Security News Digest
February 14, 2017

You might occasionally hate your computer,
so take the Love Security - Love Your Data Quiz.

Canadians Lost $17M In Online Dating Scams Last Year: RCMP

http://www.huffingtonpost.ca/2017/02/14/canada-online-dating-scam-2016_n_14751214.html

It started with a Facebook conversation with a stranger, then progressed to Skype exchanges, declarations of affection and promises to meet up in person. By the time Louise, 56, contacted police roughly a year later, she still hadn't met her online connection - but she had sent roughly $100,000 overseas at his request, and spent another $25,000 on travel and related expenses. "He was very charming, very nice," said Louise, who did not want her full name used in order to protect her privacy. "I thought he was sincere, that he would pay me back." With people increasingly looking for love online, RCMP are warning Canadians to protect their wallets as well as their hearts. [article gives details about how Louise's situation slowly escalated over time]

RCMP said many people who fall prey to such scams are reluctant to report the crime, out of embarrassment or.-.in the case of older people - out of fear that they will lose independence as concerned family members step in. Scammers create fake online profiles in order to gain someone's trust then ask for money, often claiming to be faced with an emergency, RCMP said. That can involve fake social media profiles as well as those on dating sites or apps. *Some red flags to watch for include someone professing their love before meeting in person, or claiming to be from the same town but working overseas, which may be a setup to ask for money later, the force said*.

Don't send money at all: RCMP The best solution is to simply not send anyone money, it said. RCMP also said there are safety risks with online dating because it's difficult to verify a person's identity or motivations before meeting them. They recommend having the first date in a public place and arranging your own transportation so that the other person doesn't know where you live [and it is easier to leave]. *They also suggest telling a friend or family member the person's name and where you're meeting them as well as when you expect to be back*.

Here's Why Reports of Data Breaches Will Skyrocket This Year

http://www.cbc.ca/news/technology/cyber-attacks-data-breaches-reporting-canada-privacy-law-1.3972862

Nobody likes to talk about getting hacked. For one, it's embarrassing. And for companies, it's a quick way to lose customers' trust. It's why you rarely hear about data breaches or cyberattacks on big businesses unless the companies are forced to admit something happened. *But over the next few months, more Canadian companies will have to start speaking up, whether they like it or not - especially if the theft of personal information is involved. Upcoming changes to Canadian privacy law and recent guidance from the Canadian Securities Administrators mean that Canadian companies will not only have to disclose more about cyberattacks than they have in the past, but be more proactive about disclosing specific risks that could lead to attacks in the future.* For Canadians, it should mean more insight into what companies are doing to protect your data. And if your data is lost or stolen, companies will have to tell you, or risk being fined. No more sweeping attacks under the rug.

…"There are a significant number of breaches that never get reported because there's no obligation to report them," says Imran Ahmad, a partner at the law firm Miller Thomson, who specializes in cybersecurity. But later this year that will start to change. *The short history is that in June 2015 the Canadian government passed the Digital Privacy Act requiring, among other things, that data breach notification and reporting regulations become part of Canadian privacy law. The government expects to publish draft regulations "sometime in early 2017,"* according to an Innovation, Science and Economic Development spokesperson, but couldn't say when the final regulations will be published, or when they might come into force. However, Ahmad, as well as others in the industry, say they expect the

regulations to take effect by the fourth quarter of this year. From then onward, organizations will have to log all breaches, and users will have to be notified of any breach that poses "a real risk or significant harm."

…The Canadian Securities Administrators (CSA), on the other hand, is doing its part to ensure that publicly traded Canadian companies are more transparent about their cybersecurity practices before they get hacked - and not just afterward. Last month the CSA looked at how 240 publicly traded companies in Canada talked about cybersecurity in their financial filings - the potential impact of a cyberattack, information at risk, who handles the company's cybersecurity, and any disclosures of previous breaches or attacks. *The CSA found that 40 per cent of companies failed to address cybersecurity risks in their disclosures. And generally speaking, the CSA found that filings tend to use generic, boilerplate language - even though different types of companies face different types of cyberattacks or threats, and hold different types of data subject to varying degrees of risk*. For banks, Ahmad said, the big risk is phishing (fraudulent emails purporting to be from a legitimate source), while for an online store, it's a distributed denial of service (DDoS) attack - which are two different risks. "Taking down the website of a manufacturer may not have the same impact on their operations as a DDoS attack on an e-commerce business," Ahmad said. *In its guidance note, the CSA says it expects issuers "to provide risk disclosure that is as detailed and entity specific as possible" and that it will be monitoring companies for compliance*. "I think the next step is probably going to be, what is the enforcement action for non-compliance?" Ahmad said. "We're not there yet, but that's where we're headed."

City [Guelph] Notifying Staff whose Private Information was Compromised

https://www.guelphtoday.com/local-news/city-notifying-staff-whose-private-information-was-compromised-533512

City staff whose private information may have been compromised in an email leak last month are being notified by the city. The province's Information and Privacy Commissioner is also involved in the matter, as per protocol, said city CAO Derrick Thomson on Friday. "We have a duty to contact them and we've done that," Thomson said of the independent body that reviews government decisions and practices concerning access and privacy. *Early last month over 50,000 email items were accidentally given to a former city employee as part of an ongoing $1 million wrongful dismissal lawsuit early last month. Court documents claim that included on a flash drive handed over to former building official Bruce Poole were many documents containing private and confidential information regarding city employees, including at least 30 performance reviews of staff*.

City clerk Stephen O'Brien said that initial notification has already taken place in some cases and written notifications will also be sent out. Given the sheer volume of information that was "inadvertently" handed over to the fired employee, the city is still in the process of figuring out just what it included. The information was all from the email account of former Deputy Chief Administrative Officer and city treasurer Al Horsman. "There's a significant amount of information," O'Brien said. Deputy CAO Mark Amorosi was fired on Thursday as a result of the information leak.

Canada Revenue Agency Monitoring Facebook, Twitter Posts of Some Canadians

http://www.cbc.ca/news/politics/taxes-cra-facebook-big-data-1.3941416

[Jan19] The Canada Revenue Agency is scrutinizing the Facebook pages, Twitter feeds and other social media posts of Canadians it suspects could be cheating on their taxes. That's just one example of the agency's increasing focus on what it can learn by collecting and analyzing many kinds of data - both its own internally generated information and what it calls "publicly available information." "The CRA does practice risk-based compliance, so for taxpayers identified as high risk, any relevant, publicly available information relating to the specific risk-based factors for the taxpayer may be consulted as part of our fact-gathering processes," said spokesperson David Walters. Among those considered high risk are wealthy Canadians with offshore bank accounts, said Jean-François Ruel, director of CRA's Strategy and Integration Branch. "If we go with high-risk, high-wealth individuals that do offshore [banking], then we would look at all information that is public for compliance action."

Tobi Cohen, spokesperson for the privacy commissioner, said CRA notified it of its plan to collect publicly available information from social media in connection with "tax fraud and non-compliance risk analysis, audits and investigations." However, David Christopher, of the advocacy group Open Media, said his organization opposes government agencies monitoring what Canadians are saying on social media. *"When Canadians post something on Facebook, they believe that they are sharing that with their friends and with their family. They don't believe that they are sharing that with some government bureaucrat in*

Ottawa," he said. *"Unfortunately, Facebook's privacy settings are notoriously complex and many people might think that they are posting something to their friends and it ends up getting shared with the whole world."*
The revelation that the Canada Revenue Agency is checking social media posts comes as the agency is also expanding its use of cutting-edge technology and data analysis to better catch tax cheats, to target people for audits and to improve its service for Canadians. *Business intelligence, also known as big data, is a rapidly growing area within CRA*. In 2016 alone, the agency posted three separate privacy impact assessments centred on its plans to use business intelligence techniques in its operations. [see article for details]
Colin Bennett, a University of Victoria professor who specializes in privacy, said government use of big data techniques is causing concern among privacy advocates. When Canadians provide information to the government, they provide it for a specific purpose, not for algorithms and predictive analytics, he said. "You are getting beyond the initial reason why the data were collected in the first place, which is to administer our tax system, and it is becoming far more hypothetical, far more speculative and concerning."

CRA Spends Millions But Fails to Stop Tax Workers from Snooping on Canadians, Documents Show

http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-tax-files-commissioner-1.3905608
[Dec21/16] Canada Revenue Agency workers continue to snoop on the confidential tax files of businesses, acquaintances and others, despite at least $10.5 million spent so far to try to stop them. CBC News has uncovered nine significant cases reported since Jan. 1/16 in which tax workers improperly poked around the government's electronic records to extract sensitive private information about income, deductions, benefits, payments and employment. It's a long-term, chronic problem at the agency, exposed in 2009 and again in 2013 by Canada's privacy commissioner, who was assured that managers were taking tough action to prevent the breaches. But more than three years later, confidential tax files are still susceptible to nosy workers armed with passwords and CRA-supplied computers. On Feb. 18, for example, the agency reported that a "CRA employee made unauthorized access to the accounts of 90 acquaintances and family members, 1 business and his/her own account." In another breach reported on Feb. 22, an employee improperly accessed the accounts of 227 businesses and individuals. CBC News obtained records detailing the latest crop of privacy breaches, altogether affecting about 500 Canadians, under the Access to Information Act.
Federal government departments are responsible for hundreds of significant privacy breaches each year, but most are inadvertent, such as mail sent with the wrong address or misplaced memory sticks. Most cases at CRA, on the other hand, are the result of deliberate snooping by employees. The agency has spent $10.5 million since 2013 to make its computers more secure against its own workers, and more money is earmarked for next year to comply with recommendations from the federal privacy office, including enhancing system controls so employees can only access information they need to do their jobs.

IBM's Famed Watson Computer 'Gets a Job' Fighting Cybercrime Threat

http://thechronicleherald.ca/novascotia/1441205-ibms-famed-watson-computer-gets-a-job-fighting-cybercrime-threat
A year after IBM began teaching its Watson computer system to fight cybercrime, the company is making the platform available for use. "Now he gets a job and makes us some money," quipped Caleb Barlow, vice-president of IBM Security. He said a new app called IBM QRadar Advisor is now available as a tool to help determine the seriousness of a cyber threat. *Barlow said security teams sift through over 200,000 security events per day on average, trying to determine what might be a serious threat. More than 20,000 hours per year are wasted chasing false positives, he said. "What Watson for cybersecurity does is sit beside those human beings and acts like their research assistant," he said.*
Watson - IBM's question-answering computer system - was originally designed to compete (and win) on the television quiz show Jeopardy!, but the technology has since been used on other problem-solving projects from clothing design to cancer. The University of New Brunswick is one of 40 customers around the world who have been beta testing the new app. Others included California State Polytechnic, Sun Life Financial, and the University of Rochester Medical Centres. David Shipley, UNB's director of strategic initiatives for information technology services, said *research that would take him half a day only takes Watson a few minutes. He said that before Watson, he could only select the worst cases and try to*

make an objective analysis based on what knowledge he has been able to gather. "Our ability to do that as people is limited to how much information we can learn about the latest and greatest attacks. There is a great volume of information produced every day, and I as an educated professional may be able to consume one per cent of that," Shipley said. *"With Watson, because it is a system of cognitive computing, it can consume all of this data."* Shipley said he now seeks advice from Watson on 10 to 15 cyber threats each day. Barlow won't discuss prices, but said he expects the new app will be used primarily by large universities and corporations. *It's estimated that by 2020, there will be two million unfilled cybersecurity jobs*.

Top Mistakes Users Make With Their Smart Devices

https://hotforsecurity.bitdefender.com/blog/top-mistakes-users-make-with-their-smart-devices-17685.html

As IoT [Internet of Things] grows in popularity, everyone wants a piece of it, starting with tech giants Google, Amazon and Apple, and ending with startups and the consumer. *But just because the number of companies embracing it is growing, it doesn't mean the products properly sync with all infrastructures, that they have no backdoors or that users know what they're getting into*. Sure, it sounds amazing to monitor your home, answer the door while on vacation or dim the lights through voice control. At some point, we all fall into the trap of wanting to be at the front of a new trend. *But the lax security turns them into multiple entry points for hackers. Simple user mistakes often facilitate attacks disseminated by exploited IoT devices*.

What are some top mistakes users make when embracing smart devices? (1) People are often not even aware they live in a smart home. Only a fifth or fewer consider their homes to be smart, according to Bitdefender research. (2) Not researching the legitimacy of the manufacturer and not reading product reviews for the device they want to purchase. It is vital to double check that you're dealing with a trustworthy, reputable brand. (3) *Users automatically connect all the devices to their home infrastructure. This makes them vulnerable to attacks, as it creates multiple entry points for hackers. Plus, if one device is hacked, the rest will follow*.

"On average, a household from the United States carries 13 smart devices or accessories. There are 12 in the UK and Australia, and 10 in France, Romania and Germany," Bitdefender found. *"In most homes, the top devices that have access to the home's Wi-Fi network are smartphones, Windows desktop computers and tablets, followed by smart TVs and wireless gaming consoles."* .. "42% Americans have never updated the firmware or default software package. ..*If there is anything worse than weak "1234"-type passwords, it is reusing the password for all devices, as have 16 percent of US users. The basic, default passwords allow hackers easy access into any device and network, and are the root cause for massive data leaks*. "Almost every gadget we've analyzed in our ongoing security research on IoT gadgets displayed weak user credentials and no hot-spot authentication," says Alexandru Balan, Chief Security Researcher at Bitdefender. "Changing default passwords is a critical security practice, yet a lot of users still ignore it."

DHS Uses Cyber Kill Chain to Analyze Russia-Linked Election Hacks

http://www.securityweek.com/dhs-uses-cyber-kill-chain-analyze-russia-linked-election-hacks

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) on Friday *published a new report providing additional indicators of compromise (IOC) and analysis using the cyber kill chain to detect and mitigate threats from the Russia-linked "GRIZZLY STEPPE" hackers*. On Dec. 29, 2016, the DHS and FBI published an initial Joint Analysis Report (JAR) detailing the tools and infrastructure *used by Russian hackers designated by DHS as "GRIZZLY STEPPE" in attacks against the United States election*. The previous report, however, didn't deliver on its promise, security experts argued. While the original report included a series of IOCs, some said that they were of low quality, had limited utility to defenders, and were published as a political tool attempting to connect the attacks to Russia.

The new report is described by DHS as an Analytical Report (AR) providing a "thorough analysis of the methods threat actors use to infiltrate systems" in relation to the GRIZZLY STEPPE hackers. The report provides additional details on IOCs, along with analysis along phases of the cyber kill chain, and suggests specific mitigation techniques that could be used to counter GRIZZLY STEPPE attackers. DHS analysts leveraged the Cyber Kill Chain framework created by Lockheed Martin that describes the phases of an attack. The report summarizes the activity of the campaign using each phase of the Cyber Kill Chain,

which are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on the Objective.
The report also provides detailed host and network signatures to help defenders detect and mitigate GRIZZLY STEPPE related activity, including additional YARA rules and IOCs associated with the attacks. The DHS has previously said that two different actors participated in the political attacks, one in the summer of 2015, namely APT29, and the other in spring 2016, namely APT28. The former is also known as Cozy Bear, or CozyDuke, while the latter is referred to as Fancy Bear, Pawn Storm, Strontium, Sofacy, Sednit and Tsar Team. DHS recommends that security teams read multiple bodies of work from various sources concerning GRIZZLY STEPPE.

UK Hit by 188 High-Level Cyber-Attacks in Three Months

https://www.theguardian.com/world/2017/feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin

Britain is being hit by dozens of cyber-attacks a month, including attempts by Russian state-sponsored hackers to steal defence and foreign policy secrets, GCHQ's new cybersecurity chief has said. Ciaran Martin, head of the new National Cyber Security Centre (NCSC), told the Sunday Times there had been a "step change" in Russia's online aggression against the west. His comments came as the chancellor, Philip Hammond, told the Sunday Telegraph the centre had blocked 34,550 "potential attacks" on government departments and members of the public in the past six months – about 200 cases a day. Allegations of Russia-sponsored cyber-attacks became a focal point during the US election, raising fears that the tactic was on the rise. Martin said Britain had been hit by 188 high-level attacks, "many of which threatened national security", in the last three months. He told the Sunday Times: "In the case of government departments, [it is] getting into the system to extract information on UK government policy on anything from energy to diplomacy to information on a particular sector." Attacks by Russian and Chinese state-sponsored hackers on defence and foreign policy servers are among those being investigated by the NCSC, the newspaper said. Martin added: "Over the last two years there has been a step change in Russian aggression in cyberspace. Part of that step change has been a series of attacks on political institutions, political parties, parliamentary organisations and that's all very well evidenced by our international partners and widely accepted."

NSA Contractor Could Face 200 Years in Prison for Massive Breach

https://www.databreaches.net/nsa-contractor-could-face-200-years-in-prison-for-massive-breach/

Elias Groll reports: *U.S. prosecutors unveiled an indictment Wednesday detailing what may amount to the largest data breach in the history of the National Security Agency - an archive of classified material that may total more than 500 million pages*. The incident is a black eye on the secretive spy agency's attempt to crack down on so-called insider threats and may have exposed some of the NSA's most sensitive spy tools. *Prosecutors allege Harold T. Martin III stole a huge trove of classified documents, which he stored at his home in Maryland, while working as a contractor to the NSA and other intelligence agencies*. While the full scope of Martin's collection of top secret material remains unclear, Wednesday's indictment includes 20 charges of improperly retaining classified information. If convicted, Martin could face a maximum of 200 years in prison.
…At the time of his arrest, Martin worked as a contractor for Booz Allen Hamilton, the giant defense contractor. *Martin's role in the center of a massive breach of classified information is a huge embarrassment for the firm, which also employed NSA whistleblower Edward Snowden. Since Snowden's leaks, the agency has spent billions trying to improve internal security*.
…This is a hugely concerning breach as well as an embarrassment to both the NSA and BAH. *After everything with Snowden, how was this contractor's employee able to steal so many documents?* And what kind of ongoing checks does BAH do on its employees? I imagine there will be a lot of hard questions asked in internal reviews and closed congressional hearings, but will anything actually change to prevent this type of thing again?

Apple iCloud Didn't Wipe 'Deleted' Browser Histories for Over a Year

https://hotforsecurity.bitdefender.com/blog/apple-icloud-didnt-wipe-deleted-browser-histories-for-over-a-year-17677.html

Yesterday Russian computer forensic firm Elcomsoft rang the alarm, *warning that it was possible to extract users' Safari browsing history over a year after the user believed that they had deleted their browsing history*. "We discovered that deleting a browsing history record makes that record disappear

from synced devices; however, the record still remains available (but invisible) in iCloud. We kept researching, and discovered that such deleted records can be kept in iCloud for more than a year." *Forbes reporter Thomas Fox-Brewster confirmed the behaviour, discovering almost 7000 "deleted" records from his browsing history dating back to November 2015. Each entry was accompanied by a counter for how many times the webpage had been visited, and the time and date that the history item had been "deleted"*. Obviously this is a concern. A user's browsing history can be highly sensitive, and Safari users would have an expectation that if they had deleted entries from their browser history it should have been… you know… properly deleted rather than simply hidden out of a regular user's sight.
As more than one wag has pointed out, when Apple's privacy statement declares: "Apple does not retain deleted content once it is cleared from Apple's servers." that's rather different from saying: "Apple does not retain deleted content once it is deleted by the user."
So, what's going on here? *Well, it appears that the problem was associated with Apple users' ability to sync their Safari browsing history to iCloud accounts, letting them easily access previously visited sites from other linked devices using the same Apple ID*. If you had not chosen to sync Safari with iCloud it looks like you weren't at risk. Similarly the history of anywhere you visited during a Private Browsing session had also not been collected – which I'm sure will be a huge relief to many.
The hullabaloo about deleted histories being not really deleted seems to have stirred Apple into taking action, with Elcomsoft reporting that Safari browser data stored in iCloud now seeming to be properly wiped if it is more than two weeks old.

It's Not Just Your TV That Can Track Your Habits Without Consent

http://www.cbc.ca/news/technology/privacy-tracking-personal-information-vizio-consent-data-1.3980702

What companies do with your data depends on how 'personal information' is defined. If you want to know what products and services are tracking you without your consent, their privacy policies are a good place to start. Own a PlayStation? Sony can share "non-personally identifying information and behavioural data from our studies with our affiliates and other third parties." Belkin - which makes a line of smart light switches and power plugs under the WeMo brand - may also share "aggregated and anonymized non-personal information" about how you use its products with third parties. Similarly, "service providers, business partners and other trusted affiliates" might know how often you turn your smart light bulb on or off if you own a Philips Hue.
But privacy policies only tell part of the story. *"I think what I'm frequently shocked by is how advanced the technology capabilities are to do these things," says Fatemeh Khatibloo, an analyst at Forrester Research who specializes in consumer privacy. "I'm rarely surprised by what people will do. I'm surprised by what they can do."* Vizio TV owners in the U.S. found this out the hard way last week. The company was forced to pay the U.S. Federal Trade Commission $2.2 million U.S. for tracking the viewing habits of TV owners without their consent - then combining that data with information such as sex, age, income and marital status and selling it to third parties. 'They say, "We never share personally identifiable information," [but] they're still selling a lot of identifying info.' ..To pull it off, Vizio recorded some of the pixels displayed on consumers' TVs, and matched them with a database of TV shows, movies and ads (the company said that tracking was not enabled in Canada).
Though an extreme example, the Vizio case is part of a larger trend. A new generation of smart, always-on, internet-connected devices is redefining how companies collect and share user data - both the types of data collected and who that data is shared with. *And despite vague assurances that many types of data are only shared in anonymous, aggregate form - or better yet, with your consent - it's rarely clear what's happening behind the scenes.*
Much of what we know about what companies do with our data *depends on what's considered personal information* - typically, the threshold for whether data can be shared without your explicit consent. "That's the loophole," says Pam Dixon, executive director of the World Privacy Forum, a non-profit research group. She says *the definition of "personally identifiable" is typically up to the company. "Typically when you read a privacy policy and they've carved out exclusions and they say we never share personally identifiable information, they're still selling a lot of identifying info,"* says Khatibloo.
….But as the number of connected products and services continues to rise, it's only going to get more challenging to keep up. *"I think the most important examples of data sharing that we're going to encounter in our everyday lives going forward is our cars, and our medical devices," says Dixon (think driving data and health history). "The key thing is, if you can tie that information back to a profile, like an individual or a single household, then it's identifiable. End of discussion."*

Feel free to forward the Digest to others that might be interested.
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 Technology, Innovation and Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****