July 23rd, 2019

Try our July quiz – Summer Phishing

This week's stories:

- **AI adoption in Canada could benefit from a greater focus on STEM education, experts say** 🇨🇦

- **Michael Weiss Receives Funding to Create an Open Source Cyber Fusion Centre** 🇨🇦

- **The status of Canadian women in cyber security called 'sad'** 🇨🇦

- **Average cost of a data breach is US$3.9 million, says study**

- **'Wizard' hacker charged after financial records of nearly every Bulgarian exposed**

- **Firms have to get back to cybersecurity basics, government expert tells Parliament**

- **Bulk of cyber budget should go to awareness training, not technology, says expert**

- **Real-Time Location of Millions Exposed by Mobile Loan Apps**

- **Criminals are using deepfakes to impersonate CEOs**

- **BEC Scams Average $301 Million Per Month In Illegal Transfers**

- **New 'US State Police' Extortion Scam Includes Contact Numbers**

- **Twitter Can be Tricked Into Showing Misleading Embedded Links**

- **FaceApp Makes Today's Privacy Laws Look Antiquated**

AI adoption in Canada could benefit from a greater focus on STEM education, experts say 🇨🇦

https://www.itworldcanada.com/article/ai-adoption-in-health-care-could-benefit-from-a-greater-focus-on-stem-education-experts-say/420108

Despite Canada's status as a leader in education, the country's stagnant academic scores among young people is a bad sign for future generations hoping to integrate complex technologies, such as artificial intelligence, across society, according to Phil Vokins, Intel Canada interim general manager.

Click link above to read more

Michael Weiss Receives Funding to Create an Open Source Cyber Fusion Centre 🇨🇦

https://www.itworldcanada.com/article/average-cost-of-a-data-breach-is-us3-9-million-says-study/420197

Carleton University's Michael Weiss, an associate professor in the Department of Systems and Computer Engineering, received a $560,000 grant from the Ontario Centres of Excellence (OCE), PROMPT and the Natural Sciences and Engineering Research Council of Canada (NSERC) to fund an Open Source Cyber Fusion Centre as part of the Cybersecurity R&D Challenge. The award will be shared with co-principal investigator, Mourad Debbabi, at Concordia University.

Click link above to read more

The status of Canadian women in cyber security called 'sad' 🇨🇦

https://www.itworldcanada.com/article/the-status-of-canadian-women-in-cyber-security-called-sad/420096

BRAMPTON, Ont. — Let us travel in a time machine to the dark, sexist past of Canada. Way back, about nine months ago, to the year 2018.

Lisa Kearney had recently been appointed director of product security at a British Columbia firm, which meant she oversaw design and product rollout. In addition, she was hired to design the company's cyber security framework.

Click link above to read more

Average cost of a data breach is US$3.9 million, says study

https://www.itworldcanada.com/article/average-cost-of-a-data-breach-is-us3-9-million-says-study/420197

The most recent data was pulled from interviewing officials at 507 organizations in 16 countries and regions and across 17 industry sectors that suffered breaches between July 2018 and April 2019.

For the first time this year, the report also examined the longtail financial impact of a data breach, finding that the effects of a data breach are felt for years. While an average of 67 per cent of data breach costs were seen in the first year after a breach, 22 per cent accrued in the second year, and another 11 per cent accumulated more than two years after a breach.

Click link above to read more

'Wizard' hacker charged after financial records of nearly every Bulgarian exposed

https://www.theguardian.com/world/2019/jul/18/wizard-hacker-charged-after-financial-records-of-nearly-every-bulgarian-exposed

A 20-year-old cybersecurity worker has been arrested in Bulgaria and charged with hacking the personal and financial records of millions of taxpayers, as police continue to investigate the country's biggest ever data breach.

Bulgaria's NRA tax agency is facing a fine of up to €20m ($22.43m) over the hack, which was revealed this week and is thought to have compromised the records of nearly every working adult among the country's population of 7 million – about 5 million people.

Click link above to read more

Firms have to get back to cybersecurity basics, government expert tells Parliament

https://www.itworldcanada.com/article/firms-have-to-get-back-to-cyber-security-basics-government-expert-tells-parliament/419986

Investing in the basics of cybersecurity is the best way Canadian organizations can lower the risk of data breaches, a parliamentary committee looking into the recent huge data theft at Desjardins Group of credit unions.

"Ultimately, there is no silver bullet when it comes to cybersecurity," Andre Boucher, deputy minister and director of operations at the Canadian Centre for Cyber Security told members of the House of Commons public safety committee on Monday. "We cannot be complacent."

Click link above to read more

Bulk of cyber budget should go to awareness training, not technology, says expert

https://www.itworldcanada.com/article/bulk-of-cyber-budget-should-go-to-awareness-training-not-technology-says-expert/420064

BRAMPTON, Ont. — As a penetration tester Joshua Crumbaugh has a number of weapons, the biggest of which are his research skills and his determination.

He's talked his way into getting a U.S. bank to install 'malware' and ultimately into getting into the vault and convinced the IT support department of an international law firm into giving him an administration password — both over the phone.

Click link above to read more

Real-Time Location of Millions Exposed by Mobile Loan Apps

https://www.bleepingcomputer.com/news/security/real-time-location-of-millions-exposed-by-mobile-loan-apps/

Financial data, personally identifiable information (PII), and real-time location of millions of Chinese users was leaked by an open Elastic cluster hosted on infrastructure owned by Aliyun Computing Co (also known as Alibaba Cloud).

The highly sensitive information was added to the publicly-accessible database by over 100 mobile loan-related apps used by Chinese people when applying for loans.

Click link above to read more

Criminals are using deepfakes to impersonate CEOs

https://www.fastcompany.com/90379001/criminals-are-using-deepfakes-to-impersonate-ceos

"Deepfakes" refers to media that has been altered by artificial intelligence to make it appear that a person is doing or saying something that, in fact, that person has never done or said. The technology first began appearing a few years ago, with crude deepfake tools allowing users to make it look like celebrities were recorded engaging in sexual activities they actually didn't take part in.

Click link above to read more

BEC Scams Average $301 Million Per Month In Illegal Transfers

https://www.bleepingcomputer.com/news/security/bec-scams-average-301-million-per-month-in-illegal-transfers/

The frequency of business email compromise (BEC) scams has increased year over year and so did the value of attempted thefts, reaching a monthly average of more than $300 million.

The number is drawn from the suspicious activity reports (SARs) received every month since 2016, which increased from 500 to more than 1,100 in 2018.

The Financial Crimes Enforcement Network (FinCEN) compiled statistics about BEC incidents occurring over the past two years and identified the most common types of targets along with the destination intended for the stolen funds and the techniques used by the scammers.

New 'US State Police' Extortion Scam Includes Contact Numbers

https://www.bleepingcomputer.com/news/security/new-us-state-police-extortion-scam-includes-contact-numbers/

A new extortion scam is underway that pretends to be from a US State Police detective who is willing to delete child porn evidence if you send them $2,000 in bitcoins. Pretending to be from a state police detective is a new twist, but what really stands out is that they also include a contact phone number that can be used to call the scammer.

We all know, or should know, about the sextortion emails people are receiving where the sender states they have hacked the recipient's computer and taped them doing things while on adult sites. Since then, we have seen further extortion scams that pretend to be the CIA, bomb threats, threats to ruin a website's reputation, and even from hitmen asking you to pay them to call off a hit.

Twitter Can be Tricked Into Showing Misleading Embedded Links

https://www.bleepingcomputer.com/news/security/twitter-can-be-tricked-into-showing-misleading-embedded-links/

A long standing Twitter issue allows bad actors to manipulate tweets so that they appear to contain content from one site, but actually link to a completely different one. This enables creating tweets that look like legitimate articles from well-respected sites, but actually link to pages serving phishing, malware, or scams.

FaceApp Makes Today's Privacy Laws Look Antiquated

https://www.theatlantic.com/ideas/archive/2019/07/faceapp-reveals-huge-holes-todays-privacy-laws/594358/?mkt_tok=eyJpIjoiWTJWaU9ETTRaakZsTnpZMyIsInQiOiJcLzBCVVUyaW1XVGs0bDFFYk5GM2t3UU9wNXZ5RVg0VG1iN2c5MmN5M1ZtSmU1dVVBaFB0UHJBRzlJM2lkQWJWUlBnUFk0cytIWEFwVGY4WWWxtQ0U3WHl4M3pUc2FxWERxeE5oNzNNBcGt2V2tJc0NHeDdRdHgzakpqc1A0aGUifQ%3D%3D

Americans give billions of dollars a year to industries that promise to make them look younger. FaceApp became wildly popular, seemingly overnight, for doing the exact opposite.

Applying a filter powered by artificial intelligence, the photo-editing app modifies photos of its users' faces to show them what they might look like when they're much older. The resulting images aren't the only thing about FaceApp that strikes some people as creepy.

FaceApp is the handiwork of a relatively unknown company in Russia—a provenance that, amid evidence of election interference and other misdeeds by Russian hackers, has raised widespread concerns in Washington. The Democratic National Committee and Senate Minority Leader Chuck Schumer are now calling out the app as a privacy threat.

Click Unsubscribe to stop receiving the Digest.

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:

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