Security News Digest

April 24, 2018

April is 'Digital Spring Cleaning' Month

Take our monthly quiz and test your knowledge

On this day in history (April 24th)

1916 — Polar explorer, Ernest Shackleton, and five men of the Imperial Trans-Antarctic Expedition, launch a lifeboat from uninhabited Elephant Island in the Southern Ocean to organize a rescue for the ice-trapped ship Endurance".

This week's stories:

Victoria man loses $11,000 in bitcoin-ATM tax scam

http://www.timescolonist.com/news/local/victoria-man-loses-11-000-in-bitcoin-atm-tax-scam-1.23245878

A Victoria man was bilked out of $11,000 after fraudsters posing as the tax man directed him to a bitcoin ATM and persuaded him to transfer money to them via cryptocurrency. A quick-thinking bank teller prevented the man from losing even more money, Victoria police say. The man was contacted on March 28th by scammers pretending to be from the Canada Revenue Agency, said Victoria police spokesman Bowen Osoko. They told the man he owed thousands of dollars and that he could face arrest if he did not settle up. The fraudsters told the man to withdraw a large amount of cash and then go to a bitcoin ATM at Hecklers Bar and Grill on Gorge Road East.

The scammers likely sent the man a barcode via email or text, and told him to deposit the cash into the machine and send the transaction using the barcode, said Keirnan Wright, CEO of HoneyBadger Inc., the company that owns and operates the machine. The transaction limit is $10,000 so the man made two transactions. Within minutes, he had lost $11,000.

The man then received a call from a different fraudster claiming to be a Victoria police officer. This person told the victim to go to a bank branch and wire additional funds. He demanded to stay on the phone with the man as he made the transaction. A teller at the bank recognized the ruse and intervened. When the teller confronted the caller, the line went dead. The man immediately reported the fraud to Victoria police and HoneyBadger, but it's unlikely he will be able to recoup his losses. Because cryptocurrency transfers are peer-to-peer with no bank as the middleman, they are irreversible, Wright said. The machines do not accept debit or credit cards, only cash.
HoneyBadger's website features an orange alert that reads "SCAM ALERT: Got a call from CRA/police/other and asked to send Bitcoin? It is a scam! Do not send bitcoin to anyone over the

phone!" A similar scam alert appears on the home screen of the machines. Before a transaction is finalized, a pop-up message asks the user "Do you control this [barcode] address or are you sending to someone else?" If you select "someone else" a warning pops up about a possible scam and the transaction is cancelled. Wright said it's likely the man was so panicked he flew by these safety measures.

Six weeks ago, in response to an increase in fraud cases, HoneyBadger programmed its 47 cryptocurrency machines across Canada to include a four-hour delay between the time the transaction is sent and received, Wright said. This allows the company to intervene if the sender realizes they've been scammed. In this case, more than four hours passed before the man contacted HoneyBadger, Wright said. "We're trying to find a way to stop these scammers," he said, adding that the company hears of about three to four scams a week across the country. "It's one of the most disheartening things you can experience when someone calls you on the phone and they've just had their life savings or their child's tuition fund disappear."

Brad MacDougall, the manager at Hecklers, said he was working that night but during the 35-cent wing night rush, he didn't notice someone using the bitcoin ATM. MacDougall said the machine is used daily and being a bitcoin holder himself, he often strikes up conversations with other bitcoin users. MacDougall was gutted to hear that someone had lost such a large amount of money.

Bitcoin is a digital currency with encryption that makes it difficult to track. That feature has made it a popular currency for organized crime, money launderers and fraudsters. However, it's also been employed as a quick and easy way to transfer money overseas and as an investment tool for speculators who can withstand the rollercoaster valuation. Bitcoin saw a meteoric rise in 2017, with its value increasing 1,600 per cent within the calendar year. As of Friday, one bitcoin is worth $8,840 CDN. Compare that to $426.85 CDN in December 2014, when the Times Colonist reported on the installation of Victoria's first bitcoin ATM at Hemp & Company downtown. Since then, more have popped up, with about five in the city, according to the website Coin ATM Radar.

Victoria police and other police departments have been warning people about the Canada Revenue Agency scam for years. In other cases, fraudsters ask for iTunes cards, gift cards and cash-backed credit cards. Victoria police offered tips to people to avoid being scammed in the Canada Revenue Agency fraud:

• The Canada Revenue Agency rarely, if ever, telephones. The CRA typically contacts people by mail. The agency does not take payment by bitcoin.
• Often, the fraudster will use aggressive language and actions and make threats that victims will lose their homes, businesses, and reputations, and place themselves and their families at risk of imprisonment.
• They will keep the victim on the phone for hours or repeatedly call. They will refuse to let the victim off the phone.

Anyone who believes they have been contacted by a CRA scammer should hang up the phone and talk to a loved one, a friend, or call their local police non-emergency line.

Sears, Delta Air Lines Say Customers' Payment Info May Have Been Exposed

https://www.huffingtonpost.com/entry/sears-delta-airlines-data-hack_us_5ac5bcb6e4b09ef3b243866e

(Reuters) - Department store chain Sears Holding Corp and Delta Air Lines Inc said on Wednesday [April 4] some of their customer payment information may have been exposed in a cybersecurity breach at software service provider [24]7.ai. Sears said it was notified of the incident in mid-March and the incident led to **unauthorized access to the credit card information of under 100,000 of its customers**.
Technology firm [24]7.ai, which provides online support services for Delta, Sears and Kmart among other companies, found that a cybersecurity incident affected online customer payment information of its clients, it said. The incident happened on or after Sept. 26, 2017 and was found and resolved on Oct. 12, the company said.
Personal details related to passport, government identification, security and SkyMiles information were not impacted, Delta said. The No. 2 U.S. carrier said while a small subset of its customers would have

had their information exposed, it cannot be said with certainty if their information was accessed and compromised. Sears said its stores were not compromised and their internal systems were not accessed in the breach. There was no impact on the information of customers using a Sears-branded credit card, the retailer said.

MyFitnessPal and Saks Data Breaches and the Facebook Fiasco

http://itincanadaonline.ca/index.php/security/2388-myfitnesspal-and-saks-data-breaches-and-the-facebook-fiasco

Authored by Marcello Sukhdeo on 04/09/2018

We have been hit by a wave of data breaches of recent. Should we keep trusting companies with our personal data? And the Facebook fiasco, it's not about security, it's a privacy breach that could spell the doom of social media giant.

Saks data breach:
A few days ago, three Canadian locations of department store Saks, were exposed to the data breach. This was revealed by Saks parent company, Hudson's Bay. Three Canadian Saks locations, all in Ontario, were exposed to the breach:

- Sherway Gardens in Toronto
- Bramalea City Centre in Brampton
- Pickering Town Centre

Hudson Bay itself, at the time of recording this podcast, hasn't said whether any of its Canadian locations were affected. It says the investigation is ongoing, but there's no indication the breach affected the company's digital platforms or Hudson's Bay and Home Outfitters stores. The company is asking clients to review their account statements to see if there have been activity or transactions they don't recognize and that they will notify customers affected by the breach as quickly as possible and will offer free identity protection services once they learn more about the breach.

MyFitnessPal breach:
There has been another massive data breach; **over 150 million My Fitness Pal accounts were compromised**. Under Armour, the company that owns MyFitnessPal, quickly sent out notifications to its users and once the breach was discovered, so they deserve some credit for how they responded unlike the other examples we have seen over the last few years and recently. In addition to notifying all MyFitnessPal users, the company has provided information about how users can protect their data, and asking that all users to change their passwords. They are also working with law enforcement to investigate and monitor for suspicious activity, and exploring enhancements to help detect and prevent similar unauthorized access in the future.

Facebook:
Mark Zuckerberg has responded to the current backlash that Facebook is getting regarding the way data collected by Facebook was used. The shortened version of what he said, was, "We have a responsibility to protect your data, and if we can't, then, we don't deserve to serve you. That is not right. That's not the issue here. **The Cambridge Analytica scandal is not about a failure to protect users' data; it is a failure to protect the privacy of users' data**. There is a difference there. So, let me repeat, is not about a failure to protect users' data; it is a failure to protect the privacy of users' data.

Amazon will now deliver to your car – but you might pay for it in privacy

https://www.washingtonpost.com/news/business/wp/2018/04/24/amazon-will-now-deliver-to-your-car-but-you-might-pay-for-it-in-privacy/?noredirect=on&utm_term=.f0d639e973c1

First came in-home delivery. Now Amazon is offering to drop off packages straight to the trunk of your parked car. The online giant on Tuesday announced that delivery workers will now be able to place packages in certain vehicles parked at homes, offices and other publicly accessible areas. The service is available to Prime members in 37 cities, including Washington and Seattle, who drive Chevrolet, Buick, GMC and Cadillac cars with an active OnStar account, as well as Volvos with an active Volvo On Call

account. The program is the latest effort by the online behemoth to make it easier for customers to receive online orders. Package theft has long been a persistent problem for online shoppers, and Amazon says in-car delivery is one way to combat the problem. **But privacy and legal experts say in-car delivery raises a number of concerns about consumer data, and the ways Amazon can use that information to draw conclusions about shoppers and their habits. And like with in-home delivery, shoppers may be concerned about letting a stranger into their vehicle.**

"Amazon has a voracious appetite for people's information, and this is one more example of its breathless rush to grab every piece of data and turn it into new forms of revenue," said Jeffrey Chester, executive director of the Center for Digital Democracy, a Washington non-profit group. In November, the company launched Amazon Key, a service that relies on a home-security camera and smart lock to allow couriers into shoppers' homes to deliver packages. Rival Walmart last year announced a similar program in which delivery workers could bring groceries into shoppers' kitchens and unload them into their refrigerators, even if nobody is home. "Amazon's tentacles are everywhere," said Chester. "What kind of car do you drive? Where is it parked? What do you have in the back seat? And in which ways will Amazon use that data to market products to you, especially now that they're getting into ancillary products like life insurance and health insurance?" (An Amazon spokeswoman says the company does not take photos of the car, and that Amazon Key only obtains a customer's vehicle information on the day of delivery.)

This is how it works: Prime members with the Amazon Key app can link their car to their accounts and select "in-car" delivery during checkout. On delivery day, Amazon gives customers a 4-hour delivery window and directs couriers to the parked car, which is unlocked following an encrypted authentication process. The car is relocked after delivery, and consumers receive real-time updates on their phones. The new delivery service to cars gives customers the "same peace of mind" as in-home delivery with Amazon Key, Peter Larsen, Amazon's vice president of delivery technology, said in a statement. The service comes as smart cities and connected cars become more commonplace around the country. After all, some experts say, many drivers now pay parking meters using an app on their phones, and rely on navigational services that know their location at any given time. **"If you trust Amazon with your data, as many people do, then delivery to the trunk of your car is a safe way to getting your package, and perhaps safer than in-home delivery," said Albert Gidari, director of privacy at the Center for Internet & Society at Stanford Law School. "This is another example of trading off privacy and security for convenience."**

Brainjacking – a new cyber-security threat

http://www.ox.ac.uk/research/brainjacking-%E2%80%93-new-cyber-security-threat

We live in an interconnected age where wirelessly controlled computing devices make almost every aspect of our lives easier, but they also make us vulnerable to cyber-security attacks. Today, nearly everything can be hacked, from cars to lightbulbs. **But perhaps the most concerning threat is the one posed by implanted medical devices**. Experts have demonstrated the ease with which security on pacemakers and insulin pumps can be breached, potentially resulting in lethal consequences.

In a recent paper that I *[Laura Pycroft, University of Oxford*] and several of my colleagues at Oxford Functional Neurosurgery wrote, we discussed a new frontier of security threat: brain implants. Unauthorized control of brain implants, or "brainjacking", has been discussed in science fiction for decades but with advances in implant technology it is now starting to become possible.

Deep brain stimulation:
The most common type of brain implant is the deep brain stimulation (DBS) system. It consists of implanted electrodes positioned deep inside the brain connected to wires running under the skin, which carry signals from an implanted stimulator. The stimulator consists of a battery, a small processor, and a wireless communication antenna that allows doctors to program it. In essence, it functions much like a cardiac pacemaker, with the main distinction being that it directly interfaces with the brain.

DBS is a fantastic tool for treating a wide range of disorders. It is most widely used to treat Parkinson's disease, often with dramatic results, but it is also used to treat dystonia (muscle spasms), essential tremor and severe chronic pain. It is also being trialed for conditions such as depression and Tourette's

syndrome. Targeting different brain regions with different stimulation parameters gives neurosurgeons increasingly precise control over the human brain, allowing them to alleviate distressing symptoms. **However, this precise control of the brain, coupled with the wireless control of stimulators, also opens an opportunity for malicious attackers to go beyond the more straightforward harms that could come with controlling insulin pumps or cardiac implants, into a realm of deeply troubling attacks**.

Remote control:
Examples of possible attacks include altering stimulation settings so that patients with chronic pain are caused even greater pain than they would experience without stimulation. Or a Parkinson's patient could have their ability to move inhibited. A sophisticated attacker could potentially even induce behavioural changes such as hypersexuality or pathological gambling, or even exert a limited form of control over the patient's behaviour by stimulating parts of the brain involved with reward learning in order to reinforce certain actions. Although these hacks would be difficult to achieve as they would require a high level of technological competence and the ability to monitor the victim, a sufficiently determined attacker could manage it.

There are proposed solutions to making implants more resistant to cyber-attacks, but makers of these devices are in a difficult position when trying to implement security features. There's a trade off between designing a system with perfect security and a system that is actually usable in the real world. Implants are heavily constrained by physical size and battery capacity, making many designs unfeasible. These devices must be easily accessible to medical staff in an emergency, meaning that some form of "back-door" control is almost a necessity. New and exciting features, such as being able to control implants using a smartphone or over the internet, have to be balanced against the increased risk that such features can provide.

Brain implants are becoming more common. As they get approved for treating more diseases, become cheaper, and get more features, increasing numbers of patients will be implanted with them. This is a good thing overall but, just as a more complex and interconnected internet resulted in greater cyber-security risks, more advanced and widespread brain implants will pose tempting targets to criminals. Consider what a terrorist could do with access to a politician's mind or how coercive blackmail would be if someone could alter how you act and think. These are scenarios that are unlikely to remain purely in the realm of science fiction for much longer.

It's important to note that there's no evidence to suggest that any of these implants has been subjected to such a cyber-attack in the real world, nor that patients with them currently implanted should be afraid. Still, this is an issue that device makers, regulators, scientists, engineers and clinicians all need to consider before they become a reality. The future of neurological implants is bright, but even a single high-profile incident could irreparably damage public confidence in the safety of these devices, so the risk of brainjacking should be taken seriously before it's too late.

Twitter improves user data policy ahead of new European privacy laws

https://www.reuters.com/article/us-twitter-privacy/twitter-improves-user-data-policy-ahead-of-new-european-privacy-laws-idUSKBN1HV24N

(Reuters) - Twitter Inc said on Tuesday it is updating its privacy policy to allow users to view information they share with the microblogging service and show how it's being used, ahead of new regulatory guidelines on European data privacy laws. Tech companies are under intense scrutiny about how they protect customer data after Facebook Inc was embroiled in a huge scandal where millions of users' data were improperly accessed by a political consultancy.

The European Union's General Data Protection Regulation (GDPR) goes into effect May 25 and is the biggest shake-up of privacy rules since the birth of the internet. Twitter's privacy update coincides with GDPR's rules. The changes are meant to make the privacy policy visually clear and easy to use, Twitter's Data Protection Officer Damien Kieran wrote in a blog post.
Twitter said it is expanding and revising the privacy policy content to make some legalistic or technical language as clear as possible. "We think it's absolutely essential that you know exactly what we mean when we refer to location data or data from advertising partners," it said.

Russian router spies: what you can do to protect your home internet

https://www.smh.com.au/technology/russian-router-spies-what-you-can-do-to-protect-your-home-internet-20180420-p4zaq0.html

Some troubling news was issued this week, with the Australian, US and British governments issuing joint warnings about alleged Russian state-sponsored actors maliciously targeting routers and modems around the world, including in Australia. In a press conference about the activity on Tuesday, Defence Minister Marise Payne said the Australian Cyber Security Centre believed potentially 400 Australian companies were targeted. The US said targets included "primarily government and private-sector organisations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors".

The warnings serve as a reminder that often-neglected routers — those devices that glue computer networks together and also often connect them to the internet as well— can be a key, weak entry point into the home and business networks of millions of Australians, not just by state-sponsored actors, but by hackers looking to take over your home network. "Commercially available routers were used as a point of entry, demonstrating that **every connected device is vulnerable to malicious activity**," Cyber Security Minister Angus Taylor said. "Australian businesses and individuals are constantly targeted by malicious state and non-state actors, and we must maintain rigorous cyber security practices." But what rigorous practises are those? And what can you do to protect yourself, especially given that it isn't only Russia allegedly targeting routers, but also the US and undoubtedly other countries' agencies as well?

We click a button automatically presented to us to update the security of our computers and smartphones on what feels like an almost weekly basis. Automatic updates prompt us to install patches in anti-virus and firewall software or our computer's operating system, securing us all of the time. On hearing upon the Russian news, I took a look at my router and found it too needed updating. While we may prolong them a couple of days to prevent the frustrating task of closing down and saving all of the information we have open in various apps, we get there eventually. But when was the last time you logged into your home's router or modem (be it a Wi-Fi or hard-wired one) to check whether it needed updating? My bet is never, for the majority of the population. If you haven't done so in the past six months, it's probably time to do it now, and to do it regularly. Because it's likely that dozens of security flaws have been found since you first purchased it and, if you're lucky, your router's manufacturer has released an update. **One of the best things you can do in addition to updating your router is disabling access to its management interface from the outside world. This means not allowing anyone from outside your home network to touch its settings. The other thing you can do is change the default password. Too often, router manufacturers don't prompt users to change these settings and it leads to circumstances like the one we have today, where malicious third-party actors gain entry.**

With the devices often hidden away in cupboards gathering dust, router manufacturers could and should do more to protect consumers and small businesses. It's my firm view that they should force passwords to be changed on setup, and implement automatic updates that prompt you to install when there is a new one available. Given the only time people log into their router is when there is a problem, it's about time router and other equipment manufacturers realise their responsibility to keep us safe and secure. Troy Hunt, computer security expert and creator of the website haveibeenpwned.com —which allows you to check if any of your online accounts have been compromised by a data breach — agrees. "We've seen vulnerabilities in consumer-grade routers many times in the past, often resulting in traffic being redirected to malicious websites," Mr. Hunt says. "We need to acknowledge that like all software, the code running in these devices can have bugs and that means we need a robust means of patching it. Especially for consumers, this must be automated; anything that requires human intervention will result in patches not being applied."

And now for a feel good story:

Elderly Dog Stays with Lost 3-Year-old Through the Night Before Leading Rescuers Right to Her

https://www.goodnewsnetwork.org/elderly-dog-stays-with-lost-3-year-old-through-the-night-before-leading-rescuers-right-to-her/

You might not expect much grit out of a 17-year-old dog who is deaf and partially blind, but Max has just proven that his disabilities are not going to keep him from being a hero. The courageous canine spent 15 hours in the harsh, rainy Australian bushland alongside a 3-year-old girl who had wandered away from home earlier this weekend.

The little girl named Aurora first went missing on Friday afternoon. The next day, over 100 police and emergency response members were searching the family's rural property in hopes of finding the youngster. Her grandmother, Leisa Bennett was joining the search efforts on Saturday when she heard the sound of Aurora's crying coming from the top of the mountain. As she moved closer to the sound, Max suddenly appeared out of the bush and led Leisa straight to where Aurora was stranded – and the reunion with her family was an emotional one. "I think [Aurora] was a bit overwhelmed by the tears and the howling, but I explained to her how happy those tears were," she said. "It could have gone any of 100 ways, but she's here, she's alive, she's well and it's a great outcome for our family.

The 3-year-old was located just 1.2 miles away from her family's house with minor cuts and scrapes. "The area around the house is quite mountainous and is very inhospitable terrain to go walking in, so she'd traveled quite a distance with her dog that was quite loyal to her," SES area controller Ian Phipps told ABC.net.au. "With the weather last night it's quite lucky she is well because it was cold, it was cold and raining," he added.

While it is pretty safe to assume that Max the senior dog was rewarded with a bone for his heroic efforts, he was also named an honorary Queensland police dog for his bravery.