BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
February 27, 2018

March is Fraud Awareness Month
Take our quiz and test your knowledge

Wednesday, February 28 is Anti-bullying Day in Canada - also called Pink Shirt Day - and this year the focus is on Cyber-bullying! https://www.pinkshirtday.ca/

In today's digital world, it can be impossible to escape online bullying, whether it takes the shape of harassment, spreading rumours, sharing embarrassing information or threats. This year, Pink Shirt Day is encouraging others to combat cyberbullying by thinking twice before posting something negative, and instead using the internet to spread kindness - because we know that Nice Needs No Filter!
https://nobullying.com/anti-bullying-day-in-canada/

This week's stories:

- **Worry About Yourself When it Comes to Cybersecurity, Says Federal Security Official** 🇨🇦
- **Online Romance Scams: A BBB Study on "How Scammers Use Impersonation, Blackmail, and Trickery to Steal from Unsuspecting Daters"** 🇨🇦
- **Games Technology More than Just Perfect Timing** 🇨🇦
- **Unsecured Amazon S3 Buckets are Prime Cloud Target for Ransomware Attacks**
- **Visa: EMV Cards Cut Down Counterfeit Card Fraud in the US by 70%**
- **Important Email Likely to be Missed in Flood That's About to Hit Your Inbox**

Worry About Yourself When it Comes to Cybersecurity, Says Federal Security Official 🇨🇦

https://globalnews.ca/news/3271574/worry-about-yourself-not-the-government-when-it-comes-to-cybersecurity-cse/

Russian hackers interfered with the U.S. presidential election, and Prime Minister Justin Trudeau has tasked a cabinet minister with ensuring nothing similar happens in Canada – but **it's not governments who should be most concerned about security online, it's individuals**, says Scott Jones, who is tasked with defending the federal government's networks. "When you look at cybercrime, it's the huge impact that's going to hit you and me," said Jones, the assistant deputy minister at the Communications Security Establishment. If the public's trust in the cyber world is damaged enough, Jones said, society will feel a desire to revert to behaviours predating the online world. "If that undermines our confidence, then we move back to bricks-and-mortar shopping and a paper-based bureaucracy," he said. "I don't think that's going to work." In essence, he said, while the security of the government's information is pivotal, it's not the only thing with which cybersecurity experts are concerning themselves.

"It's about everything," Jones said. The security considerations individuals ought to take mirror those at the enterprise and government levels, Jones said in an interview on The West Block.

For example, the CSE has a "Top 10 Security Actions" list it published to help protect government information. "Those are things we can apply all the way from individual persons, citizens in the country, up to the largest enterprises like the government," Jones said. "Those are [actions] you can take that actually make you a little bit safer online." Often, a person might connect networks or opt to skip a sign-in because it's simpler or faster. "When you have the option of weakening security to make it easier, think about that," he said.

Other tips Jones offered include uninstalling software no longer in use, updating software and ensuring operating systems are up to date. On the national scale, CSE is tasked with supporting Democratic Institutions Minister Karina Gould in her new mandate to help defend the Canadian political system against cyber threats and hackers.

Jones said his role will helping shed light on how the government can maintain the integrity of the vote and assure Canadian elections continue to be open, transparent and free of interference. While acknowledging there are always vulnerabilities online, Jones said Canada is "very robust" in terms of the democratic process. In terms of the big question – could what happened in the U.S. election happen in Canada? – Jones demurred. "Well, it's a different environment," he said. "Cyber is a good means to get information that you could use to shape opinion, to change people's minds. I think cyber is just a new means of doing something that's existed a long time. Every day, the Communications Security Establishment blocks more than 100 million– some days more than one billion – malicious cyber "actions," Jones said.

An "action" is not necessarily an attack, he said; an action is usually someone looking for vulnerabilities in the system, trying to poke holes and probing to see where any weaknesses might be. Those daily occurrences come from everywhere – from states to "enthusiasts," Jones said. At the same time, however, CSE looks for anything within the federal cyber system capable of being exploited, such as software vulnerabilities – anything that could allow a state or individual to "open that door and get into our systems," he said. So while 100 million or even a billion potential attacks might seem like an enormous number, Jones said the threat only becomes big if he and his colleagues stop adapting.

"We have to be investing and paying attention to this because, as technology grows and becomes more pervasive in our lives, we're starting to see that everything has some sort of cyber element to it," he said.

"If we choose to ignore it and just continue to adopt technology and not think about how to secure it, and how to protect ourselves, it will become a really big problem."

Online Romance Scams: A BBB Study on "How Scammers Use Impersonation, Blackmail, and Trickery to Steal from Unsuspecting Daters" 🇨🇦

https://www.bbb.org/en/us/article/news-releases/17057-online-romance-scams-a-bbb-study-on-how-scammers-use-impersonation-blackmail-and-trickery-to-steal-from-unsuspecting-daters

Romance scams are different from other scams. They prey on lonely people looking to connect with someone, and can often take months to develop to the point where money changes hands. The emotional harm to the victim can be even more painful than the monetary loss. The spread of online dating sites and apps has made this fraud even easier to commit. **Victims in the US and Canada have reported losing nearly $1 billion over the last three years, and BBB estimates there may be more than a million victims in the U.S. alone. Because most people do not file complaints about romance scams with BBB or law enforcement, this may just be the tip of the iceberg.** BBB's study, "Online Romance Scams: How Scammers Use Impersonation, Blackmail, and Trickery to Steal from Unsuspecting Daters" looks at how these scams work, who the scammers are, and what is being done to combat them.

Anatomy of a Romance Scam - Experts identify several distinct stages of the scam:

Contacting victims - Romance scammers use dating websites, apps, Facebook, and other social media. Many use stolen credit cards to join the sites and post fake profiles. They meet victims, interact with them, and quickly try to get them to move to a different form communication such as email or texting. This way, if the dating site identifies the scammer as being bogus and shuts them down, they are already in contact with their victims elsewhere. The scammers will often make fake Facebook pages for their aliases to help bolster their fake identity

Grooming - This is when the fraudster learns about the victim's life and builds trust. This stage can go on for months. It may include daily texts or messages. Some scammers even send flowers and small gifts. This is also when scammers may request small favors. This can help them test how open a victim ultimately may be to helping when an "emergency" pops up and the scam kicks into high gear. The grooming process also focuses on isolating victims from their friends and families so they don't have help when making decisions. The scammers will convince victims that their friends and families have questionable motives to criticize the scammer.

The sting - The scammer will finally ask for money; usually for an emergency, business problem, or plane ticket to finally meet. If the victim sends money, the scammer will find ways to keep asking for more. These scams can also be dangerous: victims have unknowingly been pulled in to money laundering or drug trafficking and, in a few cases, even convinced to fly overseas to meet their love interest only to be kidnapped and held for ransom.

The fraud continues - Even if targets realize they have been victims of a scam, the fraud may continue with a new scam pretending to help them get their money back. A fake law enforcement official may reach out to say the scammer has been caught and the victims can get their money – if they spend several thousand dollars in fees. The original scammer will also sometimes reach out and admit that the "relationship" started as a scam but then claim they actually fell in love. And the cycle continues. BBB's study gives much more detailed information on where the scams originate, how the scammers trick their victims (including by posing as military personnel), and how they get their money. It also details what we know about the victims, why they fall for the scams, and how they can be pulled into other scams. The research shows that all types of people – male, female, young, old, straight, gay – can be victims of romance scams.

Games Technology More than Just Perfect Timing 🇨🇦

https://www.thestar.com/sports/olympics/2018/02/13/games-technology-more-than-just-perfect-timing.html

The official timekeeper of the Olympics has expanded its responsibilities to capture all kinds of data for athletes, coaches and viewers. We've come a long way since the stopwatch.

When Ted-Jan Bloemen crossed the finish line in the pairing that would ultimately net him an Olympic silver medal, no one could actually see that he had won that 5,000-metre long-track race. The difference between the Canadian and Norwegian speed skater beside him was far too close for that. It took advanced photo-finish technology, which captures 10,000 digital images per second, to determine that the tip of Bloemen's skate blade crossed the finish line two one-thousands of a second ahead.

The primary job of a timekeeper at the Olympics is to determine the results in events, some of which are now so close that there would be no way to fairly pick a podium without all the gear that arrived here in massive shipping containers. But Omega, the Olympic timekeeper at the Winter Games since 1936, has moved well beyond timing and scoring events. Every bit of new technology at these 2018 Games is about enhancing the experience for television audiences with graphic displays and producing performance-based data for athletes, coaches and analysts. "In every Games we release some new technology but, in this Games, the focus was on positioning and sensor devices to give the spectators different information," Pascal Rossier, Omega's head of sports operations, said outside the ski jumping hill. "It's enhancing the TV spectator experience."

The Olympic hockey players have motion sensors attached to the backs of their jerseys to capture live in-game data, which can, among other things, show how fast each player is moving, where they've been and their position on the ice relative to the other players.

In big air — the single-trick snowboarding event that make its Olympic debut next week — motion sensors by the athletes' feet will record their speed and height and distance. That data can be used, for example, to break down the triple corks that Canadians Mark McMorris and Max Parrot will throw down in that event to help show why one might have received higher scores from judges than the other. Normally, to most people, what they're both doing is little more than an awe-inspiring but dizzying blur of flips and spins. The new big air event is part of the International Olympic Committee's attempts to draw a new and younger audience to the Olympics. That's why it has opened the Olympics doors wide to new freestyle skiing and snowboarding events and shorter more dramatic versions of older sports like mass-start speed skating, team skiing and mixed doubles curling. Skateboarding and surfing are on tap for the 2020 Summer Games.

"The big question is about how people are going to consume sport in the future and what is interesting to the new generation," Rossier said. That's far from an idle curiosity for anyone at Omega, which has signed a contract to provide timing and other services at the Olympics until 2032. The hope is that translating athlete movements into graphic and visual displays will bring more understanding and interest to television audiences. [See full article for more information]

Unsecured Amazon S3 Buckets are Prime Cloud Target for Ransomware Attacks

https://www.techrepublic.com/article/unsecured-amazon-s3-buckets-are-prime-cloud-target-for-ransomware-attacks/

Thousands of S3 buckets are incorrectly configured as being publicly writable, making them easy to exploit. Building a slide deck, pitch, or presentation? Here are the big takeaways:

- *Security researchers are dropping notes in publicly writable S3 buckets to inform owners that their configuration leaves them vulnerable to attack.*
- *Amazon has provided free access to the S3 bucket permissions checker in AWS Trusted Advisor for all users in response to this issue.*

Misconfigured S3 buckets are a too-common problem among Amazon Web Services (AWS) users, and security researchers are taking notice. **Noted security researcher Kevin Beaumont has warned that publicly writable S3 buckets could be used by criminals in ransom attacks, similar to how tens of thousands of MongoDB instances were targeted last year.** Given the nature of ransomware attacks, and the massive amount of data that can be stored in S3 buckets, it is unlikely to be cost-efficient for hackers to copy data to restore to affected users who actually pay a ransom. As such, the likelihood of being able to retrieve data in the event that a ransom is paid is rather low—making this type of attack a "false ransom."

Security researcher Robbie Wiggins has been running a script which inserts a file named "POC.txt" in buckets erroneously configured to be publicly writable. Wiggins claimed in a tweet that the note has been left in 5260 buckets thus far. The BBC reported that almost 50 such warnings have been found in systems controlled by the organization. In a statement to the BBC, Wiggins noted that, of the buckets identified so far, "Lots of buckets appear to [have] been abandoned and forgotten about." Just in the past six months, documents have been exfiltrated from unprotected S3 buckets belonging to Verizon, the NSA, the US Military, French marketing company Octoly, and analytics firm Alteryx, which included data from credit reporting bureau Experian and the US Census Bureau.

Josh Mayfield, director at enterprise security firm FireMon, stated that "AWS will likely see a sizable ransomware attack in the coming months, not due to any flaws in AWS security, but because of misconfigurations. There is a persistent belief that since the infrastructure is a 'service' (IaaS), then the responsibility falls to the IaaS provider to secure their systems." Mayfield also noted that "AWS has gone through painstaking security development to bring the most robust controls you can have with a public cloud. Still, AWS users consistently fail to configure those controls."

In an effort to mitigate potential issues, **Amazon announced this week that the bucket permissions check in AWS Trusted Advisor is now free for all users**. The utility was previously available only to Business and Enterprise support customers. Given that the aforementioned groups who had documents stolen from publicly accessible S3 buckets would have logically been in those support tiers to begin with, Mayfield's claim that users fail to proactively configure these settings rings true.

Visa: EMV Cards Cut Down Counterfeit Card Fraud in the US by 70%

https://www.bleepingcomputer.com/news/security/visa-emv-cards-cut-down-counterfeit-card-fraud-in-the-us-by-70-percent/

Visa said last week that two years after US retailers started deploying terminals that could read chip-based credit and debit cards, reports of counterfeit card fraud have dropped by 70%.

While modern chip-based payment cards - also known as EMV (Europay, MasterCard, Visa) cards after the three organizations that promoted the new technology - are the standard payment card issued in most regions of the globe, the US has always lagged behind. The reasons are many, but most banks and retailers cited that it would be more costly to issue new EMV cards and replace classic magnetic strip payment terminals with modern devices that could also accept EMV cards. But **US banks and retailers got a kick in the behind in 2015 after a series of hacks at high-profile retailers such as Home Depot and Target. Hackers stole a large number of card numbers during those incidents, which fueled a sudden rise in counterfeit magnetic strip cards that criminal groups used to buy products in the names of legitimate account owners.**

At the pressure of the US government, US card issuers began a huge push to replace classic magnetic strip cards with EMV chip-based credit and debit cards in October 2015, which eventually forced shop owners to invest in EMV-compatible gear as well.

According to statistics released by Visa last week, EMV adoption among US retailers soared from 392,000 shops in September 2015 to over 2.7 million stores in December 2017, accounting for 59% of all US storefronts. Similarly, the number of EMV chip and PIN cards grew in the US from 159 million in September 2015 to over 481 million in December 2017. According to Visa, 67% of all Visa cards in the US are EMV-based and have a chip inside it. Furthermore, most of these account for cards associated with active users. Visa says EMV chip cards accounted for 96% of all US payments in December, showing that EMV has already taken over the US market.

EU Finance Head: We Will Regulate Bitcoin if Risks are not Tackled

https://www.theguardian.com/technology/2018/feb/26/eu-finance-head-regulate-bitcoin-cryptocurrencies-risks

The European Union has warned that it will regulate cryptocurrencies if the risks exposed by the meteoric rise of bitcoin and its ilk are not addressed. The boom and bust of cryptocurrencies has seen some investors make millions where others have suffered heavy losses. **Bitcoin, which now trades at about $9,000 (£8,000) a token but recently dropped to less than $6,000, leads the pack, rising nearly 2,000% to just under $20,000 in 2017, fuelling a global investment craze.** “This is a global phenomenon and it’s important there is an international follow-up at the global level,” Valdis Dombrovskis, the EU’s financial chief, said on Monday. “We do not exclude the possibility to move ahead (by regulating cryptocurrencies) at the EU level if we see, for example, risks emerging but no clear international response emerging.” Dombrovskis was speaking after hosting a roundtable meeting attended by the European Central Bank, industry bodies and the Financial Stability Board, which writes and coordinates regulation for the Group of 20 Economies. G20 finance ministers and central bankers meet in Buenos Aires in March, with cryptocurrencies set to be on the agenda. The EU would decide how to address the issue later this year or early in 2019, the financial services commissioner said.

Regulation of cryptocurrencies could seek to bring them in line with financial legislation designed to combat money laundering and counter-terrorism, forcing traders to disclose their identities and look to make it more difficult to use bitcoin, Ethereum or others for illegal activities.

A member of the ECB’s executive board, Yves Mersch, recently called for a global clampdown on cryptocurrencies, saying the central bank was aligned with the views voiced by Agustín Carstens, the head of the Bank for International Settlements, who condemned bitcoin as “a combination of a bubble, a Ponzi scheme and an environmental disaster”.

Germany and France said this month that new opportunities arise from cryptocurrencies, but they could pose substantial risks for investors and be vulnerable to financial crime without safeguards. So far, however, there appears to be no strong consensus among G20 countries to regulate them closely.

Policymakers worry about losing jobs and growth to other regions if they crack down hard on innovation in the sector, especially stemming from the blockchain technology that underpins cryptocurrencies, which Dombrovskis said held strong promise.

Markus Ferber, a centre-right member of the European parliament, said a quick EU regulatory response was needed, rather than waiting years for international rules to trickle through. "In order to make sure that retail investors do not fall prey to market manipulation and fraud, virtual currencies should be regulated as other financial instruments," Ferber said in a statement.

Important Email Likely to be Missed in Flood That's About to Hit Your Inbox

https://www.smh.com.au/technology/important-email-likely-to-be-missed-in-flood-that-s-about-to-hit-your-inbox-20180221-p4z14q.html

"Once more unto the (data) breach, dear customer."

To misquote Oscar Wilde, there is only one thing worse than not being told about a data breach, and that is being told about a data breach 10 times a day from 10 different service providers for the rest of eternity.

From today [February 22, 2018], Australian business enters a brave new world of data protection. **Under the watchful eye of the Office of the Australian Information Commissioner, the Notifiable Data Breaches scheme will require businesses with an annual turnover of more than $3 million to let their customers know if there has been unauthorised access to personal data in a way that could cause harm.** The scheme is an attempt to have Australia catch up with the rest of the world in terms of its corporate data security. **Failure to notify a breach attracts fines of up to $360,000 for individuals and $1.8 million for businesses, for serious or repeated infringements.**

With that type of penalty, and the likelihood of the office being keen to make an early example of businesses not doing the right thing, it would be safe to assume that companies will err on the side of caution - which means plenty of emails and texts to anxious customers. **The hair-trigger notifications run the risk of not just overwhelming inboxes but of a phenomenon known as "data breach notification fatigue". That is, consumers will become so inured to notifications of every attempt at a data hack that when the big one comes they will not respond to the warnings about changing passwords and cancelling credit cards.**

When you consider that research by Symantec shows that 7 billion online identities have been stolen in the past eight years (the equivalent of one for every person on the planet), the risk of notification fatigue is very real. The issue is, what constitutes a data breach that should trigger a notification? Is it a gentle tap on the cyber-door by a hacker who then runs away? Or is it a full blown ram raid where the bad guys get away with the goods?

The definition of "data breach" is broad, as is the definition of "serious harm". Data breach includes unauthorised access to, disclosure of, or loss of customer information held by a company (for example, personal information, credit reporting information or tax file information) and puts individuals affected at "real risk of serious harm". Harm includes all imaginable forms - physical, psychological, emotional, harm to reputation, economic harm and financial harm. This will require judgement calls to be made by organisations as to when notification is required to be made, and introduces compliance uncertainty, at least until a number of incidents have occurred and been considered by the Privacy Commissioner.

The notifications need to include specific details including the information involved and how those affected can respond to the incident (by cancelling credit cards or changing passwords, for example). The entity must make such a notification when it becomes aware that there are reasonable grounds to believe that there has been an eligible data breach. The entity must comply with these notification steps as soon as practicable. There are also quite robust obligations to undertake investigations even when an entity has a mere "suspicion" that there may have been a breach. In practical terms, this could mean you receive an email every time a business suspects but can't conclusively determine that there has been a data hack, in a world where cyberattacks are occurring by the thousands every day.

Fears about the costs to business and of data breach notification fatigue were partly responsible for delays in implementing the scheme. The delays mean Australia is still playing catch-up with other major economies. And the exemption of small businesses from taking part in the scheme could still mean Australia falls afoul of its major trading partners' requirements. The European Commission has the power to determine whether a country outside the EU offers an adequate level of data protection. If the EU is satisfied, then personal data can flow from the EU to that third country without any further safeguards being necessary. The EU has recognised New Zealand as offering adequate protection, but not Australia. Exempting around 60 per cent of Australia's businesses from the new scheme is hardly likely to provide much comfort for regulators in Brussels.

Click Unsubscribe to stop receiving the Digest.

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:

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