BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest
January 16, 2018

Resolve to be a Security Star by taking the ‘Security New Year’ Quiz

Clutch Your Laptop, Wipe Your Data and Other Tips for Travellers, Courtesy of Canada’s Spy Agency 🇨🇦

https://www.theglobeandmail.com/news/national/wipe-data-before-you-leave-home-and-other-tips-for-travellers-courtesy-of-canadas-spy-agency/article37601269/

When Guy Saint-Jacques was ambassador to China, he always told his Canadian visitors to keep a close eye on their digital devices, and never to leave them unattended in hotels. "Assume that if you leave your computer in your room, somebody will come in and copy what you have on your hard drive and copy a list of contacts, everything," Mr. Saint-Jacques said in an interview. Even today, 18 months after retiring from the post, he always makes sure his laptop is within reach whenever he returns to China. That is not paranoia – it is Canadian government policy, according to a document obtained under Access to Information laws.

Far From Home: A Travel Security Guide for Government Officials is circulated by Canada's spy service. The Globe obtained the most recent version of this primer, which is **for federal civil servants who journey abroad. "Canadian citizens travelling abroad may be the target of foreign-intelligence collection," it states**. While it is directed at readers who may carry classified information, **the guide includes tips that could be useful for everyone, from business travellers to backpackers**. "It's a pretty reasonable document that outlines a broad range of potential threats," said Chris Parsons of the University of Toronto's Citizen Lab, the digital-rights group that last month put out its own security planner to help people thwart surveillance.

Today's reality is that many governments mass-collect information. Not just state secrets, but also corporate correspondence or even people's contact lists. The Far From Home guide refrains from naming the most problematic places, **broadly suggesting that government officials carry devices that have been completely wiped of data before they leave Canada**. Foreign spy services, border guards, even criminal gangs are all said to want to copy the contents of travellers' laptops and smartphones. **And any phone that is known to a hostile government can be a tracking device**. "Your phone has a unique signature that, once brought to the attention of an attacker, can be followed anywhere in the world," the guide says.

While CSIS must get approval from judges for its most invasive domestic-spying techniques, travellers do not have the same privacy rights as citizens who stay put. For example, **border agents everywhere do not need warrants to search devices. The U.S. government last week said such seizures by its own border guards were up 60 per cent over the past year**.

Citing growing governmental use of facial-recognition software and similar tools, the CSIS brochure points out that travellers may even be recognized in places they have never been to before. "A number of countries share the biometric information they collect with neighbouring countries. It is possible this information is readily available in a country you have never travelled to."

The standard warnings against using hotel WiFi connections and Internet cafés are repeated, given that communications sent from these places can be easily intercepted. "Use encryption and Virtual Private Networks (VPN) if you must work using non-secure networks," the guide says. Foreign hotels are deemed risky places in general because authorities can direct staff to conduct surreptitious searches of unattended safes, phones and rooms. If a traveller discovers such activity, hotel staff "may deliberately want to mislead you by passing off the operation as a criminal activity," the guide says. That's one of the reasons the CSIS guide urges government travellers to carry a smartphone or laptop that "contains no information when you leave and that, **upon your return, it is completely wiped clean and the operating system re-installed**."

The reason for doubling down on data hygiene upon return is that **hackers can try to activate microphones on any device compromised abroad and listen in on privileged conversations federal officials would have once back in Canada**. Meanwhile, conventional eavesdropping campaigns remain an everyday reality for diplomats stationed abroad.

Mr. Saint-Jacques says he found out all about that on an earlier posting to China in the late 1990s. The former Canadian ambassador vividly recalls his then-teenage daughter telling him about a chat with a schoolmate on an unsecured telephone line. When the conversation turned toward practising conversational Spanish for their class, the two teenagers were suddenly interrupted. "Switch back to French or the line will be cut," an unfamiliar voice said.

A previous iteration of the CSIS Far From Home guide came to the public's attention in 2013, after it was obtained by The Canadian Press. That report highlighted the guide's continued warnings about traditional espionage threats such as "honey traps," which it explained were "the clandestine recording of an intimate encounter" for blackmail purposes.

Canadian [B.C. man] Charged with Unleashing 'Spambot' Army on Twitch

http://www.cbc.ca/news/canada/british-columbia/twitch-brandan-apple-spambot-mischief-1.4483998

A B.C. man accused of overwhelming the American social media giant Twitch with an army of spambots now faces an unprecedented charge of "mischief in relation to computer data." **Brandan Lukus Apple is also subject to an unusual civil order restraining him from creating or selling "any robot, bot, crawler, spider, blacklisting software or other software" aimed at harming the popular streaming service.**

Twitch Interactive hosts more than two million people from around the world who earn money by streaming video-game related content. **The site claims to attract 100 million viewers each month, many of whom engage in chats with both Twitch broadcasters and each other in the channel's margins**. The incident which sparked the criminal mischief charge allegedly happened between February and May of 2017 when thousands of Twitch broadcasters were deluged with a crippling stream of racist, homophobic and otherwise harassing comments. According to a filing sworn in Port Coquitlam provincial court last month, Apple is accused of "wilfully causing multiple repetitive messages to be transmitted." The criminal charge is separate from a B.C. Supreme Court civil action which saw Twitch file a notice of claim last April to stop the 20-year-old from running a web service that promised it could "be used to bomb/spam/flood any TwitchTV chat." Apple did not file a defence in relation to the civil claim.

The Supreme Court documents describe a spambot as "a computer program used to send unsolicited messages (or spam) via email or other online forums." They claim that "spambot flooding" renders a broadcaster's chat service unusable. "Flooding overwhelms the chat service through the sheer volume of spam messages, ultimately disrupting the broadcaster's stream and the viewers' experience," Twitch claimed. **According to the civil action, more than 1,000 broadcaster channels were attacked with 150,000 messages**. "The volume of spam messages on the attacked channel was enormous. **The bots were posting an average of 34 spam messages per minute, while on some channels the rate was 600 messages per minute," the claim says.** "Twitch has received hundreds of individual reports regarding spam messages containing racism, homophobia, sexual harassment, links to shock imagery, false implications of view-botting and soliciting child sex exploitation material." View-botting is manipulating the number of viewers a TwitchTV player appears to have in an effort to get others to click on their live stream.

'Simple service to flood/destroy just simply demolish'. The attacks sparked online anger. Frustrated broadcasters turned to forums where they posted images of screens full of obnoxious comments and images. **In Supreme Court, Twitch claimed its employees spent 300 hours tracing the deluge to a site called chatsurge.net - and Brandan Lukus Apple.** A chatsurge video entitled "How to flood Twitch" - a "simple service to flood, destroy, just simply demolish any TwitchTV chatroom" - can still be found on YouTube. It was posted last April. During a three-minute demonstration, a broadcaster watches despondently as the chatlog beside her explodes with comments saying "you suck." A few days after that video was posted, Supreme Court Justice Maria Morellato issued an order permanently restraining Apple from making or disseminating any products aimed at hurting Twitch.

Apple has not entered a plea in relation to the mischief charge, which has not been proven in court. His next appearance is in February. The tall, heavyset young man had no comment on either the civil action or the criminal accusation this week when a CBC reporter knocked at the door of his Coquitlam home.

His residence sits at the end of a cul de sac, which borders a forest. Apple wore dark grey shorts and a light grey T-shirt, and his chin is lined with sparse facial hair. He appeared surprised after descending the stairs to come to the door, but simply said "no" when asked if had anything he wanted to say. Twitch declined comment on the charge. But in arguments for the civil order, the company claimed the attacks had disrupted service and "caused injury to Twitch's brand, goodwill, reputation and customer relationships."

Jordan Evan Bloom Charged for Selling Billions of Pieces of Personal Data: RCMP 🇨🇦

http://www.huffingtonpost.ca/2018/01/15/jordan-evan-bloom-charged-for-selling-billions-of-pieces-of-personal-data-rcmp_a_23333944/

An Ontario man who allegedly peddled information from an online database containing 1.5 billion usernames and passwords faces several criminal charges. The RCMP accuse Jordan Evan Bloom of Thornhill, Ont., of **selling stolen personal identities through the website Leakedsource.com, which had a total of some three billion pieces of data**. Bloom, 27, is charged with offences including trafficking in identity information, unauthorized use of a computer, mischief with data and possession of property obtained by crime. **He is alleged to have earned about $247,000 by selling the data**. The police operation began in 2016 when the RCMP learned the website in question was being hosted by servers located in Quebec. The RCMP worked with the Dutch National Police and the U.S. Federal Bureau of Investigation on the case.

Canadians Ready to Ditch Passwords for Facial, Fingerprint Recognition: Survey 🇨🇦

https://globalnews.ca/news/3956684/canadians-passwords-facial-fingerprint-recognition-security/

Canadians are ready to forget the many, many passwords they have for online accounts in favour of biometric technology, according to **a new survey by Visa. The credit card company released results of a survey of 1,000 Canadians, which indicated that 69 per cent are interested in using fingerprint recognition over passwords for identification purposes. Canadians were also interested in using other biometrics such as eye scans, and voice or facial recognition**.

They also expressed interest in using the technology as authentication when it comes to making payments because it means no longer having to remember passwords or PINs. Forty-four per cent of respondents also felt biometrics are more secure, while others thought it was the more convenient option. Thomas Keenan, a University of Calgary computer science professor and the author of book *Technocreep*, told Global News that the support for biometrics is not surprising. “People are disgusted with passwords - I guess that’s the best way to put it - and looking for something better,” he said. “Biometrics could be something better.” **Keenan explained that passwords used to be simple, but have gotten increasingly complicated to remember. Respondents in the survey agreed; 32 per cent said they’ve given up online purchases because they couldn’t remember their passwords.**

How secure are biometrics? Keenan noted that passwords have been the cause of major security concerns. They often need to be written down, are susceptible to hacks, and can be stolen in lost phones or laptops. While biometrics aren’t perfect, Keenan says they don’t carry many of those risks. The professor gave the example of one German researcher who created plastic fingers that could fool Apple’s biometric technology for fingerprint recognition. He is usually successful, Keenan noted. But he also added that the same researcher still uses fingerprint recognition because he says it’s “good enough.” “I don’t think people are going to go around making plastic fingers and doing all that work. For most people, it’s just fine.”

Privacy concerns. The survey found that the top concern for Canadians is that biometrics may lead to sensitive information being compromised - about 44 per cent expressed concern that unlike passwords that are stolen, fingerprints can’t be changed. Keenan said that when it comes to privacy concerns, **Canadians just have to trust that companies will be secure and not exploit information.** And he acknowledged that sometimes, companies don’t follow ethical practices. **However, he explained that facial and fingerprint recognition on phones isn’t as intrusive as many people may think**. “When you enroll your fingerprint, it’s not actually grabbing your entire fingerprint,” the professor noted. “What it’s doing is studying your fingerprint, or if it’s your face, it’s studying your face, and taking a sample of it enough so it can tell you apart from other people.” **Keenan said the real concern is how intrusive it may become in the future. “There’s research going on at many companies to look at your face to decide if you’re happy or sad, and the fear is that when they’re looking at your face to identify you, what else might they be doing?”**

Should you start using biometrics? Keenan said that those looking into biometrics should start off testing it out on their personal devices, such as smartphones and tablets. Then, establish trust when you're familiar with the way the system works. **But he noted that biometrics is where technology is going - so those hesitant to try it out may not have the option to opt out soon.** Governments in developed countries are increasingly moving toward using the technology for identification, Keenan said, citing airport security as an example. Some banks in the United States have also started offering facial recognition as an authentication method. (*This survey was conducted by AYTM Market Research on behalf of Visa between Oct. 25-Nov. 1, 2017. It was completed by 1,000 Canadian adults who use at least one credit card, debit card or mobile pay.)*

Pay Centres Overwhelmed as Phoenix Overpayment Deadline Approaches 🇨🇦

http://www.cbc.ca/news/canada/ottawa/phoenix-pay-overpayment-deadline-to-report-1.4482983

[*Continuing to update readers on this story…*] Federal government workers who've been overpaid through the troubled Phoenix pay system are voicing frustration with a plan to report the overpayments in order to avoid costly tax implications. Public Services and Procurement Canada has given public servants until Jan. 19 to declare overpayments so they can be processed by Jan. 31. Under the plan, employees who report by the deadline will only have to pay the net amount they received. Those who don't declare the overpayment on time will have to repay the gross overpayment, including tax and other deducted amounts that they never actually received, which for some could add up to thousands of dollars.

Busy signals frustrate workers. But many of those public servants have complained of busy signals or being put on hold indefinitely when calling the Phoenix pay centre. …Public Services acknowledged the centre is experiencing higher-than-normal call volumes as the deadline approaches and recommends employees fill out an online form instead.

180,000 workers affected by Phoenix. Other public servants complained that deductions were already being taken from their paycheques for overpayments, even if they didn't receive any extra pay or had already paid money back. "I can't get an explanation why they are taking the money or how much they think I owe," Lindsey Welsh wrote in a Facebook message. "I am a single mom so if I had received any extra monies I would definitely notice." **More than half of all federal public servants - about 180,000 workers - have reported being overpaid, underpaid or not paid at all since the Phoenix pay system went live nearly two years ago.**

But those receiving overpayments have been treated as a low priority as the government struggles to ensure employees who are underpaid or not paid get the money they earned. **In some cases, public servants who have moved to jobs in a higher classification have been paid two salaries. Others who have retired continued to receive paycheques after leaving government while some received double severance payments.**

Government lost track of reimbursement, retiree says. Public Services was unable to provide a tally Thursday of the number of public servants who have received overpayments to date, but reports last year indicated the figure was in the tens of thousands by summer. **A report by the auditor general released in November indicated that, as of June 2017, 59,000 employees owed the government a total of $295 million as a result of overpayments. Another 51,000 employees who were underpaid were owed $228 million at that time, the report said.**

Mediator to Help Fix Problems with Nanaimo IHealth Records Project 🇨🇦

http://www.timescolonist.com/news/local/mediator-to-help-fix-problems-with-nanaimo-ihealth-records-project-1.23143541

An independent investigation has found the IHealth project in Nanaimo is severely over budget, has been badly mismanaged by Island Health and should not be rolled out across Vancouver Island until problems are fixed. It does not recommend pulling the plug on the project. Instead, Health Minister Adrian Dix said he will appoint a mediator to help it move forward.

The Ernst and Young report, commissioned by Dix, followed protests by some doctors at Nanaimo Regional General Hospital who were concerned the electronic health system put patient safety at risk. Doctors said the system has resulted in drug dosage errors and other concerns since its introduction as a pilot project at the hospital in March 2016. "I would describe the review as highly critical, even quite devastating, of how the system was implemented here in Nanaimo and has been implemented on Vancouver Island," Dix said. It will cost at least $54.1 million, on top of its initial

$173.5-million budget, to complete the project. “It’s significantly over budget,” Dix said. “Worse than that, of the initial budget, $20 million was completely unfunded.”
The report found IHealth was not properly planned or implemented. Some issues could have been prevented if Island Health had heeded advice from other Canadian health jurisdictions. IHealth was put in place before the hospital was prepared. Local staff weren’t adequately engaged, consulted or trained to use the system. And a climate of distrust at the hospital, with “deeply polarized” stakeholders, made things worse. Although patient safety has been the primary concern raised by staff, the report found only three of 28 “critical” patient-safety events reported since March 2016 were related to the computer system. An expert panel found that some patient-safety events are expected, but that improvements in safety relative to paper systems tend to outweigh any new safety risks introduced. However, the report criticizes Island Health’s investigation of safety concerns and the process for reporting their resolution.
Dix said he would accept and implement nine recommendations from Ernst and Young. The recommendations include fully investigating safety concerns, reviewing the governance structure for IHealth and Island Health more broadly, ensuring readiness and training before future activations, and developing a realistic financial forecast and funding model. Dix said he would appoint a mediator - under whom Island Health will be treated on equal footing with other stakeholders, instead of taking a leadership role, he said. Deputy health minister Stephen Brown will act as “tie breaker” on any disputes. Although the report found less than half of staff and physicians surveyed agreed it would be possible to work collaboratively to make IHealth a success, **Dix said it’s necessary to move forward with the software. Island Health already uses a software system by Cerner, the company that developed IHealth, at facilities across Vancouver Island, he said. And the money already spent on the project is significant. “We have to continue with the IHealth project, but we have to change the way we do business here in Nanaimo,” he said.**
Dr. David Forrest, president of the Nanaimo Medical Staff Association, said he was relieved to see the report validate healthcare workers’ concerns. ….Island Health interim president and CEO Kathy MacNeil said the health authority accepts the report findings and recommendations….

Sask. Health Authority Sends More Private Health Info to Computer Shop, Says Frustrated Owner

http://www.cbc.ca/news/canada/saskatchewan/sask-private-health-information-1.4480337
The Saskatchewan Health Authority has again faxed private medical information about a patient to a North Battleford computer shop, according to the frustrated owner of the business. Darryl Arnold says his company fax machine received a 21-page medical report from the Shellbrook Hospital that was intended for a North Battleford-area doctor. He said he did not read the document, but the cover page included the patient's name. "I feel really bad for [the patient] - because, obviously if they are seeking medical help, the doctor needs the information that is in this medical report," said Arnold.
Business keeps getting health faxes. Arnold says Kelly's Computer Works has received numerous faxes from health authority facilities, dating back to January of last year. He previously received a fax from the non-invasive cardiology unit at St. Paul's Hospital - then part of the Saskatoon Health Region, and since amalgamated into the Saskatchewan Health Authority. In 2017, Arnold contacted Saskatchewan's information and privacy commissioner, Ron Kruzeniski, who urged the health region to start following its own policies when it comes to sending internal faxes. "I find that [the health region's] faxing practices do not follow its internal policy and procedure regarding faxing personal health information," he wrote in a report responding to Arnold's complaint last October.
….. The health authority said in an emailed response Tuesday night that strengthening patient confidentiality practices was a "high priority," and that the incident would be reported to the Office of the Saskatchewan Information and Privacy Commissioner and an investigation would be conducted. Dahl said the investigation will have recommendations for how to reduce or eliminate the possibility that similar incidents will happen, but he doesn't know if the recommendations will apply province-wide….

Internal CSIS Note Details 'Mega Trends' Set to Alter Economy, Society, Security

http://www.timescolonist.com/news/national/internal-csis-note-details-mega-trends-set-to-alter-economy-society-security-1.23144472
From cryptocurrencies, to artificial intelligence, to the rise of millennials, a top-secret document by Canada's spy agency explores the so-called "mega trends" on its radar and details how they will transform the economy, society and security. The evolution of these trends - set to play out over the next

five to 15 years - will unlock new opportunities and new threats, said the recently released document prepared for Michel Coulombe, who was director of the Canadian Security Intelligence Service at the time. The draft discussion paper was created ahead of Coulombe's participation at a November 2016 deputy ministers' committee meeting on national security.

In the briefing, CSIS officials shared their insights on cyber security and privacy, the economy's evolution toward knowledge-based sectors, the arrival of blockchain and cryptocurrencies, artificial intelligence, the emergence of the millennial generation, encryption and the advance of quantum technologies. "Each of these trends bring promise and challenge," said the paper, which was labelled "top secret." "The rate and impact of technological advances and interactions are often misunderstood or underestimated. Organizations - faced with time, money and people constraints - will struggle to make effective planning and investment decisions." It warned that significant and sustained leadership, innovation, partnerships and investments will be necessary to deal with the complexity and accelerated pace of these changes.

A take-home message of the document is that policy-makers must figure out how much they really know about these disruptive technologies, their potential national-security risks and how to ensure Canada stays secure and prosperous. The briefing was obtained by The Canadian Press under the Access to Information Act.

….. The CSIS document also warned that, as the world's knowledge-based sectors evolve, we should expect increasingly fierce competition as states, organizations and individuals target new expertise and intellectual property belonging to others. It called this information, which would mostly exist in electronic format, a "highly valuable commodity" that will need protection from cyber-attacks. [article has more discussion on other points]

FTC, OPC, PCPD Collaborate on Connected-Toy Enforcement 🇨🇦

https://iapp.org/news/a/ftc-settles-first-case-involving-connected-toys/

The Federal Trade Commission has settled its first enforcement action involving the privacy and data security of connected toys. On Monday [Jan8], VTech Electronics and its U.S. subsidiaries agreed to settle allegations that **the company violated the Children's Online Privacy Protection Act, as well as the FTC Act, and pay a $650,000 fine**. "As connected toys become increasingly popular, it's more important than ever that companies let parents know how their kids' data is collected and used and that they take reasonable steps to secure that data," said Acting FTC Chairman Maureen K. Ohlhausen. "Unfortunately, VTech fell short in both of these areas.

The settlement comes after a two-year investigation which found that VTech violated COPPA by collecting "personal information from children without providing direct notice and obtaining their parent's consent, and failing to take reasonable steps to secure the data it collected," according to a FTC statement. The FTC's investigation followed a Dec. 2015 discovery that VTech suffered a data breach exposing the personal information of both children and adults, effectively highlighting the company's poor cybersecurity practices.

In its investigation into the case, the FTC collaborated with the Office of the Privacy Commissioner of Canada, which published its own findings report. In comments provided to The Privacy Advisor, Jacqueline Connor, FTC staff attorney and lead lawyer on the case, said, "As consumers around the world adopt new technologies, they increasingly share personal information with companies that operate globally. Therefore, it is crucial that the FTC cooperates with its foreign partners in enforcing privacy and security laws."

Connor added, "In this instance, the FTC and the Office of the Privacy Commissioner of Canada shared information gathered in their own investigations to facilitate this matter. To assist its international partner, the FTC relied upon the U.S. SAFE WEB Act, which strengthens the FTC's ability to cooperate with foreign counterparts. In addition to authorizing confidential information-sharing, the Act also enhances the FTC's authority to provide investigative assistance to counterparts, and provides mechanisms to strengthen enforcement relationships. The FTC and the OPC are both members of the **Global Privacy Enforcement Network**."

…. In a press call held Monday, FTC Bureau of Consumer Protection Acting Director Tom Pahl explained that **allegations raised against VTech included the company's failure to provide adequate privacy notices to parents that allowed for consent before collecting personal information from children, failure to establish and maintain reasonable security procedures to protect personal information**

once collected, and misrepresenting whether certain registration information submitted by consumers would be encrypted.
In addition to paying a $650,000 fine, the company will be obligated to comply with COPPA requirements, implement a comprehensive data security program and undergo a third party audit every two years. Pahl said considerations such as the company's "degree of culpability, the history of prior conduct, the company's ability to pay, the effect of their ability to pay and continue business" were among considerations in deciding the monetary settlement. Pahl added that the settlement was thought to reflect the seriousness of the obligations… As for the FTC's future enforcement efforts, Pahl said, "Certainly privacy and data security, particularly when it comes to products that deal with children's information, remains a priority for us," adding, "This is an area that deserves a lot of scrutiny and we will continue to look at it."

Pornographic Malware Found in Android Apps for Kids

http://money.cnn.com/2018/01/12/technology/porn-ads-apps-google-android/index.html

Google has removed from its Google Play Store more than 60 gaming apps, many seemingly targeted at kids, that contained malware that showed pornographic ads. **Researchers from security firm Check Point discovered the malware, called AdultSwine, in apps that have been downloaded more than 3 million times, according to a report released Friday. The gaming apps include titles such as Mcqueen Car Racing Game, Subway Banana Run Surf, and Paw Puppy Run Subway Surf.**
An individual or group of hackers created these malicious games under fake publisher names to distribute their malware and make money off the scheme, Check Point researcher Daniel Padon told CNN Tech. Once downloaded, the malicious apps displayed "highly pornographic" pop-up advertisements in a new web page, and attempted to scare users into installing fake security apps. It also intended to get users to buy worthless premium services, the researchers found.
According to Check Point, Google removed the malicious apps hours after they were notified of the issue. "We've removed the apps from Play, disabled the developers' accounts, and will continue to show strong warnings to anyone that has installed them," a Google spokesperson told CNN Tech. "We appreciate Check Point's work to help keep users safe."
One user said in a comment on the Google Play Store that his son saw pornographic content on one of the apps, according to Check Point's findings. **The malware was not found in apps that are a part of Google's "Designed for Families" program. Google staffers manually review apps designed for children. Apps made primarily for kids under 13 must participate in this program, according to the company's website.** Google said the malicious advertisements did not come from its ad network. Despite Google's security precautions, malicious apps can find their way into the Google Play Store. Check Point found 303 malicious apps in the Play Store last year.
Android users should make sure they download apps from known developers and parents of young users are urged to download apps from Google's family program. Padon also suggested checking apps' reviews before downloading. But **some malware authors create fake reviews** to make their apps seem legitimate.

How to Protect Your Personal Data in 3 Simple Ways

https://www.hackread.com/how-to-protect-your-personal-data-in-3-simple-ways/

As the big tech corporations are coming under increased attack from hackers, it can make the domestic users unsure of which way they can turn to best protect themselves against cyber-attack: if the big guns are struggling, how does the average Joe keep his personal data safe? No matter how soon new software is available, new scams arise that have identified and taken advantage of the flaws that the makers were previously unaware of. **Defense against cyber-criminals needs to be multi-layered to ensure that the risk of security breaches is minimized**. Here are 3 ways that you can protect yourself against online attack.
(1) E-mail - You will be aware of the threats that come to you via e-mails. They come in many guises and are usually quite easy to identify – if you know where to look. Check out the sender's e-mail address. Typically, the name displayed will be of the trusted organization, but the e-mail address from which it sent will be quite clearly not them. Never respond to these phishing e-mails, by replying you are confirming to the sender that they have a legitimate e-mail address. **If the e-mail's content is sent from an authentic organization, there will be no spelling mistakes or requests for personal data**. **Never click on a link that the e-mail has provided.** Contact the alleged sender by the details on the genuine website.

An authentic bank, for example, would never request that you input personal details, and even if the e-mails say that they have identified a security breach that you need to clarify, your bank would telephone you or contact you via letter.

(2) Passwords - Your passwords need to be complex. Never choose your date of birth, the name of your child, or another piece of information that could be found in the public domain. **Each app and website that you need to log on to should have a different password**. Remembering all your different passwords can be troublesome, and as it is advised that you don't jot them down, you can use heavily encrypted software to store the passwords. This may feel counterintuitive, but as 81% of business security breaches are due to password weaknesses, it is advisable to use enterprise level security in the domestic sphere. You can find out more about this software by clicking here to read the LastPass review to further understand the benefits available to you. *[note: some frustrated security researchers are suggesting that it is okay to write down passwords if you keep and use them at your home and hide them, but never at work, or carried on you – and only if it will mean better passwords practices – complex and separate]*

(3) Update - Software security updates are regularly distributed by service providers. They are released as new threats and viruses are identified, and **failing to update your desktop or other devices means that you are not protected by the latest security versions of the software**. While you may think that the update is only to fix cosmetic bugs, the reality is that **the updates contain essential security fixes** that have been coded to protect you, the user.

The information that you provide to websites and apps is enough for hackers to exploit you for their benefit. Think about what you sign up for and the information that you are providing. **It is prudent to have a separate e-mail address that you can use for the non-important communications**: newsletters, competitions and the such like. Update your devices as and when requested to, and choose passwords that are complex to make life as hard as possible for the scammers.

Man Charged Over Super Creepy Apple Mac Spyware [FruitFly] That Snooped On Victims Via Webcams

https://www.forbes.com/sites/thomasbrewster/2018/01/10/man-charged-over-super-creepy-apple-mac-fruitfly-malware/#31cea740273b

Earlier this year *Forbes* reported on an especially creepy strain of malware known as FruitFly targeting Apple Macs. At the time, it was unclear just what the spy tool was for, though it appeared to be used for surveilling people's personal Macs, in particular peeping at them through their webcam. Now the U.S. Department of Justice has unveiled an indictment against 28-year-old North Royalton, Ohio, resident **Phillip Durachinsky, who is not only accused of spying on Apple Mac owners via Fruitfly but also of producing child pornography. Prosecutors alleged Durachinsky had been installing spyware on people's PCs for more than 13 years "in order to watch, listen to and obtain personal data from unknowing victims."**

Whilst his malicious tools found their way into individuals' computers, they also infiltrated PCs at companies, schools, a police department and the government, including a body owned by a subsidiary of the U.S. Department of Energy, according to the charges. **FruitFly was capable of stealing files, pilfering passwords, as well as turning on the microphone and the camera. Thousands of PCs were infected, prosecutors said.** Durachinsky would listen in on people's conversations and watch them in secret, whilst taking detailed notes of his alleged snooping, the DoJ said. **In some cases, FruitFly would alert him when the victim was searching for pornography, according to the indictment**. FruitFly didn't only work on MacOS, Durachinsky had developed a Windows version too, the DoJ claimed. "For more than 13 years, Phillip Durachinsky allegedly infected with malware the computers of thousands of Americans and stole their most personal data and communications," said Acting Assistant Attorney General Cronan.

There's little information on the child pornography charges, according to an indictment obtained by *Forbes*. The DoJ claimed that between October 2011 and January 2017, Durachinsky "did use a minor and minors to engage in sexually explicit conduct" to produce "a visual depiction" of such conduct," knowing that it would be transmitted to others. *Forbes* also unearthed a complaint filed against Durachinsky back in January last year, in which **he's accused of hacking into computers at Case Western Reserve University (CWRU), where he had been a student. CWRU had reported more than 100 computers infected to the Cleveland division of the FBI just as 2017 was getting started. The FBI later found the computers had been infected for "several years" and that the same**

malware had infected other universities. *Forbes* attempted to contact Durachinsky's representation listed for that case, but had not received a response at the time of publication. A spokesperson from the Ohio branch of the DoJ said **Durachinsky was arrested in January last year and has been in custody ever since**.

What made FruitFly particularly interesting, when first detailed by security researcher Patrick Wardle, was its ability to infiltrate Apple Macs, which see fewer infections than Windows PCs. Apple had not responded to a request for comment at the time of publication.

Mac malware 'spying on kids'. The indictment against Durachinsky didn't specify whether the Apple Mac strain of FruitFly was used to spy on children, though Wardle told *Forbes* he understood that to be the case. Wardle was also annoyed that Apple didn't take the opportunity to educate Mac users on the threats facing them. "These threats are out there," he said. "Creepy sickos are hacking Macs and spying on kids."

Facebook Warned It Faces Legal Action from 'Revenge Porn' Victims

https://www.theguardian.com/technology/2018/jan/12/facebook-faces-legal-action-from-victims-of-revenge-porn

Facebook is facing a number of lawsuits from victims of "revenge porn", a leading libel lawyer has warned, after a teenager reached a settlement with the social networking site over naked images of her that were posted online. The Belfast-based libel and privacy expert Paul Tweed has also told the Guardian his office was being "deluged" by inquiries from people who claim naked and compromising pictures had been posted on Facebook, Twitter and other sites. Tweed said this was in addition to a "very significant number of cases" his Belfast office was already dealing with in relation to complaints about revenge porn being posted on social networks.

"Because Facebook, Twitter and other social media giants have their European headquarters in Dublin most of these cases will be heard in the Dublin courts. There are quite a number pending and the settlement in the case last week at Belfast high court will undoubtedly have a bearing on them."

Facebook reached a confidential settlement with a 14-year-old girl this week who sued them after a photo of her was posted on a so-called "shame page" on the site. The child's legal team took on the case after her photo appeared several times between November 2014 and January 2016. She alleged misuse of private information, negligence and breaching the Data Protection Act. Her lawyers at McCann and McCann solicitors claimed the settlement had "moved the goalposts" in terms of how social media networks such as Facebook would have to respond to indecent and abusive messages and images being posted on their sites.

"The social networks' presence in Dublin also means they are subject not only to Irish laws but also European privacy legislation, which entails they could be sued anywhere in Europe over this issue of so-called revenge porn," they said. Tweed said Facebook already has an algorithm that has removed naked images, after the site took down the image of the nine-year-old Vietnamese girl Kim Phuc running away from an American napalm attack in 1972. "It was an algorithm that picked up that image and censored it initially and it is obvious that the same algorithm could easily be used to filter out naked pictures of people that are posted for more sinister reasons on Facebook. The network cannot argue it doesn't have the power to filter out these images," he said. The international outrage forced Facebook to reinstate the image on its site.

Tweed said he was unable to reveal further details of the cases pending in the Irish Republic to protect the privacy of his clients. He established his own practice last summer and opened a new office after 39 years as a senior partner in the Johnsons law firm. Part of the reason for opening new premises and recruiting a larger legal team was due to the increase in the number of cases being taken against social media giants, he said.

Police Hand Out Malware-Infected USBs as Prize in Cyber-Security Quiz

https://www.bleepingcomputer.com/news/security/police-hand-out-malware-infected-usbs-as-prize-in-cyber-security-quiz/

Taiwanese police have handed out malware-infected USB thumb drives to the winners of a cyber-security quiz at a data security expo hosted in December last year by the country's Presidential Office. **The Criminal Investigation Bureau said last week that 54 of the 250 8GB thumb drives it handed out to winners contained malware. The incident came to light after quiz winners reported that antivirus software showed alerts when users inserted the thumb drive into computers.** The USB sticks were handed out on December 11, but police stop distributing them the next day after user complaints. The Bureau said it recovered 20 of the 54 infected USBs.

USB thumb drives infected by third-party contractor. An investigation revealed the USB thumb drives came from a third-party contractor. Police said one of the contractor's employees tested some USB thumb drives to verify that their storage capacity was 8GB, as intended. The computer to which the employee connected the thumb drives was infected with malware, which then spread to the USB sticks. The malware was a mundane and nondescript strain named XtbSeDuA.exe, which was tied to a cyber-fraud ring Europol shut down in 2015. The malware was only designed to work on 32-bit systems. It collected data from infected devices and sent it to a web server located in Poland. Because the server was previously shut down, no actual harm came to the people who infected themselves via the USB thumb drives.

Police apologizes for the blunder. Albeit the USB thumb drives were manufactured in China, the Criminal Investigation Bureau ruled out the possibility of this being a cyber-espionage operation carried out by Chinese government agencies. The Bureau apologized to the Presidential Office, members of the government, and quiz participants, according to Taipei Times, a local newspaper who broke the story last week.

And Now, This:

Five Ways Quantum Computing will Change Cybersecurity Forever

https://www.raconteur.net/technology/five-ways-quantum-computing-will-change-cybersecurity-forever

A new generation of quantum computing has the potential to transform cybersecurity. **Still years away from the mainstream, quantum power is nevertheless a reality, a certainty and an inevitability.** Traditional old-fashioned digital computers run on data that is encoded according to the binary system. In binary, the state of any single bit can only be 0 or 1. The options are quite literally binary. Any single computing bit can only reside in one of two positions. Now emerging as the next generation of computing, quantum computers run on data that comes in the shape of qubits or quantum bits. Quantum goes beyond binary by virtue of a qubit's ability to reside in more than one of two positions. A qubit can represent a quantum state made up of two or more values simultaneously, called a superposition. A qubit's superposition can also be differentiated depending upon the context in which it is viewed, so in basic terms we get more computing power in the same space.

But quantum states are fragile and quantum errors are notoriously difficult to measure, so we need to treat this new power with respect. How then could this new thrust of computing strength give us new tiers of power to analyse IT systems at a more granular level for security vulnerabilities and protect us through more complex layers of quantum cryptography? [The remainder of the article has been edited a little – go to the link if you want to read the full text.]

01 SPEED - Quantum computing is a game-changing technology for cybersecurity due to the inherent speed boost it offers to solve complex mathematical problems. …"Traditional cryptography relies on the fact that factoring large prime numbers is mathematically complex and hackers attempting to brute-force an answer need a long time. For quantum computers, this kind of factorisation is where they excel, potentially reducing the time to solve problems from billions of years to a matter of seconds. We can now use that power to build more complex protection layers," says Mr Ferguson. But could quantum computing also arm the hackers? "Obviously yes," he says. "What we need to remember is that the majority of attacks in today's threat landscape target the user in one way or another and social engineering plays as large a part, if not larger, than technical expertise. As long as a human can be persuaded to part with a secret in inappropriate circumstances, all the cryptography in the world will not help, quantum or not."

02 SECURITY - Perhaps the most compelling near-term impact of quantum is the role of security "distribution functions" that use quantum effects, providing us with a powerful mechanism for sharing cryptographic keys between remote parties with a high degree of implicit security. According to IBM computer scientist Leigh Chase, we should also look more generally at the types of data transformation operations we can perform in quantum computers to exploit effects that are not present in the classical world of IT. Effects such as superposition and entanglement offer information-processing benefits, many of which can be meaningfully applied to cryptography, such as improved random number generation…

03 RESPONSIBILITY - Although the money is more generally on quantum power keeping us safer, we should constantly remind ourselves that the responsibility for safe use is by no means guaranteed. Senior threat analyst at FireEye Parnian Najafi agrees that quantum computers running what is known as

Shor's algorithm pose some risks to current cryptography. "Some encryption algorithms are thought to be unbreakable, except by brute-force attacks. Although brute-force attacks may be hard for classical computers, they would be easy for quantum computers making them susceptible to such attacks," says Ms Najafi. But she agrees it is unlikely that hacktivists and cybercriminals could afford quantum computers in the foreseeable future. However, nation states do have the ability to afford and run them…

04 SAFETY - So is a quantum apocalypse on the horizon and will cryptocurrencies be a key target? As a security company FireEye's research highlights there are several efforts currently underway to make cryptocurrency more secure, including the quantum-resistant ledger. It would appear then that as fast as we are building quantum power, we are also working to secure against its misuse. …"Such great computing power, however, will present a huge challenge for cryptography in the future as cybercriminals will be able to target organisations with highly complex quantum attacks. To pre-empt this, security specialists are currently developing quantum-resistant algorithms, but we are yet to see how quantum computing will really revolutionise cryptography in the future."

05 RESISTANCE - Human vulnerabilities notwithstanding, could we really use quantum computing to build an unbreakable computer truly resistant to hacking? Director of product strategy at Gemalto Joe Pindar is upbeat. "What is special about random numbers from quantum computing, and why their early prototypes are being used by Swiss banks and governments, is they can be used to create a 'one time pad'. This is a special kind of encryption key that is essentially unbreakable. Interestingly, one time pads were first used in World War One and are made exceptionally secure by being used only once, for a single message, so codebreaking techniques simply don't work," he says.

Mr Pindar offers some reassurance on the potential misuse of quantum computing. He says that while it will change most of the encryption algorithms commonly used on the internet, it is not true that quantum will break all encryption. "The encryption systems that are used to secure data stored in database records and archives, such as legal documents, use a different technique which quantum computing has been unable to break, so far," he adds.

Feel free to forward the Digest to others that might be interested.
Click Unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity 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:
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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

****