July 9th, 2019

Try our July quiz – Summer Phishing

This week's stories:

- University of Ottawa student news site nearly wiped off Internet
- Cyber Security main obstacle for Canadian companies: study
- 'No magic fix' to ease Desjardins privacy breach concerns, Liberal MP says
- New Zealand gov't pledges $5m to implement better cybersecurity
- 7-Eleven Japanese customers lose $500,000 due to mobile app flaw
- VMware, Cisco Systems issue security warnings
- UK regulator proposes fining British Airways a record $300 million CAD over data breach
- Facebook isn't listening to you, but through tracking what you do, it can serve up ads like it is
- Georgia courts (mostly) shrug off ransomware attack
- Researchers crack open Facebook campaign that pushed malware for years
- FBI Releases Warning on Sextortion Scams Targeting Teenagers
- Over $800,000 Stolen by Scammers in Atlanta Area City BEC Fraud

---

University of Ottawa student news site nearly wiped off Internet

https://www.itworldcanada.com/article/university-of-ottawa-student-news-site-nearly-wiped-off-internet/419605

A week-old backup has saved the University of Ottawa's online student news site The Fulcrum from being wiped off the internet after an attacker deleted years of content over the weekend.

On Saturday a staffer discovered the site was void of news stories except for a stock photo of a person lifting his middle finger with the headline: "Anti-union rag gets its entire website DELETED."

Click link above to read more

Cyber Security main obstacle for Canadian companies: study

https://montreal.ctvnews.ca/cyber-security-main-obstacle-for-canadian-companies-study-1.4500015

At a time when the issue of privacy is at the heart of the news, a new study suggests that cybersecurity is the main obstacle to the online growth of many companies.

This is reflected in a study released Tuesday by the Business Development Bank of Canada (BDC) on the benefits of the online presence on the growth of companies outside their market.

Click link above to read more

'No magic fix' to ease Desjardins privacy breach concerns, Liberal MP says

https://www.cbc.ca/news/politics/security-meeting-desjardins-1.5205025

The chair of the House of Commons public safety and national security committee says it will hold an emergency meeting to discuss the massive personal data breach at the Desjardins Group, but concedes there's "no magic fix."

Last month, the Quebec-based bank revealed that an employee with "ill-intention" collected information about almost three million people and businesses and shared it with others. Desjardins flagged a suspicious transaction to Laval police in December, but officials said it took several months for them to understand the scope of the scheme.

Click link above to read more

New Zealand gov't pledges $5m to implement better cybersecurity

https://portswigger.net/daily-swig/new-zealand-govt-pledges-5m-to-implement-better-cybersecurity

New Zealand's government has pledged a further NZ$8 million ($5.3m) to implement a revised cybersecurity strategy released yesterday.

The Cyber Security Strategy 2019 (PDF) will "enable New Zealand to thrive online" by working with public and private sector companies to implement a cybersecurity culture and response to threats.

It follows two previous strategies, launched in 2011 and 2015, which were both criticized for not going far enough.

The government responded to this by also increasing support for CERT NZ, allocating NZ$9.3 million ($6.2m) in funding for the national response center.

Click link above to read more

7-Eleven Japanese customers lose $500,000 due to mobile app flaw

https://www.zdnet.com/article/7-eleven-japanese-customers-lose-500000-due-to-mobile-app-flaw/

Approximately 900 customers of 7-Eleven Japan have lost a collective of ¥55 million ($510,000) after hackers hijacked their 7pay app accounts and made illegal charges in their names.

The incident was caused by an appalling security lapse in the design of the company's 7pay mobile payment app, which 7-Eleven Japan launched in the country on Monday, July 1.

Click link above to read more

VMware, Cisco Systems issue security warnings

https://www.itworldcanada.com/article/vmware-cisco-systems-issue-security-warnings/419635

IT administrators have been warned by two of the biggest suppliers of enterprise products of security vulnerabilities.

–VMware issued an “important” alert this week for updates after finding 30 of its products are vulnerable to the recently discovered Linux kernel TCP Selective Acknowledgement (SACK) vulnerabilities. Those bugs could lead to a distributed denial of service attack against those products, the company said.

Click link above to read more

UK regulator proposes fining British Airways a record $300 million CAD over data breach

https://www.itworldcanada.com/article/uk-regulator-proposes-fining-british-airways-a-record-cdn300-million-over-data-breach/419721

Anyone who doubted European Union regulators wouldn’t take the opportunity to whack companies for data breaches under the new General Data Protection Regulation (GDPR) has been shaken awake with news that the U.K.’s information commissioner has proposed fining British Airways the equivalent of $300 million CAD for a 2018 incident.

Click link above to read more

Facebook isn’t listening to you, but through tracking what you do, it can serve up ads like it is

https://www.thestar.com/business/technology/2019/06/27/facebook-isnt-listening-to-you-but-through-tracking-what-you-do-it-can-serve-up-ads-like-it-is.html

My editor, Michelle, was at a birthday party for her son’s friend recently, when the mom mentioned a company she liked called Joymode. Minutes later, an ad for Joymode appeared on Michelle’s Facebook newsfeed.

When she told me about it, we both wondered whether the urban legend could be true. Does Facebook really listen to our conversations to serve us ads?

Click link above to read more

Georgia courts (mostly) shrug off ransomware attack

https://arstechnica.com/information-technology/2019/07/georgia-courts-systems-recovering-from-apparent-ryuk-ransomware/

A spokesman for Georgia's Administrative Office of the Courts has confirmed that the AOC's information technology team discovered ransomware on the organization's servers on Saturday. While the spokesman could not provide specific details about the ransomware involved in the attack, its characteristics are consistent with the Ryuk ransomware that has struck multiple companies and government agencies over the past few months—including at least two Florida cities.

Bruce Shaw, communications and outreach specialist for the AOC, told Ars that a file containing contact information for the ransomware operators was left on the affected servers but that no specific ransom was demanded. "After an assessment of our system, it was determined that it would be best to take our network offline," Shaw said.

Click link above to read more

Researchers crack open Facebook campaign that pushed malware for years

https://arstechnica.com/information-technology/2019/07/five-year-old-facebook-campaign-pushed-malware-on-100000-followers/

Researchers have exposed a network of Facebook accounts that used Libya-themed news and topics to push malware to tens of thousands of people over a five-year span.

Links to the Windows and Android-based malware first came to researchers' attention when the researchers found them included in Facebook postings impersonating Field Marshal Khalifa Haftar, commander of Libya's National Army. The fake account, which was created in early April and had more than 11,000 followers, purported to publish documents showing countries such as Qatar and Turkey conspiring against Libya and photos of a captured pilot that tried to bomb the capital city of Tripoli. Other posts promised to offer mobile applications that Libyan citizens could use to join the country's armed forces.

Click link above to read more

FBI Releases Warning on Sextortion Scams Targeting Teenagers

https://www.bleepingcomputer.com/news/security/fbi-releases-warning-on-sextortion-scams-targeting-teenagers/

The U.S. Federal Bureau of Investigation (FBI) issued a warning on Twitter regarding sextortion campaigns used by scammers to target young people from all over the United States.

"The internet connects you with the world. Do you know who in the world is connecting with you? Sending one explicit image can start a scary cycle," says the FBI in a tweet shared on July 3.

Click link above to read more

Over $800,000 Stolen by Scammers in Atlanta Area City BEC Fraud

https://www.bleepingcomputer.com/news/security/over-800-000-stolen-by-scammers-in-atlanta-area-city-bec-fraud/

Over $800,000 were stolen from the City of Griffin, Georgia, by scammers in a BEC (Business Email Compromise) attack by redirecting two transactions to their own bank accounts according to local media sources.

BEC (also known as Email Account Compromise - EAC) fraud schemes are widespread scams in which crooks deceive employees of privately-held companies and public organizations into wiring money entities they trust but whose bank accounts were changed with ones controlled by the criminals before the attacks.

Click link above to read more

OCIOSecurity@gov.bc.ca