. Though there has been much speculation about the potential applications of nanotechnology, many benefits the technology remain quite underdeveloped. One exception is in the area of cybersecurity.

Click link above to read more

Phishing attacks hiding in Google Cloud to steal Microsoft account credentials

https://www.techrepublic.com/article/phishing-attacks-hiding-in-google-cloud-to-steal-microsoft-account-credentials/

Phishing campaigns often attempt to evade detection not only by impersonating well-known companies and brands but by storing their malicious content on a legitimate website. The idea is that such phishing pages will better elude detection by security products and more easily ensnare unsuspecting victims. A recent phishing attack analyzed by cyber threat intelligence provider Check Point Research is using Google Cloud services to conceal its malicious intent.

Click link above to read more

Facebook's NSO Group Lawsuit Over WhatsApp Spying Set to Proceed

https://threatpost.com/facebooks-nso-group-lawsuit-whatsapp-spying/157571/

Facebook's lawsuit against NSO Group over alleged spying on WhatsApp users will be allowed to go forward.

WhatsApp-owner Facebook is alleging that NSO Group exploited a vulnerability in WhatsApp to deploy its spyware against human rights activists, journalists and political dissidents.

Click link above to read more

Paving the Path to Passwordless

https://threatpost.com/duo-paving-the-path-to-passwordless/157502/

Passwords seem to be the digital equivalent of the phrase, "can't live with 'em, can't live without 'em." They're supposed to protect sensitive information and data, but passwords can also be incredibly frustrating; you shouldn't use the same one across the board, which means you probably have variations of the same one, which means you have to remember which one is for which site, and then when you have to reset your password because inevitably you can't remember it, you get an error that says your new password can't be the same as your old password. Phew! (Oh, and don't forget that your password also has to be complex enough that it's hard to guess. So, add that to the list.)

Click link above to read more

A New Flaw In Zoom Could Have Let Fraudsters Mimic Organisations

https://thehackernews.com/2020/07/zoom-vanity-url-vulnerability.html

In a report shared with The Hacker News, researchers at cybersecurity firm CheckPoint today disclosed details of a minor but easy-to-exploit flaw they reported in Zoom, the highly popular and widely used video conferencing software.

The latest Zoom flaw could have allowed attackers mimic an organization, tricking its employees or business partners into revealing personal or other confidential information using social engineering tricks.

Click link above to read more

Iranian Spies Accidentally Leaked Videos of Themselves Hacking

https://www.wired.com/story/iran-apt35-hacking-video/

WHEN SECURITY RESEARCHERS piece together the blow-by-blow of a state-sponsored hacking operation, they're usually following a thin trail of malicious code samples, network logs, and connections to faraway servers. That detective work gets significantly easier when hackers record what they're doing and upload the video to an unprotected server on the open internet. Which is precisely what a group of

Iranian hackers may have unwittingly done.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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