Security News Digest
November 14, 2017

Take the November Defensible Security Quiz to learn about this comprehensive cyber security model.

Canadians More Web-Connected, but at Possible Cost to Work-Life Balance, StatsCan Says

http://www.cbc.ca/news/business/statscan-work-life-balance-technology-1.4401290

[Some readers may want to keep this article as the stats are a very useful resource.]

Canadians are leading more and more digitally connected lives, and that's having both positive and negative implications on our well-being, a new Statistics Canada survey suggests. The data agency said in a report Tuesday that more and more Canadians are accessing the internet on a regular basis, with 91 per cent of Canadians over the age of 15 using the internet at least a couple of times every month last year. That's up from 86 per cent three years earlier 2013, and the prevalence of the internet in people's lives gets higher depending on how young you are.

The percentage for those between the ages of 15 to 44 was over 90 per cent last year, but it was similarly high in 2013 too. Among 65- to 74-year-olds, however, internet penetration has shot up in the past three years, from 65 per cent to 81. For those over 75, usage jumped from 35 per cent to 50 per cent. People offered many ways in which technology has improved their lives, with 77 per cent noting that it helps them to communicate with others, 66 per cent saying it saves time, 52 per cent stating that it helps to make more informed decisions, and 36 per cent saying it helps them be more creative.

And Canadians are going online via a wider variety of devices, too. The overwhelming majority of 15- to 34-year-olds reported having a smartphone last year, compared with 69 per cent of those aged 55 to 64 and just 18 per cent of Canadians 75 years and older. **All in all, more than three quarters of Canadians had a smartphone last year, and having one, the data agency said "now appears to be a near-necessity for the young."** For the most part, people say their lives are better because of their increasing use of online technology. Just over three out of every five people between the ages of 15 and 65 said their life was better as a result of their use of technology. From age 65 on, it declined to just over half of those aged 65 to 74 and continued falling to a little more than a third of Canadians aged 75 and older.

But there's a downside, too. Statistics Canada says that technology "blurs the boundaries by keeping one connected at all times and in all places," and there's a price being paid in terms of Canadians work-life balance. Between 2008 and last year, the proportion of working Canadians who were either satisfied or very satisfied with their work-life balance declined by 10 percentage points, dropping from 78 per cent to 68 per cent in that eight-year period. "While the majority still felt positive about their ability to balance work and home, the downward trend may have implications for the well-being of Canadians," the data agency said.

Professor Linda Duxbury at the Sprott School of Business at Carleton University in Ottawa says **her research makes it clear that work-life balance "is becoming more of a problem, not less of a problem**." Technology that makes people available all the time is great for connecting people, but comes with a corresponding cost in people's personal lives in terms of burnout, she said in an interview with CBC News Tuesday. **"The problem is those kinds of technologies give people the ability to work 24/7 and depending on the organization you work for … they might be connecting 24/7, all the time." A major problem is people's inability or reluctance to say no, she said**. "We see availability as a career move and saying no as a career-limiting move, and that is yet another added pressure."

Mira Akl is one Canadian who says technology is a double-edged sword in terms of her work-life balance. "It creates an obsession that's at your fingertips," the financial services worker said of the constant stream of emails she receives on her smartphone. "But then that creates a dependency, because people around you and your clients expect that kind of quick response ... if you're not answering this quickly." In the StatsCan report, women were slightly less likely than men to report they were happy with the balance

between their working and their personal lives, with 66 per cent responding so. Among men, the ratio jumped up 70 per cent. People with children were just as likely to say they were satisfied with their work-life balance as those without were. **But just over one in five people with a job reported that they either always or often had difficulties fulfilling family responsibilities because of the amount of time they spent on their job.** "Overall," the data agency said, "14 per cent of Canadians felt that technology often interfered with other things in life."

Torontonian Michael Yhip summed up the pros and cons succinctly. "Technology helps because you're more flexible, you don't have to be at the job," he said in an interview, "but it hurts because you're working at times when maybe you shouldn't." Duxbury's advice to phone-addicted workers is blunt: When you get home from work, "if you actually don't have the strength to shut it off, put it in a different room and don't check it," she said. "If that causes you to lose your job, you probably didn't want that job to begin with."

Federal Government Blocking Social Media Users, Deleting Posts

http://www.cbc.ca/news/politics/twitter-facebook-socialmedia-porn-1.4394127

Canadian government departments have quietly blocked nearly 22,000 Facebook and Twitter users, with Global Affairs Canada accounting for nearly 20,000 of the blocked accounts, CBC News has learned. Moreover, nearly 1,500 posts - a combination of official messages and comments from readers - have been deleted from various government social media accounts since January 2016. However, there could be even more blocked accounts and deleted posts. In answer to questions tabled by Opposition MPs in the House of Commons, several departments said they don't keep track of how often they block users or delete posts.

It is not known how many of the affected people are Canadian. It's also not known how many posts were deleted or users were blocked prior to the arrival of Prime Minister Justin Trudeau's government. **But the numbers shed new light on how Ottawa navigates the world of social media - where it can be difficult to strike a balance between reaching out to Canadians while preventing government accounts from becoming a destination for porn, hate speech and abuse.** The numbers came as Environment Minister Catherine McKenna found herself in a social media firestorm over a tweet from her official departmental account on Tuesday which praised Syria for joining the Paris climate change agreement. But while McKenna announced very publicly that that tweet had been deleted, the numbers tabled in the House of Commons reveal there were 97 other posts deleted from that department's accounts between Jan. 1, 2016 and Sept. 18, 2017.

In the department's answer, signed by McKenna, it said posts were deleted that were inconsistent with Treasury Board guidelines or "when it was necessary to correct errors in information, grammar or visual imagery, to clarify or more accurately reflect a priority, or to ensure adequate service in both official languages." **The Treasury Board sets rules for government communications, including social media.** "Social media moves quickly and sometimes mistakes happen."

But the environment department isn't the only one that has deleted an awkward tweet. [The remainder of this article details how many tweets were deleted by various federal departments and the reasons.]

Vancouver Police Issue $368 Ticket to Driver Playing Pokemon Go

https://globalnews.ca/news/3859140/vancouver-police-issue-368-ticket-to-driver-playing-pokemon-go/

[A definite candidate for the Darwin Award…] A Vancouver driver better have caught a Pikachu when police caught an individual playing Pokemon Go while at the wheel. Police issued a $368 ticket to a driver who pulled up right next to two police officers while playing the game, the Vancouver Police Department tweeted Monday afternoon. “While playing Pokemon Go may be fun, it’s not worth risking your life or the lives of others so that you can play while driving!” the police tweeted. A picture tweeted by the police clearly shows Pokemon Go displayed on a device.

This isn’t the first time that the Vancouver police have issued a cheeky tweet in response to a distracted driver. In late September, police caught someone using an electronic device behind the wheel. The person was issued a $368 ticket. This same driver was then caught eight minutes and six blocks later, doing precisely the same thing. The driver was issued a total of $736 in fines.

Phishing is the Greatest Threat to Account-Based Online Services – Research

https://hotforsecurity.bitdefender.com/blog/phishing-is-the-greatest-threat-to-account-based-online-services-research-19208.html

Internet giant Google has teamed up with the University of California, Berkeley to better understand how hijackers manage to trick users into taking over their online accounts via keyloggers, phishing attacks, or by using data exposed in large breaches. **By tracking black markets that traded third-party password breaches, as well as blackhat tools for phishing and keylogging, the team found that 788,000 credentials were stolen via keyloggers between March 2016 and March 2017.**
During the same period, 12 million credentials were stolen via phishing, and 3.3 billion credentials were exposed by third-party breaches.
Looking at data breaches only, the team found that 12% of the exposed records included a Gmail address serving as a username and a password, while 7% of those passwords proved valid for reuse. Attacks leveraging phishing schemes and keyloggers also successfully targeted Google accounts, with 12-25% of attacks yielding a usable password. To its defense, Google notes that, while its study focused on its own user base, "these password stealing tactics pose a risk to all account-based online services."
Google's research further uncovered that, because it uses various safeguards to prevent hackers from stealing user credentials, hijackers are employing increasingly sophisticated methods to try to collect sensitive data that the company may request when verifying an account holder's identity. In other words, both the vendor and the user must guard against scams.
Google lists a number of safeguards that users can leverage to detect phishing attacks, but doesn't mention dedicated anti-malware solutions with anti-spam and anti-phishing mechanisms. "We found 82% of blackhat phishing tools and 74% of keyloggers attempted to collect a user's IP address and location, while another 18% of tools collected phone numbers and device make and model," write Kurt Thomas, of the Anti-Abuse Research team, and Angelika Moscicki, of the Account Security team. "By ranking the relative risk to users, we found that phishing posed the greatest threat, followed by keyloggers, and finally third-party breaches," Google says.
Google is publishing this information so other vendors of online services can use the data to better secure their offerings. The company further notes that all account-based online services should "supplement their authentication systems with more protections beyond just passwords."

Twitter Suspends Verification Tool After White Nationalist Rally Organizer Gets Check Mark

https://globalnews.ca/news/3853681/twitter-verification-tool-white-supremacist/
Twitter's blue verification badge has evolved to signify importance within the Twitter community, though the social giant recently faced backlash by awarding a badge to well-known white supremacist Jason Kessler. Kessler recently made headlines for being an organizer of the far-right Unite the Right protest in Charlottesville, Va. this past August.
Twitter's current policy is to add a blue check mark to accounts that are verified as genuine to "authenticate identity and voice," as the company said in a statement. After Kessler received the badge next to his name, the known white nationalist tweeted to his 13,000 followers about the development. "Looks like I FINALLY got verified by Twitter," Kessler wrote in his tweet. "I must be the only working-class white advocate with that distinction."
Twitter removed the verification badge on Thursday after complaints about the verification began swirling on the platform. "Verification was meant to authenticate identity & voice but it is interpreted as an endorsement or an indicator of importance," Twitter support said. "We recognize that we have created this confusion and need to resolve it. We have paused all general verifications while we work and will report back soon." Twitter Chief Executive Jack Dorsey responded to the tidal wave of complaints a few days later, saying the verification policy was correctly followed in this circumstance but that it's a system that's long required an upgrade. "Our agents have been following our verification policy correctly, but we realized some time ago the system is broken and needs to be reconsidered," he tweeted, saying he should have addressed the issue sooner. "And we failed by not doing anything about it. Working now to fix faster."
Kessler is best known for his role in organizing the white nationalist rally in Charlottesville, Va., which eventually turned violent and led to the death of one woman. In addition, he was chased by an angry crowd after attempting to hold a press conference the day after the rally took place.

Facebook Wants You to Upload Your Nude Photos - To Help Fight Revenge Porn

https://globalnews.ca/news/3849836/facebook-nude-photos-revenge-porn/

Facebook is testing a new way to combat revenge porn **in Australia**: it involves uploading your nude photo or video directly to Messenger. **It may seem counterintuitive, but the idea is to upload intimate photos before an abuser or hacker has a chance to share them on Facebook or Instagram without your consent.** According to the Australian Broadcasting Company (ABC), Facebook is piloting the technology in partnership with the Australian government **in order to deter online harassment**. "We see many scenarios where maybe photos or videos were taken consensually at one point, but there was not any sort of consent to send the images or videos more broadly," Australia's safety commissioner, Julie Inman Grant told ABC.

How does it work? If there is a photo or video out there you are worried will be shared without your consent, Australians can contact the e-Safety commissioner. The organization will then tell you to send the image to yourself on Messenger. "It would be like sending yourself your image in an email, but obviously this is a much safer, secure end-to-end way of sending the image without sending it through the ether," Inman Grant said.

Once the nude image is uploaded, Facebook will use technology to "hash it," which is essentially giving it a digital fingerprint. "**They're not storing the image. They're storing the link and using artificial intelligence and other photo-matching technologies. So if somebody tried to upload that same image, which would have the same digital footprint or hash value, it will be prevented from being uploaded**," she said. If it works, then the photo or video will never show up on Facebook, even if a hacker or an ex-partner tries to upload it. **Australia is one of four countries taking part in this pilot project**, Facebook's head of global security, Antigone Davis told ABC.

Back in April, Facebook took steps aimed at combating revenge porn in Canada and the U.S., allowing users to flag an image they suspect was posted without consent. It's not known if the new pilot project in Australia will come to Canada or the U.S. Global News reached out to Facebook but did not hear back at the time of publication.

Kirsten Thompson, a cybersecurity and data lawyer, said Facebook may have a difficult time selling this idea to the public. ….She does give Facebook credit for the initiative. "Revenge porn is a huge problem and Facebook could be held liable for it, so they are trying to do something." **According to a 2016 study by the Data & Society Research Institute, one in 25 people have either been victims of revenge porn threats or posts, and 93 per cent of victims report significant emotional distress afterwards.**

Hackers Claim to Defeat iPhone X 'Face ID' Authentication

https://www.databreachtoday.com/hackers-claim-to-defeat-iphone-x-face-id-authentication-a-10452

The face-off between security researchers and the latest biometric authentication techniques continues, with a group from Vietnam claiming to have fooled the facial-recognition system, called Face ID, that's built into Apple's latest iPhone. **Face ID allows a user to unlock their iPhone X, make purchases from various Apple digital stores and authenticate Apple Pay transactions to pay using stored payment card data**.

Researchers from Vietnam-based information security firm Bkav say that since they first obtained an iPhone X on Nov. 5, they've been working nonstop to find a way to bypass the Face ID feature. On Friday, the researchers claimed to have been successful, and they published a video demonstrating their "proof of concept" hack, saying that Face ID is "not as secure" as Apple has suggested. [Article shows the 'mask' they developed.]

"The mask is crafted by combining 3D printing with makeup and 2D images, besides some special processing on the cheeks and around the face, where there are large skin areas, to fool [the] AI of Face ID," says Ngo Tuan Anh, Bkav's vice president of cybersecurity. His face was used as the model for the mask and then to unlock an iPhone X on which his face had been registered with Face ID. Apple didn't immediately respond to a request for comment. **When Apple announced the iPhone X at an event on Sept. 13, it claimed that there is only a one in a million chance that the wrong face could be used to unlock Face ID and said that the feature could not be fooled by masks**.

But Bkav claims that it has found a fake face fix that does the trick. The company says its recipe combines a handmade silicone nose that the company commissioned - it required unspecified tweaking before working - plus printouts from a 3D printer as well as two-dimensional printouts and handmade artwork, especially for the skin. The total cost of materials was $150, Bkav says.

The company says potential targets of this type of attack could be "billionaires, leaders of major corporations, [national] leaders." Having a team of researchers go to "Mission Impossible" lengths to craft a fake face that can be used to fool Apple's Face ID might seem to be an unlikely threat.

Attackers would need to gain physical access to a powered-on iPhone X as well as launch a successful attack within 48 hours. That's because Face ID has the same timeouts as Apple's Touch ID feature. A user's passcode or password must be entered after any restart, if 48 hours have elapsed since the device unlocked or if there have been more than five unrecognized access attempts in a row. **Users can also remotely disable Face ID if they lose their iPhone**.
But as Bkav emphasizes, applying their knowledge about how the iPhone X attempts to verify a face allowed them to put together a mask that defeated that system after just five days of work. **"It just goes to show that biometrics are still not the panacea that some hope they will one day become,"** says Alan Woodward, a professor of computer science at the University of Surrey. "And until all of these wrinkles are out of biometrics, we have the problem that once copied, unlike passwords, you can't change it." Expect Apple to issue an update for the Face ID software or new generations of the iPhone with hardware designed to block these circumvention techniques. But biometrics remains a cat-and-mouse game. **"These hacks may be made more expensive to mount, but the problem is that once successful, the biometric effectively becomes useless for that individual, Woodward says. "It makes an excellent way of hacking high-value targets - something criminals are doing in increasing numbers."**
Until biometrics can be made perfect, Woodward recommends users rely on tried-and-true security defenses. "I suspect it will be a long time before we have a universally acceptable biometric, or any other single form of access control," he says. "Until then, **we really do need to take two-factor authentication as the benchmark**."

School Websites Across U.S. Hacked with Pro-Islamic State Message

https://globalnews.ca/news/3848374/us-school-websites-hacked-islamic-state-message/
[Nov7] Hackers temporarily redirected people looking for hundreds of local school webpages across the U.S. to a video in support of the Islamic State group. The FBI is trying to determine who was behind the hack, which hijacked school websites in Tucson, Arizona; Newtown, Connecticut; Gloucester County, Virginia; and Bloomfield, New Jersey. The Bloomfield school district said their website displayed the IS video for about two hours Monday before it was taken down.
SchoolDesk, the Atlanta-based company that maintains the site, said in a statement that **technicians discovered a small file was injected into the root of one of its websites. That redirected approximately 800 school and district webpages to a YouTube video containing an audible Arabic message, unknown writing and a picture of Saddam Hussein**. "It looked like it was some sort of ISIS recruitment or support video," SchoolDesk founder Rob Freierson told NJ.com.
SchoolDesk's statement said **the hack also affected other organizations, including private and government websites**. The company has added more protections and is requiring users of its websites to reset their passwords. The Bloomfield district said no confidential student or teacher information was compromised. SchoolDesk said it was working with various investigative agencies to track the source of the hack.

Estonia Deals with Massive Security Flaw in Digital ID Cards

https://hotforsecurity.bitdefender.com/blog/estonia-deals-with-massive-security-flaw-in-digital-id-cards-19200.html
Estonians were not allowed to use online government services for an entire weekend, as efforts were made to fix a security flaw in the chip encryption of the national identity cards, writes the BBC. The security flaw was detected by researchers in September who warned the government about possible identity theft risks.
"[The] danger of the security threat becoming real was increased by the fact that it was not a flaw of the Estonian ID card alone, but also included cards and computer systems around the world that use the chips by the same producer," said Kaspar Korjus, managing director for the e-resident program. "This brought the safety flaw to the attention of international cybercrime networks which had significant means to take advantage of the situation." This was a huge problem, as **the digital ID system is used by Estonian citizens and residents to access all important public and private services, including online government services, medical records, online banking and voting systems**.
760,000 Estonians, almost half of the country's population, were affected earlier this year by the security flaw which could have permitted hackers access to private data and citizen impersonation. "As far as we currently know, there has been no instances of e-identity theft, but the threat assessment of the Police

and Border Guard Board and the Information System Authority indicates that this threat has become real," said the country's Prime Minister Juri Ratas. "The functioning of an e-state is based on trust and the state cannot afford identity theft happening to the owner of an Estonian ID card."
ID cards issued between October 2014 and October 25th, 2017 will be blocked until the security certificates are updated. Users are to update the security certificates by March 2018. To avoid error messages and a system crash, updates for the digital ID cards are performed based on priority: medical professionals and frequent users first. "We are aware that many citizens, residents and e-residents have been receiving error messages due to the high volume of people updating at the same time," Korjus said. "As a result, the ability to update certificates was temporarily restricted last weekend in order to prioritize people who use their digital ID cards to provide vital services, such as medical professionals inside Estonia, as well as the most frequent users, which will include e-residents that will be notified by email."

And Now, This: Volume 1.

The FDA has Approved the First Digital Pill

https://www.theverge.com/2017/11/14/16648166/fda-digital-pill-abilify-otsuka-proteus

The Food and Drug Administration has approved **the first digital pill for the US which tracks if patients have taken their medication. The pill called Abilify MyCite, is fitted with a tiny ingestible sensor that communicates with a patch worn by the patient - the patch then transmits medication data to a smartphone app which the patient can voluntarily upload to a database for their doctor and other authorized persons to see.** Abilify is a drug that treats schizophrenia, bipolar disorder, and is an add-on treatment for depression. [add-on = "off label" = not specifically approved but doctors are encouraged by drug companies to prescribe for 'other conditions']
The Abilify MyCite features a sensor the size of a grain of sand made of silicon, copper, and magnesium. An electrical signal is activated when the sensor comes into contact with stomach acid - the sensor then passes through the body naturally. A patch the patient wears on their left rib cage receives the signal several minutes after the pill is ingested. The patch then sends data like the time the pill was taken and the dosage to a smartphone app over Bluetooth. The patient's doctor and up to four other people chosen by the patient, including family members, can access the information. The patient can revoke access at any time.
The pill comes after years of research and is a venture between Japanese pharmaceutical company Otsuka and digital medicine service Proteus Digital Health, which makes the sensor. The pill is one way to address the prevalent problem of patients not taking their medication correctly, with the IMS Institute estimating that the improper and unnecessary use of medicine cost the US healthcare sector over $200 billion in 2012. The approval also opens the door for pills that are used for other conditions beyond mental health to be digitized.
Experts though, have expressed concerns over what the pill might mean for privacy. Some are worried that tracking pills will be a step towards punishing patients who don't comply. Ameet Sarpatwari, an instructor in medicine at Harvard Medical School told *The New York Times* the digital pill "has the potential to improve public health. [But] if used improperly, it could foster more mistrust instead of trust." *The Wall Street Journal* reports that **the FDA is anticipating a potential raft of approval requests for other digital pills**. A spokesperson told the publication the FDA is planning to hire more staff with "deep understanding" of software development in relation to medical devices, and engage with entrepreneurs on new guidelines. Otsuka hasn't indicated how much the digitized Abilify pills will cost yet. The *WSJ* reports the company plans to work with some insurers in covering the digitized pills with production planned to be ramped up only if it can find willing insurers.

And Now, This: Volume 2.

[I just had to share this exciting news! Hmm… Silmarillion?]

Amazon Announces Lord of the Rings TV adaptation

https://www.theguardian.com/tv-and-radio/2017/nov/13/lord-of-the-rings-amazon-tv-show-confirmed

The streaming service has acquired the rights to JRR Tolkien's fantasy epic and has committed to a multi-season series with potential spin-offs.
Bilbo Baggins, Gandalf and the rest of Middle Earth are making the switch to the small screen after Amazon announced it has committed to a multi-series adaptation inspired by JRR Tolkien's classic fantasy novels. *The television adaptation will tell new stories based in the period preceding The Fellowship of the Ring*, the novel that provided the basis for the first part of Peter Jackson's film trilogy.

A Lord of the Rings series had been rumoured, but on Monday the streaming service confirmed it had acquired rights to Tolkien's work and would be pursuing the project with a potential spin-off. "The Lord of the Rings is a cultural phenomenon that has captured the imagination of generations of fans through literature and the big screen," said Sharon Tal Yguado, Amazon's new head of scripted programming, who took on the role after the resignation of Roy Price last month amid sexual harassment allegations. "We are honored to be working with the Tolkien Estate and Trust, HarperCollins and New Line on this exciting collaboration for television and are thrilled to be taking The Lord of the Rings fans on a new epic journey in Middle Earth."
Matt Galsor, a representative for the Tolkien estate and trust and the publisher HarperCollins, said: "We are delighted that Amazon, with its longstanding commitment to literature, is the home of the first-ever multi-season television series for The Lord of the Rings. *"Sharon and the team at Amazon Studios have exceptional ideas to bring to the screen previously unexplored stories based on JRR Tolkien's original writings."* According to the Hollywood Reporter, the move comes as Amazon attempts to find a challenger to HBO's Game of Thrones, and establish a big-name franchise after a run of poorly received scripted programmes. The news comes after Disney announced it was working on a live-action Star Wars TV project led by The Last Jedi director Rian Johnson, which will feature completely new characters in "a corner of the galaxy that Star Wars lore has never before explored". Jackson's cinematic adaptations of The Lord of the Rings grossed nearly $6 billion worldwide, winning 17 Academy Awards, including Best Picture.