Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

July 24th, 2018

July is "Security while you travel" Month

This week's stories:

- Malicious codes in third-party screens can make you vulnerable to attacks
- Toronto man sues Facebook $500,000 for 'anxiety' related to Cambridge Analytica breach
- New Zealand company violated rights of Canadians, says privacy commissioner
- Email mistakes by U.K. inquiry lead to $345,000 privacy fine
- WhatsApp to cap message forwarding in effort to stop India lynchings
- Rowan Atkinson not 'dead': Viral Mr. Bean hoax is spreading a real virus
- Microsoft exec: We stopped Russia from hacking 3 congressional campaigns
- $1 million heist on Russian bank started with hack of branch router
- The Two Biggest Disruptions To Cybersecurity Since The Invention Of The Firewall
- Vietnam's New Cybersecurity Law and Push for Internet Sovereignty Reduces Freedom
- Egyptian 'Fake News' Law Threatens Citizens with 5000-plus Followers

---

Malicious codes in third-party screens can make you vulnerable to attacks

http://itincanadaonline.ca/index.php/security/2424-malicious-codes-in-third-party-screens-can-make-you-vulnerable-to-attacks

A university in Israel has shown that it's possible to impersonate a user by tracking touch movements on smartphones with compromised third-party touchscreens. Some of these third-party screens have malicious code embedded in them.

Whether you're sending emails, doing a financial transaction or even playing games, the codes are capturing the touches that can be used against you.

The research pointed out that "if an attacker can understand the context of certain events, he can use the information to create a more effective customized attack."

Click link above to read more

Toronto man sues Facebook $500,000 for 'anxiety' related to Cambridge Analytica breach

https://www.itworldcanada.com/article/toronto-man-sues-facebook-500000-for-anxiety-related-to-cambridge-analytica-breach/407270

A Toronto resident is suing Facebook for $500,000 in relation to the Cambridge Analytica privacy breach.

Alfonzo Mattucci has filed a suit against Facebook Inc., Facebook Canada. and Cambridge Analytica, claiming he has experienced hundreds of unwarranted calls and emails since the breach.

In a release from Diamond and Diamond, the law firm retained by Mettucci, he claims to have received two notifications from Facebook in April, notifying him that on a couple occasions his "personal information had been improperly accessed and shared with Cambridge Analytica without his consent or knowledge."

Click link above to read more

New Zealand company violated rights of Canadians, says privacy commissioner

https://www.itworldcanada.com/article/new-zealand-company-violated-rights-of-canadians-says-privacy-commissioner/407292

How far can companies go using personal information of people copied from a publicly-available website? Not far at all if it involves Canadians who don't give their consent, according to a decision released Wednesday by Canada's privacy commissioner.

New Zealand's Profile Technology Ltd. violated the privacy rights of potentially some 4.5 million Canadians by copying the profiles of Facebook users around the globe and posting them on its own website, the office of the federal privacy commissioner has ruled.

Click link above to read more

Email mistakes by U.K. inquiry lead to $345,000 privacy fine

https://www.itworldcanada.com/article/email-mistakes-by-u-k-inquiry-lead-to-345000-privacy-fine/407240

Technology can do wonders to strengthen the security and privacy activities of an organization, but it can only go so far. Sometimes employees are clumsy when handling personal information and the result can be painful.

The latest example is the roughly $345,000 fine levied Wednesday by the U.K. information commissioner against the country's Independent Inquiry into Child Sexual Abuse for an email mistake.

On Feb. 27, 2017, an inquiry staff member sent a blind carbon copy (bcc) email to 90 inquiry participants — some of whom might have been victims of abuse being investigated — telling them about a public hearing. A "bcc" wouldn't have allowed recipients to see the names of other people. So far so good.

However, after noticing an error in the email a correction was sent — but this time email addresses were entered into the 'to' field, instead of the 'bcc' field. This allowed all of the recipients to see each other's email addresses, identifying them as possible victims of child sexual abuse.

Click link above to read more

WhatsApp to cap message forwarding in effort to stop India lynchings

https://globalnews.ca/news/4342904/whatsapp-india-rumour-child-kidnapping/

Facebook Inc's (FB.O) WhatsApp is rolling out a global test measure to rein in messages forwarded by users, the messaging app said, after the spread of rumours led to several killings in India and sparked calls for action from authorities.

Violence triggered by incendiary false messages in India, WhatsApp's biggest market with more than 200 million users, has spurred government demands to prevent circulation of false texts and provocative content and caused a public relations nightmare.

Click link above to read more

Rowan Atkinson not ‘dead’: Viral Mr. Bean hoax is spreading a real virus

https://globalnews.ca/news/4340576/rowan-atkinson-dead-fake-mr-bean-virus-scam/

Rowan Atkinson, the actor who plays Mr. Bean, is not dead – but your computer might be if you clicked the fake news story about his untimely demise.

The viral hoax presents itself as a video tribute to Atkinson from “FOX BREAKING NEWS,” with his birth and alleged death dates featured next to the preview image.

Users who click the video link will be redirected to a falsified security page prompting them to dial a phone number, according to reports. Anyone who calls the number will be asked to provide their credit card information in order to purchase a so-called software fix, which will actually riddle the targeted computer with viruses.

Click link above to read more

Microsoft exec: We stopped Russia from hacking 3 congressional campaigns

https://arstechnica.com/information-technology/2018/07/microsoft-detected-russian-attempt-to-hack-3-congressional-candidates-this-year/

In a panel discussion at the Aspen Institute's Security Summit yesterday, Microsoft Corporate Vice President for Customer Security and Trust Tim Burt said that in the course of hunting for phishing domains targeting Microsoft customers, members of Microsoft's security team detected a site set up by Russian actors that was being used in an attempt to target congressional candidates.

"Earlier this year," said Burt, "we did discover that a fake Microsoft domain had been established as the landing page for phishing attacks, and we saw metadata that suggested those phishing attacks were being directed at three candidates who are all standing for election in the midterm elections." While Burt would not disclose who the candidates were, he did say that they "were all people who, because of their positions, might have been interesting from an espionage standpoint as well as an election disruption standpoint."

Click link above to read more

$1 million heist on Russian bank started with hack of branch router

https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank/

A prolific hacking group has struck again, this time stealing close to $1 million from Russia’s PIR Bank. The July 3 heist came about five weeks after the sophisticated hackers first gained access to the bank’s network by compromising a router used by a regional branch.

The theft—which according to kommersant.ru is conservatively estimated at about $910,000—is the latest achievement of a group researchers at security firm Group-IB call the MoneyTaker group. In a report published last November that first detailed the group, researchers said its members had conducted 20 successful attacks on financial institutions and legal firms in the US, UK, and Russia. In a follow-up report, Group-IB said MoneyTaker netted about $14 million in the hacks, 16 of which were carried out on US targets, five on Russian banks, and one on a banking-software company in the UK.

Click link above to read more

The Two Biggest Disruptions To Cybersecurity Since The Invention Of The Firewall

https://www.forbes.com/sites/forbestechcouncil/2018/07/19/the-two-biggest-disruptions-to-cybersecurity-since-the-invention-of-the-firewall/#49d193126d4e

One might consider the firewall the most significant invention in cybersecurity in the last 30 years. The firewall has certainly evolved since its inception in 1988 as simple packet filters, launching with stateful filters, then upgrading to its third-generation application layer firewall and more recently upgrading again to the next-generation firewall (NGFW).

While NGFW is certainly part of the cybersecurity stack, NGFW is no longer revolutionizing the way we protect our critical business assets.

Today's cybersecurity strategies have been disrupted by two new models: the Zero Trust model and DevSecOps.

Click link above to read more

Vietnam's New Cybersecurity Law and Push for Internet Sovereignty Reduces Freedom

https://www.databreaches.net/vietnams-new-cybersecurity-law-and-push-for-internet-sovereignty-reduces-freedom/

On June 12th the Vietnamese National Assembly voted in a new cybersecurity law. The legislation did not come easily having gone through more than 12 drafts and much debate in government and the business sector. The claimed purposes of the legislation are to increase Vietnam's Internet sovereignty, that is the data of Vietnamese people should remain within and under the control of Vietnam, and to improve the cybersecurity of the country by controlling what and how people communicate online.

Click link above to read more

Egyptian 'Fake News' Law Threatens Citizens with 5000-plus Followers

https://thehackernews.com/2018/07/social-media-fake-news-law.html

Do you or someone you know lives in Egypt and holds an account on Facebook, Twitter, or/and other social media platforms with more than 5000 followers?

If yes, your account can be censored, suspended and is subject to prosecution for promoting or spreading the fake news through social media platforms.

On July 16, the Egyptian parliament approved a new law that classifies a personal social media account, blog or website with more than 5,000 followers as media outlets, allowing the state to block social media accounts and penalize journalists for publishing fake news.

Social media networks are no doubt a quick and powerful way to share information and ideas, but not everything shared on Facebook or Twitter is true.

Click link above to read more

OCIOSecurity@gov.bc.ca