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

July 10th, 2018

July is "Security while you travel" Month

This week's stories:

New Cyber Security Strategy bolsters cyber safety, innovation and prosperity

https://www.canada.ca/en/public-safety-canada/news/2018/06/new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity.html

The Government of Canada is committed to defending Canada and Canadians against cyber threats.

The Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness, the Honourable Harjit S. Sajjan, Minister of National Defence, and the Honourable Navdeep Bains, Minister of Innovation, Science & Economic Development delivered the *National Cyber Security Strategy.* This new strategy will guide the Government of Canada's cyber security activities to safeguard Canadians' digital privacy, security and economy.

The strategy strengthens both how we combat cybercrimes and how we defend against them. It consolidates federal cyber operations into the new Canadian Centre for Cyber Security, which will create one clear and trusted national authority. Instead of several different departments, the Centre will provide a single window for expert advice and services for governments, critical infrastructure operators, and both the public and private sector to strengthen their cyber security. The Centre's first head will be Scott

Jones, who is currently responsible for the IT Security Branch at the Communications Security Establishment.

A new National Cybercrime Coordination Unit in the RCMP will support and coordinate cybercrime investigations between police forces across the country. New investments will bolster the RCMP's capacity to investigate major cybercrimes that affect the Government of Canada, impact critical infrastructure, and cause the most harm to Canadians. These investments will also enhance the RCMP's ability to conduct criminal investigations with domestic and international partners and provide specialized cyber capability to major investigations.

Click link above to read more

Vladimir Putin calls for countries to combat cyberattacks together

https://globalnews.ca/news/4316574/vladimir-putin-cybersecurity/

MOSCOW — President Vladimir Putin on Friday called for closer international cooperation in fending off cyberattacks.

Addressing a cybersecurity conference in Moscow, Putin said it's important to develop common cybersecurity standards that take into account interests of all nations. He noted that cyberthreats have mounted around the world.

"Cyberthreats have reached such a scale that they could only be neutralized by combined efforts of the entire international community," Putin said.

Click link above to read more

Why are there so many robocalls? Here's what you can do about them

https://www.thestar.com/wsj/technology/2018/07/03/why-are-there-so-many-robocalls-heres-what-you-can-do-about-them.html

Remember when phone calls meant people wanted to talk to you about something other than lowering your interest rates? These days, the phone rings so often with recorded robocall messages — You qualify! You owe! You've won! — answering feels like a hazard.

I hit my own robocall breaking point a month ago. I was grabbing a quick shower before catching a flight. My phone rang. Fearing I'd miss a call from my boss, who had been trying to reach me, I jumped out. But no, it was a recording instead.

I resisted the urge to throw my phone across the bathroom and went looking for answers. Why can't anyone stop this madness? When will it end?

First, the bad news: Almost every person I talked to about robocalls used the phrase, "There's no silver bullet."

But developments in the works should get the robocall problem more under control. And there are steps to take on your own that actually do reduce calls. Where did this evil come from? Back when phone calls were transmitted over copper wires, businesses paid a lot of money for phone systems that allowed 1,000 employees to make calls without needing 1,000 phone lines. These systems inserted caller ID so, for instance, customers all saw the same business number, regardless of which employee made the call.

Click link above to read more

Google docs are secure, company says, despite privacy issues reported in Russia

https://globalnews.ca/news/4314393/google-docs-privacy-issues-russia/

MOSCOW — Google said Thursday that its document writing tool Google Documents was secure even as Russian internet users discovered scores of files that appeared to be intended for private use.

The Russian internet company Yandex said in a statement that some users contacted the company Wednesday to say that its public search engine was yielding what looked like personal Google Documents files, suggesting there may have been a data breach.

On Wednesday night, Russian social media users started posting scores of such documents, including an internal memo from a Russian bank, press summaries and company business plans. The veracity of those documents could not be independently confirmed.

Click link above to read more

Millennials to blame for data breaches too, Shred-it claims

https://www.itworldcanada.com/article/millennials-to-blame-for-data-breaches-too-shred-it-claims/406838

Millennials have been blamed for killing many fine and decent things – ranging from products to hobbies to entire industries – and now you can add data protection to the list of casualties as well, according to a new report from Shred-it.

Shred-it, a global information destruction services firm, hired Ipsos to conduct a study in Canada of small business owners (surveying 1,002) and C-suite executives of companies with more than 100 employees (surveying 100). The results were made available in late June in Shred-it's Security Tracker 2018.

Segmenting out the respondents into age groups, the study reports that millennials (defined here as age 18-34) are "not as savvy as we thought" when it comes to data protection practices.

Here are a few of the data protection sins that millennials commit, leading to greater risks of data breaches:

48 per cent leave their notebooks on their desk after they leave work for the day. Comparatively, 37 per cent of Gen-X and 21 per cent of baby boomers also do this.

37 per cent report leaving their computer on and unlocked after work, compared to 22 per cent of Gen-X, and 12 per cent of boomers.

Only half of millennials regularly shred confidential documents, compared to 65 per cent of Gen-X, and 52 per cent of boomers.

Click link above to read more

Are vacationing employees at risk of identify theft?

https://www.canadiansecuritymag.com/news/data-security/are-vacationing-employees-at-risk-of-identify-theft

Identity theft is a massive problem for every business. It is a crime that threatens every employee regardless of age, income level or type of employment. It is estimated that Canadians lost over $290 million to fraudsters, from January 2014 to December 2016. This concern is rising. In a 2017 survey from the Chartered Professional Accountants of Canada, more than 71 per cent of respondents indicated a concern about fraud today.

With the summer break fast approaching, employees will be taking off for vacation with families and friends. Since 66 per cent of employees take work away with them on vacation, businesses need to consider implementing information security vacation policies to ensure employees are identity fraud safe when traveling. Failure to take precautionary measures can ultimately affect your business's bottom line and corporate reputation.

Click link above to read more

How much all seeing AI surveillance is too much?

https://www.canadiansecuritymag.com/news/industry-news/how-much-all-seeing-ai-surveillance-is-too-much

BOSTON — When a CIA-backed venture capital fund took an interest in Rana el Kaliouby's face-scanning technology for detecting emotions, the computer scientist and her colleagues did some soul-searching — and then turned down the money.

"We're not interested in applications where you're spying on people," said el Kaliouby, the CEO and co-founder of the Boston startup Affectiva. The company has trained its artificial intelligence systems to recognize if individuals are happy or sad, tired or angry, using a photographic repository of more than 6 million faces.

Recent advances in AI-powered computer vision have accelerated the race for self-driving cars and powered the increasingly sophisticated photo-tagging features found on Facebook and Google. But as these prying AI "eyes" find new applications in store checkout lines, police body cameras and war zones, the tech companies developing them are struggling to balance business opportunities with difficult moral decisions that could turn off customers or their own workers.

El Kaliouby said it's not hard to imagine using real-time face recognition to pick up on dishonesty — or, in the hands of an authoritarian regime, to monitor reaction to political speech in order to root out dissent. But the small firm, which spun off from an MIT research lab, has set limits on what it will do.

Click link above to read more

Deloitte report warns of growing Canadian cybersecurity talent gap

https://www.canadiansecuritymag.com/news/data-security/deloitte-report-warns-of-growing-canadian-cybersecurity-talent-gap

A new report by Deloitte says Canada is facing growing demand for cybersecurity talent that schools and other organizations are struggling to address.

The consultancy says demand for cyber talent in Canada is climbing by seven per cent annually and estimates there will be more than 5,000 cybersecurity roles to fill between 2018 and 2021, but did not say how big a recruitment shortfall it expects.

Deloitte says the skills shortage is part of a global problem where the cybersecurity workforce gap is expected to stand at 1.8 million by 2022.

The firm say addressing cybersecurity risks is critical as they could slow the pace of global technological innovation by as much as US$3 trillion in lost economic value in 2020.

Deloitte says Canadian schools are struggling to keep up with the rapidly evolving field, while also facing competition from industry for qualified instructors.

It says companies will need to make use of consultants, adapt to rising pay expectations, and broaden recruitment efforts to try and fill the gap.

Click link above to read more

Samsung’s texting app reportedly sent pictures to people’s contacts without permission

https://www.thestar.com/business/technology/2018/07/03/samsungs-texting-app-reportedly-sent-pictures-to-peoples-contacts-without-permission.html

A handful of Samsung smartphone owners say that their phones have sent their stored photos to their contacts completely on their own.

The problem appears to stem from Samsung Messages, as first reported by Gizmodo. Samsung Messages is the default messaging app on Samsung phones. The few reports of this bug indicate that the phones are sending the messages without the app recording any trace of an outgoing message.

It’s not clear how many people have reported this sort of thing happening, but if it is a bug it would be a major privacy violation.

“We are aware of the reports regarding this matter and our technical teams are looking into it. Concerned customers are encouraged to contact us directly at 1-800-SAMSUNG,” Samsung said in a statement. The company did not propose a solution to the problem.

Click link above to read more

Polar App Disables Feature That Allowed Journalists to Identify Intelligence Personnel

https://www.bleepingcomputer.com/news/technology/polar-app-disables-feature-that-allowed-journalists-to-identify-intelligence-personnel/

Finnish-based fitness tracking app Polar has temporarily disabled its global activity map feature after last week journalists used it to track down the real-world identities of military and intelligence personnel.

The investigations were carried out by reporters from Dutch newspaper DeCorrespondent and online investigations group Bellingcat.

These two group of reporters discovered that Polar Flow, one of the Polar apps, was allowing anyone access to a feature called Explore, which is an activity map. Data exposed on this map included a user's past activity, such as running or biking routes, but also the user's personal details such as heart rate, physical attributes, and more.

While other fitness apps have released activity maps in the past —for showing popular running, hiking, or biking paths— Polar made the mistake of exposing the username and personal details of each user for each individual activity/route.

Click link above to read more

Timehop Security Breach Affects the Company’s Entire 21 Million Userbase

https://www.bleepingcomputer.com/news/security/timehop-security-breach-affects-the-company-s-entire-21-million-userbase/

Timehop, a mobile app that surfaces old social media posts from the same day but from previous years, has announced a security breach affecting its entire userbase of over 21 million users.

Not all users were affected to the same extent. The company said a hacker gained access to its infrastructure and stole details on its users that included usernames, emails, telephone numbers, and access keys.

According to preliminary evidence from the investigation, the intrusion took place on December 19, 2017, when a hacker gained access to an admin account for Timehop’s cloud infrastructure. Timehop says it failed to secure that account with multi-factor authentication, making the attack possible.

Click link above to read more

Attackers could use heat traces left on keyboard to steal passwords

https://www.welivesecurity.com/2018/07/06/thermanator-attackers-heat-keyboard-password/

A team of academics from the University of California, Irvine (UCI), have presented a type of attack that could enable a malefactor to retrieve sensitive information you entered via your keyboard – possibly up to a minute after you typed it.

The researchers had 30 users enter 10 different passwords, both strong and weak, on four common external keyboards. Using a thermal imaging camera, the researchers then scanned the residual heat left on the recently-pressed keys. In the second stage, they enlisted the help of eight non-experts in the field

who, acting as “adversaries”, were asked to derive the set of pressed keys from the thermal imaging data – which they reliably did.

Long story short, the subjects successfully retrieved entire sets of key-presses that were captured by the camera as late as 30 seconds after the first key was entered. In addition, recovery of a partial set of key-presses was possible one minute after the first key was pressed, according to the researchers, who described their findings in a paper called “*Thermanator: Thermal Residue-Based Post Factum Attacks On Keyboard Password Entry*”. The pieces of the puzzle thus obtained could be easily leveraged for password-cracking attacks.

Click link above to read more

UK to Establish Court for Cybercrime in London

https://www.bankinfosecurity.com/uk-to-establish-court-for-cybercrime-in-london-a-11174

The U.K. has approved a plan to build a cutting-edge court complex in London designed to handle cybercrime, fraud and economic crime.

The decision comes after a feasibility study was launched last October. That study took into account the economic benefits that would flow from an upgrade of London's legal services facilities.

The complex, which will also handle criminal and civil cases, is intended to replace an aging civil court, the Mayor's and City of London County Court and Magistrates' Court, according to a news release from the Ministry of Justice and HM Courts and Tribunals Service. The U.K. government plans to spend £1 billion (US$1.32 billion) on modernizing its courts and tribunals in England and Wales.

"It's essential that we have bespoke facilities able to deal with modern crime and modern issues," says Catherine McGuinness, policy chairman, City of London Corporation, in a video.

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:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca