BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
February 20, 2018

Don’t Miss our February Quiz:
'Love Your Online Life' Security Quiz

A Special Message to Security News Digest Readers:
My name is Arlene. I have been the editor of the Security News Digest for many years and it has always been the favourite part of my job in Security Awareness. I am someone who devours and dissects the news with my sociology brain - analyzing the growth and implications of technology and the internet on our privacy, security, and social behaviour. This is my last issue of the Security News Digest – I am retiring from the public service. My very capable colleagues in Security Awareness will be continuing to bring you “the news that matters”.
Even though the Digest is a compilation of news articles, it has felt like a blog that I put together for you, as the articles are chosen based on what would benefit the average user to be aware of what is happening in the constantly evolving cyber world and how to protect their information. Thank you for your participation in the success of the Digest. It has been my pleasure to communicate to you every week. Farewell, and remember to ‘Keep it Secret and Keep it Safe’.

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/

Nine Out of 10 of Canadian Companies Suffered a Cybersecurity Breach in 2017

https://www.canadiansecuritymag.com/news/data-security/nine-out-of-10-of-canadian-companies-suffered-a-cybersecurity-breach-in-2017
According to the 2018 Scalar Security Study (commissioned by Scalar and conducted independently by IDC Canada), **Canadian organizations are attacked in varying degrees of severity more than 450 times per year, with 87 per cent suffering at least one successful breach. Almost half (46 per cent) are not confident in their ability to defend against attacks.** “As cybersecurity breaches become the new normal, organizations can’t be complacent. Many companies are still reporting gaps in their defences despite hiring full-time security staff, which may point to a deficit in the availability of highly skilled IT workers,” said Theo Van Wyk, Chief Security Architect, Scalar Decisions. “The rising number of high-impact breaches coincides with the increasing costs of recovery.”
The study, examining the cybersecurity readiness of Canadian organizations and year-over-year trends in handling and managing growing cyber threats, also found: (1) Of the companies that suffered a security breach, 47 per cent had sensitive data stolen, (2) One in five breaches were classified as “high impact,” where sensitive customer or employee information was exposed, (3) 36 per cent of respondents are not confident in their company’s ability to respond to security breaches, (4) The average company spends $3.7 million in direct and indirect costs to recover from security breaches, (5) One-fifth of smaller organizations believe they don’t have enough resources to effectively defend against attacks, (6) Firms dedicate about 10 per cent of their IT budgets to security spending, (7) A majority of respondents do not train employees to identify attacks, such as phishing scams, or to update software with the latest security measures, and (8) Almost three-quarters of respondents don’t comprehensively analyze how third-party relationships effect their overall cybersecurity planning.

“Canadian companies are getting better at prioritizing cybersecurity, but there is still a substantial lack of training and planning,” added Van Wyk. “Organizations need to look beyond their infrastructure and weigh the insider and third-party risks they face. If this can’t be tackled in-house, then external expertise is an efficient way to shore up their defences.” All responses for the study were captured in November and December 2017 by IDC Canada through a Canada-wide cross-industry survey of 421 IT security and risk & compliance professionals.

Cyberspies Defend Proposed New Authority to Go On the Offensive 🇨🇦

https://www.canadiansecuritymag.com/news/data-security/cyberspies-defend-proposed-new-authority-to-go-on-the-offensive

A senior official from Canada's cyberspy agency says proposed new powers would allow it to stop a terrorist's mobile phone from detonating a car bomb, block the ability of extremists to communicate, or prevent a foreign power from interfering in the country's democratic process. A Liberal bill would help the Communications Security Establishment counter various forms of cyber aggression and violent extremism, Shelly Bruce, associate chief of the CSE, told a House of Commons committee studying the legislation. A December report by leading Canadian cybersecurity researchers said there is no clear rationale for expanding the CSE's mandate to conduct offensive operations. It said the scope of the planned authority is not clear, nor does the legislation require that the target of the CSE's intervention pose some kind of meaningful threat to Canada's security interests. Bruce stressed the proposed legislation contains safeguards that would prohibit the agency from directing active cyber operations at Canadians. It would also forbid the CSE from causing death or bodily harm, or wilfully obstructing justice or democracy.

The Ottawa-based CSE intercepts and analyzes foreign communications for intelligence of interest to the federal government. It is a member of the Five Eyes intelligence alliance that also includes the United States, Britain, Australia and New Zealand. The Liberal bill provides a statutory mandate for the highly secretive agency, which traces its roots to 1946, while giving it new muscle to conduct both defensive and offensive cyber operations. The powers would help keep Canadians safe against global threats, including cyberthreats, in a rapidly evolving technological world, Bruce said during the committee meeting. She provided some concrete examples of how the CSE might use its new offensive capabilities - with input from other federal officials as well as accountability measures in the new law to prevent abuse. "Active cyber operations are meant to achieve an objective that the government has established and that's a team sport," she cautioned. Bruce said a cyber operation could be aimed at interrupting communications of an extremist group like the Islamic State of Iraq and the Levant "in a way that would stop attack planning before things reach a crisis pitch." An effort might involve preventing the spread of ransomware - software that holds people's valuable data hostage in return for payment, she said. Or the CSE could try to corrupt data on systems abroad that had been stolen from Canadian servers, rendering it useless to the thieves.

Bruce tried to allay concerns about how the CSE would use publicly available information under the new legislation and what effect this might have on the privacy of Canadians. CSE would carry out "basic research" from the sort of public resources available to anyone in Canada, Bruce said. "CSE does not, and would not use publicly available information to investigate Canadians or persons in Canada, or build dossiers on them," she said. "That is not our mandate, and for us, mandate matters." The cyberspy agency would use publicly available materials to provide general background information for a foreign intelligence or cybersecurity report, to assess the nationality of a person or organization, or to consult technical manuals, Bruce said. Under no circumstances would the agency use this provision to acquire information - such as hacked or stolen data - that was unlawfully obtained, she added.

Advertisers Warn Social Media to Step Up, or They're Out 🇨🇦

http://www.cbc.ca/news/technology/social-media-advertising-facebook-google-1.4538685

Trust in what we read online is eroding quickly, and social media and "Big Tech" are facing blame. It's even reaching a tipping point for advertisers, who are threatening to pull their ad dollars from the digital domain unless things change - fast. "Consumers don't trust what they see online."

That was a central theme in a speech by Unilever's chief marketing officer Keith Weed on Monday, at the Interactive Advertising Bureau's Annual Leadership Meeting in Palm Desert, California. The company, which owns brands including Dove, Lipton and Ben & Jerry's, is one of the world's biggest advertisers, spending over two billion dollars a year on online advertising alone. **Citing fake news, racism, sexism,**

terrorists spreading messages of hate, and toxic content directed at children, Weed proclaimed that trust in social media is at an all-time low. He threatened to pull ads from major platforms such as Facebook and Google unless the digital giants take steps to filter out misinformation and abusive content. Weed said it is "acutely clear" that "people are becoming increasingly concerned about the impact of digital on well-being, on democracy and on truth itself," he said. "This is not something that can brushed aside or ignored."

Canadians are concerned- Consumers' waning trust in social media and online search engines is also the focus of a new report from Edelman Intelligence. The 2018 "Trust Barometer" is the global communications firm's 18th annual trust and credibility survey. The online survey, conducted last fall, included 1,500 Canadian respondents over the age of 18, with 200 of them considered to be "informed public respondents" who pay attention to news and public affairs. **According to this year's report, Canadians rank their trust in journalism substantially higher than their trust of social media platforms.** The survey shows that over 60 per cent are unable to distinguish between false reporting and objective journalism, and "65 per cent of Canadians worry about fake news being used as a weapon," underscoring the concerns flagged by Weed in his speech.

"It's clear that consumers have lost trust, and it's not just Unilever making this claim," says Mary Joyce, the impact design director for Harmony Labs in New York, an incubator devoted to tackling issues such as filter bubbles and people's ability to detect persuasion online. **"The growth of social media is partly to blame for this trend, reducing the power of traditional news gatekeepers to define truth and outsourcing legitimacy to anyone who can set up a Twitter account or use Photoshop."** To that point, the Edelman report found that **trust in social media has been steadily declining, since its peak at 40 per cent in 2012**. "Having become sophisticated advertising channels, these platforms have valued clicks and eyeballs over truth and trust up until this point," says Joyce. [article has more discussion]

International Day of Women and Girls in Science Encourages Girls to Consider STEM 🇨🇦

https://www.thestar.com/news/gta/2018/02/11/international-day-of-women-and-girls-in-science-encourages-girls-to-consider-stem.html

When Milica Mijalkovic grows up, she wants to work in the field of economics. She wants to be an investment analyst, she specifies, because she really loves data analytics. Mijalkovic is a Grade 11 student at Victoria Park Collegiate Institute. Two years ago, she was one of five girls out of 30 students in her introduction to computer science class. “It was a bit discouraging actually that I only saw a few girls in class,” she said. “But I think it’s really important to invest myself in technology.”

Things were a little different on Sunday. Mijalkovic was in a group of 60 girls who met with three female science pioneers on the second International Day of Women and Girls in Science. **Held at Facebook headquarters in Toronto, the event served as the launch of the federal government’s second phase of its plan to encourage increased female participation in science, technology, engineering and mathematics (STEM).**

The next phase is called “Choose Science” - a digital campaign sharing why women chose to work in the sciences. The aim is to create a network of mentors to inspire future female STEM leaders. “We need to include all people to make sure we have the right answers for our future, and if you only have men making those decisions that’s not good,” said Kate Young, parliamentary secretary for science. “Young girls do need to hear these stories to know there’s a place for (them).”

In 1987, only 20 per cent of the people working in STEM fields were female, a number that has moved up to just 22 per cent today. Just 29.6 per cent of individuals with a post-secondary STEM credential and 26.9 per cent of those employed in a STEM-intensive occupation in Canada are women.

Julia Wagner, a Grade 12 student, is the only female programmer on her school’s robotics team, and was the only girl in her computer technology class. She chose science because her father, an engineer, inspired her. “I think a lot of girls, especially when they’re younger, get scared seeing so many men in technology and engineering,” she said. “It kind of intimidates them and they don’t want to take part in engineering. “But I want more girls to take these classes, because it’s such a great experience.” The panellists echoed Wagner’s sentiments in their discussion. To great applause, Joelle Pineau, the director of Facebook artificial-intelligence research in Montreal, said that she had four children and two jobs. “Everyone has to make choices,” said Pineau. Her decision to join the Facebook team after 12 years as a university professor was a risk she wasn't sure would work. "But we have to encourage girls to take risks much more. We have to embrace girls taking risks." ….

North Korean Hacking Group APT37 Expands Targets

https://www.securityweek.com/north-korean-hacking-group-apt37-expands-targets

A lesser known hacker group believed to be working on behalf of the North Korean government has been expanding the scope and sophistication of its campaigns, according to a report published on Tuesday by FireEye. The threat actor is tracked by FireEye as APT37 and Reaper, and by other security firms as Group123 (Cisco) and ScarCruft (Kaspersky). APT37 has been active since at least 2012, but it has not been analyzed as much as the North Korea-linked Lazarus group, which is said to be responsible for high-profile attacks targeting Sony and financial organizations worldwide.

Cisco published a report in January detailing some of the campaigns launched by the threat actor in 2017, but APT37 only started making headlines in early February when researchers revealed that it had been using a zero-day vulnerability in Adobe Flash Player to deliver malware to South Korean users. APT37, whose goals appear to align with North Korea's military, political and economic interests, has mainly focused on targeting public and private entities in South Korea, including government, defense, military and media organizations. **However, according to FireEye, the group expanded its attacks to Japan, Vietnam and even the Middle East last year. The list of targets includes organizations in the chemicals, manufacturing, electronics, aerospace, healthcare, and automotive sectors.**

One of the targets in the Middle East was a telecommunications services provider that had entered an agreement with the North Korean government. The deal fell through, which is when APT37 started hacking the Middle Eastern company, likely in an effort to collect information, FireEye said. APT37 has exploited several Flash Player and Hangul Word Processor vulnerabilities to deliver various types of malware, including the RUHAPPY wiper, the CORALDECK exfiltration tool, the GELCAPSULE and HAPPYWORK downloaders, the MILKDROP and SLOWDRIFT launchers, the ZUMKONG infostealer, the audio-capturing tool SOUNDWAVE, and backdoors tracked by FireEye as DOGCALL, KARAE, POORAIM, WINERACK and SHUTTERSPEED. This malware has been delivered using social engineering tactics, watering holes, and even torrent sites for wide-scale distribution.

FireEye is highly confident that APT37 is linked to the North Korean government based on several pieces of evidence, including the use of a North Korean IP, malware compilation timestamps consistent with a typical workday in North Korea, and objectives that align with Pyongyang's interests. "North Korea has repeatedly demonstrated a willingness to leverage its cyber capabilities for a variety of purposes, undeterred by notional redlines and international norms," FireEye said in its report. "Though they have primarily tapped other tracked suspected North Korean teams to carry out the most aggressive actions, APT37 is an additional tool available to the regime, perhaps even desirable for its relative obscurity. We anticipate APT37 will be leveraged more and more in previously unfamiliar roles and regions, especially as pressure mounts on their sponsor." Neither Kaspersky nor Cisco have explicitly attributed the APT37 attacks to North Korea.

13 Russians Indicted for Massive Operation to Sway US Election

http://www.darkreading.com/attacks-breaches/13-russians-indicted-for-massive-operation-to-sway-us-election/d/d-id/1331085

[Feb16] A federal grand jury has indicted 13 Russian nationals and three Russian entities for a massive operation intended to interfere with the 2016 US presidential election. US Special Counsel Robert Mueller has accused the defendants of posing as Americans to sway election results. The Internet Research Agency, a Russian organization, and the 13 actors reportedly began targeting the United States back in 2014. **Mueller's indictment claims they "had a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election."** To do this, they launched an operation to support the Trump campaign and denigrate Hillary Clinton. In April 2014 the agency formed a department focused on the US population and operated on social platforms including Facebook, Instagram, Twitter, and YouTube. By 2014, its strategy included fomenting distrust in US presidential candidates and the US political system.

Activity included buying political advertisements on social media with the identities of US citizens and businesses. The defendants concealed their Russian identities and affiliation with the Internet Research Agency by using stolen data like Social Security numbers and birthdates of real

American people. They also recruited Americans to aid efforts to spread promotional and derogatory information. **The actors posed as US citizens and groups to create and control social media accounts.** An example is the Twitter account "Tennessee GOP" under the handle @TEN_GOP, which falsely claimed to be operated by a US political party and amassed more than 100,000 followers. On other sites, particularly Facebook and Instagram, they posted content about political issues.

Around June 2016, the defendants began posing as American citizens and communicating with Americans to gather intelligence and learn where they should focus their efforts. Some traveled to the US to collect info for their operations and stage political rallies. **To further conceal their identities, the defendants and their co-conspirators bought space on servers based in the US to set up VPNs. They used these VPNs to connect from Russia to the US and access online social media accounts, open new accounts, and talk with US citizens.**

The first time the United States indicted nation-state threat actors was in 2014, when the DoJ indicted five members of the Chinese military for allegedly hacking major American manufacturing companies and stealing trade secrets. In 2016 it indicted seven Iranian hackers for distributed denial-of-service (DDoS) attacks against US financial companies. It's worth noting these indictments are rare and don't usually end with an arrest.

Russian Twitter Bots Keep Up Attack After Florida Shooting

https://www.cnet.com/news/russian-twitter-bots-still-a-menace-after-florida-shooting/

The Russian Twitter bots are back. Or more accurately, they never left. After Wednesday's mass shooting at Marjory Stoneman Douglas High School in Parkland, Florida, thousands of tweets poured in using the hashtag #guncontrolnow and jumped on the trending topic #Parklandshooting. These weren't coming from Americans with thoughts on the country's gun-rights debate. They were from Russian-controlled bots jumping on this divisive issue.

Among the most tweeted two words from the Russian bots were "gun control" and "school shooting," according to Botcheck.me, a tracking website that follows 1,500 propaganda bots on Twitter. Sound familiar? The way the bots seized on this issue and played both sides is eerily familiar with how they have taken control of debates ranging from Black Lives Matter to the 2016 US presidential election. It's a strategy direct from the Russian trolling playbook: Jump on a hot button issue and stir outrage on both sides of the argument. The continued resurgence of bot influence underscores the difficulty that tech giants like Twitter, Facebook and Google face in fighting propaganda - even after they've identified the problem.

Despite the grilling these companies have received since the 2016 election, the bot influence didn't end. And it didn't end Friday, with the US government's indictment of the Internet Research Agency, a Russian troll factory that's spread chaos across social media. **The Alliance for Securing Democracy, which tracks Russian bots on Twitter, has created a website called Hamilton 68 to follow the propaganda in real time.** Before the school shooting, the bot army had been tweeting about US special counsel Robert Mueller but then quickly stormed both sides of the gun control debate once the news broke, according to the New York Times. ….. But last week, the gun-related tweets escaped skepticism and were believable enough to pop up on Twitter's trending topics, hijacking popular hashtags to muddy the debate. Over the last few months, Twitter and Facebook have vowed to fix these issues, with Facebook CEO Mark Zuckerberg making it his new year's resolution. And in a blog post last month, Twitter acknowledged that 1.4 million people were exposed to Russian propaganda on its social network and said it's focused on preventing bot accounts from surfacing. **The social network said it blocks 523,000 bots a day on Twitter. Yet somehow, thousands of bots still thrive on the platform and managed to pounce on the Florida school shooting.**

US Joins UK in Blaming Russia for NotPetya Cyber-Attack

https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

The US and UK governments have publicly blamed Russia for a crippling cyber-attack last year that targeted Ukraine and spread around the world. On Thursday, Sarah Sanders, the White House press secretary, said that the NotPetya ransomware attack in June 2017 “was part of the Kremlin’s ongoing effort to destabilise Ukraine and demonstrates ever more clearly Russia’s involvement in the ongoing conflict.” She added: “This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.” Sanders said it had caused billions of dollars of damage.

The statement came after the British defence secretary, Gavin Williamson, accused the Russian government of “undermining democracy” with the attack, which primarily targeted Ukraine’s financial, energy and government sectors before it spread across the world. **The two governments’ unusual public accusation echoed the conclusions already reached by many private sector cyber security experts.**
Ukraine has been in conflict with Kremlin-backed separatists since Russia annexed Crimea in 2014. Williamson said: **“We have entered a new era of warfare, witnessing a destructive and deadly mix of conventional military might and malicious cyber-attacks.** “Russia is ripping up the rulebook by undermining democracy, wrecking livelihoods by targeting critical infrastructure and weaponising information ... We must be primed and ready to tackle these stark and intensifying threats.”
Russia has denied responsibility for **the attack, which is estimated to have cost companies more than $1.2billion** (£850m). It claimed that Russian businesses were among those with systems affected. The foreign minister, Lord Ahmad, said the UK’s decision to identify the Kremlin as responsible showed that the government would not tolerate malicious cyber activity. “The UK government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017 ... The Kremlin has positioned Russia in direct opposition to the west, yet it doesn’t have to be that way.

Russian Hackers Sentenced to Prison in US for Compromising 160 Million Credit Cards

https://hotforsecurity.bitdefender.com/blog/russian-hackers-sentenced-to-prison-in-us-for-compromising-160-million-credit-cards-19606.html

Two Muscovites [Moscow citizens] have been sentenced to years in prison for their roles in the biggest data breach conspiracy ever prosecuted in the United States. Three co-conspirators are still at large. Vladimir Drinkman, 37 and Dmitriy Smilianets, 34, had previously pleaded guilty for their roles in the conspiracy to commit wire fraud, before receiving their final sentences in a Camden, New Jersey federal court last week. They are just two of the five conspirators who, **since 2009, had systematically targeted major corporate networks, compromising 160 million credit card numbers and inflicting hundreds of millions of dollars in losses**.
The fraudsters compromised the computer networks of some of the biggest players in various major industries, such as NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard. **Financial statements by just three of these organizations revealed damages upwards of $300 million because of the breaches, according to justice.gov.** Drinkman and Alexandr Kalinin, 31, **specialized in penetrating network security and gaining access to corporate systems**, while Roman Kotov, 36, (along with Drinkman) **then mined the networks to steal credit card data**. Mikhail Rytikov, 30, **hid these activities using anonymous web-hosting services – acting as the others’ personal ISP (internet service provider)**. Rytikov also **made it possible for the party to monetize the heists by selling the stolen information on the underground web**.
Leveraging known vulnerabilities in the Structured Query Language (SQL) employed by some databases, the perps used injection attacks to deploy malware and create a back door they could later use to exfiltrate data. When their efforts were hampered by security systems, they would employ “persistent attacks,” otherwise known as advanced persistent threats, or APTs. They used end-to-end encrypted messaging services to discuss their operations, and sometimes met in person, fearing authorities were onto them, court documents say.
“Instant message chats obtained by law enforcement revealed the defendants often targeted the victim companies for many months, waiting patiently as their efforts to bypass security were underway,” according to the justice.gov report. “The defendants had malware implanted in multiple companies’ servers for more than a year. **“To protect against detection by the victim companies, the defendants altered the settings on victim company networks to disable security mechanisms from logging their actions. The defendants also worked to evade existing protections by security software,”** the report adds. For their actions, Drinkman and Smilianets were sentenced to 12 and 4.5 years, respectively, behind bars, plus three years of supervised release. The others in the party – Kalinin, Kotov and Rytikov – are still fugitives.

Millions Stolen From Russian, Indian Banks in SWIFT Attacks

https://www.securityweek.com/millions-stolen-russian-indian-banks-swift-attacks

Malicious hackers attempted to steal millions of dollars from banks in Russia and India by abusing the SWIFT global banking network. A report published last week by Russia's central bank on the types of attacks that hit financial institutions in 2017 revealed that an unnamed bank was the victim of a successful SWIFT-based attack.

A copy of the report currently posted on the central bank's website does not specify how much the hackers stole, but Reuters said they had managed to obtain 339.5 million rubles (roughly $6 million). According to the organization, the number of targeted attacks aimed at lenders increased in 2017 compared to the previous year. Attackers used widely available tools such as Metasploit, Cobalt Strike, Empire, and Mimikatz to achieve their goals – Cobalt Strike was reportedly used to steal more than 1 billion rubles (roughly $17 million).

The news comes after Russia's Globex bank admitted in December that hackers had attempted to steal roughly $940,000 through the SWIFT system. The attackers reportedly only managed to steal a fraction of the amount they targeted. In India, City Union Bank issued a statement on Sunday saying that it had identified three fraudulent transfers abusing the SWIFT payments messaging system. One transfer of $500,000 through a Standard Chartered Bank account in New York to a bank in Dubai was blocked and the money was recovered. The second transfer of €300,000 ($372,000) was made to an account at a bank based in Turkey via a Standard Chartered Bank account in Germany. The funds were blocked at the Turkish bank and City Union hopes to recover the money. The third transfer was for $1 million and it went to a Chinese bank through a Bank of America account. City Union Bank said the funds were claimed by someone using forged documents.

The news comes after reports that India's Punjab National Bank was the victim of a massive $1.7 billion fraud scheme involving the company's employees. City Union, however, clarified that this was a "cyber attack initiated by international cyber criminals and there is no evidence of internal staff involvement."

SWIFT-based attacks made many headlines in the past years ever since hackers successfully stole $81 million from Bangladesh's central bank in early 2016. The organization behind the SWIFT system, the Society for Worldwide Interbank Financial Telecommunication, has taken measures to prevent attacks, but malicious actors have continued to target financial institutions in sophisticated campaigns. Hackers attempted to steal $60 million from a bank in Taiwan, $12 million from a bank in Ecuador, and $1.1 million from a bank in Vietnam.

Half A Million People Don't Know Criminals Stole Their Identities to Get Jobs

http://www.nextgov.com/cybersecurity/2018/02/half-million-people-dont-know-criminals-stole-their-identities-get-jobs/146077/

A programming error kept the IRS from notifying hundreds of thousands of identity theft victims about criminals using their Social Security numbers to get themselves jobs in 2017, according to an internal investigation. Last year, more than half a million Americans had their identities used by others to get hired, but only first-time victims received a notification from the IRS, the Treasury Inspector General for Tax Administration found. As a result, nearly 460,000 previous victims of employment identity theft were left in the dark about their information getting stolen yet again. "Most identified victims remain unaware that their identities are being used by other individuals for employment," TIGTA wrote in its report.

Auditors determined a programming error limited theft notifications to only those who were not labeled as victims in prior years. The inspector general brought the error to the attention of the IRS in April 2017, and the agency said it planned to implement a correction by Jan. 27. IRS could not confirm to *Nextgov* whether the system has been updated. To spot employment identity theft, IRS compares the Individual Taxpayer Identification Numbers and Social Security numbers on electronically submitted tax returns. When it finds a mismatch, the agency alerts the individual their identity may be compromised. Of the 112,445 people who received notifications in 2017, investigators found roughly 13.5 percent weren't actually victims of identity theft. The false alerts most commonly stemmed from couples double-filing returns that included the other spouse's wages and Social Security numbers.

"Employment identity theft can cause a significant burden to innocent taxpayers, including the incorrect computation of taxes based on income that does not belong to them," said investigators, adding, "erroneously marking taxpayers' accounts with the employment identity theft marker causes taxpayer burden and confusion when they receive the [identity theft] notice." In addition to updating the identity verification system, TIGTA recommended the IRS tell as-of-yet unnotified victims their Social Security numbers were stolen and alert those who accidentally received identity theft alerts to the agency's mistake. IRS agreed with all recommendations.

And Now, This:

Apple's New Spaceship Campus Has One Flaw – and It Hurts

https://www.bloomberg.com/news/articles/2018-02-16/apple-s-new-spaceship-campus-has-one-flaw-and-it-hurts

[On the theme of: "nothing is perfect"…] **The centerpiece of Apple Inc.'s new headquarters is a massive, ring-shaped office overflowing with panes of glass, a testament to the company's famed design-obsessed aesthetic. There's been one hiccup since it opened last year: Apple employees keep smacking into the glass.**

Surrounding the building, located in Cupertino, California, are 45-foot tall curved panels of safety glass. Inside are work spaces, dubbed "pods," also made with a lot of glass. Apple staff are often glued to the iPhones they helped popularize. That's resulted in repeated cases of distracted employees walking into the panes, according to people familiar with the incidents. Some staff started to stick Post-It notes on the glass doors to mark their presence. However, the notes were removed because they detracted from the building's design, the people said. They asked not to be identified discussing anything related to Apple. Another person familiar with the situation said there are other markings to identify the glass.

Apple's latest campus has been lauded as an architectural marvel. The building, crafted by famed architect Norman Foster, immortalized a vision that Apple co-founder Steve Jobs had years earlier. **In 2011, Jobs reportedly described the building "a little like a spaceship landed." Jobs has been credited for coming up with the glass pods, designed to mix solo office areas with more social spaces.** The building is designed to house some 13,000 employees.

Wired magazine, first to pay a visit at its opening last year, described the structure as a "statement of openness, of free movement," in contrast to Apple's typically insular culture. "While it is a technical marvel to make glass at this scale, that's not the achievement," Jony Ive, Apple's design chief, told the magazine in May. "The achievement is to make a building where so many people can connect and collaborate and walk and talk."

An Apple spokeswoman declined to comment. It's not clear how many incidents there have been. A Silicon Valley-based spokeswoman for the Occupational Safety and Health Administration referred questions about Apple's workplace safety record to the government agency's website. A search on the site based on Apple's name in California found no reports of injuries at the company's new campus.

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

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.

****