Security News Digest
September 26, 2017

You will still be using your mobile devices next week, but the..
September Living Mobile Quiz
will move to the previous quizzes page.

October is Cyber Security Awareness Month

B.C. Liberals Rapped Over Delays Responding to FOI Requests

http://www.timescolonist.com/news/local/b-c-liberals-rapped-over-delays-responding-to-foi-requests-1.22883546

The previous B.C. government routinely broke the freedom of information law by missing deadlines and failing to respond to access requests in a timely manner, a new report shows. Drew McArthur, acting information and privacy commissioner, said the former Liberal government exceeded the 30-day time limit and any legitimate time extensions in one of every five cases in 2016-17. "This should be an extraordinary finding; however, I am concerned that it has instead become normal for government to operate in violation of [the law]," McArthur writes in the 60-page report, Timing is Everything. "This level of contravention is unacceptable. I find it difficult to imagine a circumstance where government would tolerate its citizens breaking the law 20 per cent of the time, yet this is the circumstance in which government found itself."

McArthur said the findings are particularly troubling given that his office has seen a 75 per cent increase in requests for time extensions over the past two years. "Time extensions under [the law] are intended to be the exception rather than the norm," he writes. Minister of Citizens' Services Jinny Sims said she's still reviewing the report, but said the new NDP government will improve timeliness and make government more transparent. "We do have to do in-depth consultation," she said. "We're not planning to take years, but on the other hand, it can't be done within 60 days, either.

….The review, which was carried out this year, examined 194 randomly selected files to assess government's response to information requests from April 1, 2015, to March 31, 2017. McArthur acknowledged that the number of access requests has increased to nearly 10,000 a year from about 6,000 in 2008. But he argues that's no excuse for missing legislated deadlines. "Government may be receiving more access requests now compared to when [the law] was first enacted, but the law does not permit non-compliance simply because more people are exercising their rights," he said. The report calls on government to "take whatever action is necessary" to comply with the law, allocate more resources to close overdue files and expand its proactive disclosure program.

Watchdog Flags Privacy Breaches in Phoenix Pay System

https://globalnews.ca/news/3761113/watchdog-flags-privacy-breaches-in-phoenix-pay-system/

The federal privacy watchdog says inadequate testing, coding errors and poor monitoring of the beleaguered Phoenix federal pay system resulted in exposure of the personal information of public servants. In his annual report tabled today, privacy commissioner Daniel Therrien found **at least 11 breaches occurred and the personal information at issue included employee names and salary information**. Therrien says **most of the vulnerabilities were government-wide**, meaning the information of all employees in the Phoenix system at the time of each breach was at risk.

In some cases, the commissioner found, information could be changed and transactions could be conducted. In addition, Therrien determined there may be lingering vulnerabilities that could lead to future breaches. The Phoenix pay system has been riddled with other problems, leaving some public servants without pay cheques for many weeks.

Therrien also warns in his report that in a general sense, Canadians fear they are losing control over their personal information in the digital age. In addition to Phoenix, his office looked into potential privacy issues with the mydemocracy.ca website used to consult Canadians last year on electoral reform. Therrien found that the site contained third-party scripts that could disclose users' personal information to

Facebook without their consent. The privacy watchdog also tackled the Canada Border Services Agency's "Scenario Based Targeting Program" which uses advanced analytics to identify potential terrorist threats based on traveler demographics. "The review raised the concern that some of the national security scenarios used by CBSA are broad and based on personal characteristics which identify a large number of law abiding individuals, whose personal information is used and shared without sufficient privacy protections," Therrien wrote in a summary of the report. Therrien is expected to address the findings at a news conference in Ottawa on Thursday afternoon.

After Woman Goes Public, Montreal Police Arrest Man Accused of Posting Her Personal Info in Escort Ads

http://www.cbc.ca/news/canada/montreal/after-woman-goes-public-montreal-police-arrest-man-accused-of-posting-her-personal-info-in-escort-ads-1.4299259

Montreal police have arrested a man they believe is responsible for posting a woman's personal information in three online ads for an escort in late August. CBC News first reported the story of Melissa, a Montreal woman whose personal information was posted in three escort ads without her consent or knowledge. Melissa is not her real name. Her identity is being protected because she is concerned the situation could escalate if her name is published. Her phone number, address, photo and real name were posted in the ads, which advertised free "kinky" sex. Shortly afterward, she received a number of text messages requesting sex. A strange man knocked on her apartment door, prompting her to move out of her home immediately.

Police obtained warrant. Melissa said when she went to police, they told her they wouldn't be able to do anything unless they got a warrant, and they were unlikely to be able to get one. After she went public with her story, police succeeded in obtaining a warrant to investigate further. Police say a suspect was arrested late last week and released on the condition he'll appear in court to be formally charged. It's unclear what charge or charges he'll face. Police say he is expected to appear in court in the next few days to be formally charged.

Kik Messenger Promised To Remove Child Predators - I Just Found 10 In 2 Hours

https://www.forbes.com/sites/thomasbrewster/2017/09/20/kik-slow-to-delete-child-abuse-profiles-despite-promise/#3b77d206dda8

In August, when *Forbes* reported it'd found nearly 20 profiles of charged or sentenced pedophiles on Kik Messenger, the hugely popular chat app's owners promised to do better and proactively remove accounts "for users who have been convicted of crimes related to child abuse." Up until today, though, it's unclear what efforts **$1 billion-valued Canadian firm** went to in order to remove those profiles. With its **15 million monthly active users, 57% in the 13-24 age bracket**, Kik had seemingly deleted just one user named in *Forbes*' investigation. But subsequently, this publication gathered more than 25 active Kik profiles linked to horrific crimes against minors, many of whom have been convicted.

In just two hours, some simple Google searching on Thursday last week turned up 11 profiles police had linked to child abuse crimes. Searching the Department of Justice website via Google, with terms like "Kik" and "username," provided a quick way to find profiles of convicted child abuse crimes. ..In another example, the profile *jmayes773*, operated by Jarrod Mayes, who was sentenced in 2016 to 60 months in prison, was still online. According to the DoJ, he admitted to first encountering child pornography on Kik, where he would later go on to share and acquire the illegal content.

Forbes' search for usernames of profiles of convicted child abusers and those sharing exploitation material occurred last Thursday. By Tuesday, Kik had been supplied with the full list of names linked to illegal activity. Later on Wednesday Kik said it had terminated users where it found publicly-verifiable information linking a Kik ID to a convicted sex offender. It didn't terminate those for which it couldn't find that data, but was continuing to dig Wednesday, a spokesperson said.

As part of its investigation into child exploitation on Kik, *Forbes* created fake profiles of 14-year-old girls, which received almost-instant contact from male users, some sending sexually-explicit content. A vast number of search warrants also revealed widespread sharing of child abuse material on Kik; in one startling case, a single suspect was found to be a member of more than 200 Kik groups all set up for users to share such illegal content.

Kik investing $10 million in safety. Kik, meanwhile, is building up to a big funding boost and the safety of children on the platform should benefit. The Canadian app is looking to raise a massive $125 million through the sale of its own cryptocurrency, Kin. On September 12, it announced it had already raised $50

million in a presale round. *Forbes* understands Kik Interactive, the firm behind the messenger app, will devote $10 million of the funds raised to safety on its platform. That could see more roles dedicated to deleting profiles of pedophiles and child abusers. CEO Ted Livingston confirmed in a statement sent to *Forbes* that Kik had launched "a new safety initiative, which is supported by a $10 million budget over the next 18 months." "We have already increased our investment in moderation and are dedicating additional product development and engineering resources to this initiative," Livingston added.
"As a result, we have recently been able to conduct sweeps of more than 15,000 Public Groups, and terminated 4,000 of those groups after determining they were in violation of our terms of service. In the process of conducting these reviews, we also terminated 500 users and when appropriate made referrals to law enforcement. We want all users to feel safe on Kik and will continue to make Kik a safe, positive and productive place for our users to interact."

House Investigators Demand Details on Private E-Mail Use by Trump Advisers

https://beta.theglobeandmail.com/news/world/us-politics/house-investigators-demand-details-on-private-e-mail-use-by-trump-advisers/article36395138/

A top House Republican has demanded details on the use of private emails by some of President Donald Trump's closest advisers. Rep. Trey Gowdy, a South Carolina conservative who chairs the House Oversight and Government Reform Committee, and the top Democrat on that panel, Rep. Elijah Cummings, **cite a recent Politico report that Jared Kushner set up a private email account after the election to conduct work-related business. The New York Times is reporting that at least six of Trump's closest advisers, including Kushner, Steve Bannon and Reince Priebus, used private email to discuss White House matters**.
During the 2016 presidential campaign, Trump repeatedly attacked Democratic opponent Hillary Clinton for setting up a private email server as secretary of state, a decision that prompted an FBI investigation that shadowed her for much of the campaign. Gowdy is best known for his two-year investigation into the 2012 attacks in Benghazi, Libya, in which he focused heavily on Clinton's role as secretary of state. In letters Monday to White House general counsel and State Department, Gowdy and Cummings said they want details on all employees.
"With numerous public revelations of senior executive branch employees deliberately trying to circumvent these laws by using personal, private, or alias email addresses to conduct official government business, the committee has aimed to use its oversight and investigative resources to prevent and deter misuse of private forms of written communication," the lawmakers wrote. White House press secretary Sarah Huckabee Sanders told reporters Monday that the use of private email accounts by staff was "to my knowledge, very limited." "White House counsel has instructed all White House staff to use their government email for official business, and only use that email," she said, adding that "we get instructed on this one pretty regularly."
Kushner's lawyer, Abbe Lowell, on Sunday confirmed Kushner's use of a personal email in his first few months of the administration. He said the emails usually involved news articles and political commentary. Lowell also said that any non-personal emails were forwarded to Kushner's official account and "all have been preserved in any event." Sanders would not say whether the White House would release Kushner's private emails that dealt with government business.

GO Keyboard Apps Could Be Spying On Over 200 Million Android Users

https://www.phonearena.com/news/GO-Keyboard-apps-could-be-spying-on-over-200-million-Android-users_id98312

According to a new report, a pair of third party keyboard apps that are listed in the Google Play Store under GO Keyboard could actually be spying on you. The developer, listed as the GOMO Dev Team, says that "We will never collect your personal info including credit card information. In fact, we cares for privacy of what you type and who you type!" That hardly seems to be the case as the apps allegedly have access to data showing your identity, phone call records, and can listen in to the microphones on your handset.
These apps have over 200 million users and allegedly communicate with "dozens" of ad networks and third-party trackers. **As soon as you install one of the two GO Keyboard apps, information about you is being transmitted**. And yet, in 20 countries, the apps were voted best app of 2016! According to the report, the GO apps send to its server information like your Google email account, screen size, Android version, build and device model. Since we are talking about an app that records every letter you

type on your phone, the server owner could start collecting whatever information he/she wants from GO Keyboard users.
Google has been informed, and while the search giant decides what to do, **your best bet is to uninstall any GO Keyboard app that you might have downloaded on your Android phone**. The two apps are named "GO Keyboard-Emoji keyboard, Swipe input, GIFs" and "GO Keyboard-Emoticon keyboard, Free Theme, GIF." As you can tell, both apps offer emoji and GIFs to spruce up your texting. Both are freemium apps, which can be installed for free and include ads and in-app purchases. **But the bottom line is, both apps could be turning over personal information to a server in China**. "Unfortunately, everything listed above is a norm nowadays. Recent research showed that **7 in 10 mobile apps share your data with third-party services**. However, this developer crossed the red line and directly violated the Google Play content policies - malicious behavior section."

I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets

https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold
[This article is presented in almost its entirety because of its security and privacy awareness value.]
UK - At 9.24pm (and one second) on the night of Wednesday 18 December 2013, from the second arrondissement of Paris, I wrote “Hello!” to my first ever Tinder match. Since that day I’ve fired up the app 920 times and matched with 870 different people. I recall a few of them very well: the ones who either became lovers, friends or terrible first dates. I’ve forgotten all the others. But Tinder has not.
The dating app has 800 pages of information on me, and probably on you too if you are also one of its 50 million users. In March I asked Tinder to grant me access to my personal data. Every European citizen is allowed to do so under EU data protection law, yet very few actually do, according to Tinder. With the help of privacy activist Paul-Olivier Dehaye from personaldata.io and human rights lawyer Ravi Naik, I emailed Tinder requesting my personal data and got back way more than I bargained for. Some 800 pages came back containing information such as my Facebook “likes”, my photos from Instagram (even after I deleted the associated account), my education, the age-rank of men I was interested in, how many times I connected, when and where every online conversation with every single one of my matches happened … the list goes on.
“I am horrified but absolutely not surprised by this amount of data,” said Olivier Keyes, a data scientist at the University of Washington. **“Every app you use regularly on your phone owns the same [kinds of information]. Facebook has thousands of pages about you!”** As I flicked through page after page of my data I felt guilty. **I was amazed by how much information I was voluntarily disclosing**: from locations, interests and jobs, to pictures, music tastes and what I liked to eat. But I quickly realised I wasn’t the only one. A July 2017 study revealed Tinder users are excessively willing to disclose information without realising it. “You are lured into giving away all this information,” says Luke Stark, a digital technology sociologist at Dartmouth University. **“Apps such as Tinder are taking advantage of a simple emotional phenomenon; we can’t feel data. This is why seeing everything printed strikes you. We are physical creatures. We need materiality.”**
Reading through the 1,700 Tinder messages I’ve sent since 2013, I took a trip into my hopes, fears, sexual preferences and deepest secrets. Tinder knows me so well. It knows the real, inglorious version of me who copy-pasted the same joke to match 567, 568, and 569; who exchanged compulsively with 16 different people simultaneously one New Year’s Day, and then ghosted 16 of them. “What you are describing is called **secondary implicit disclosed information**,” explains Alessandro Acquisti, professor of information technology at Carnegie Mellon University. “Tinder knows much more about you when studying your behaviour on the app. It knows how often you connect and at which times; the percentage of white men, black men, Asian men you have matched; which kinds of people are interested in you; which words you use the most; how much time people spend on your picture before swiping you, and so on. **Personal data is the fuel of the economy. Consumers’ data is being traded and transacted for the purpose of advertising.” Tinder’s privacy policy clearly states your data may be used to deliver “targeted advertising”.**
….So why does Tinder need all that information on you? “To personalise the experience for each of our users around the world,” according to a Tinder spokesperson. “Our matching tools are dynamic and consider various factors when displaying potential matches in order to personalise the experience for each of our users.” Unfortunately when asked how those matches are personalised using my information, and which kinds of profiles I will be shown as a result, Tinder was less than forthcoming.

“Our matching tools are a core part of our technology and intellectual property, and we are ultimately unable to share information about our these proprietary tools,” the spokesperson said.
The trouble is these 800 pages of my most intimate data are actually just the tip of the iceberg. “Your personal data affects who you see first on Tinder, yes,” says Dehaye. “But also what job offers you have access to on LinkedIn, how much you will pay for insuring your car, which ad you will see in the tube and if you can subscribe to a loan. **“We are leaning towards a more and more opaque society, towards an even more intangible world where data collected about you will decide even larger facets of your life. Eventually, your whole existence will be affected.”**
Tinder is often compared to a bar full of singles, but it’s more like a bar full of single people chosen for me while studying my behaviour, reading my diary and with new people constantly selected based on my live reactions. **As a typical millennial constantly glued to my phone, my virtual life has fully merged with my real life. There is no difference any more. Tinder is how I meet people, so this is my reality. It is a reality that is constantly being shaped by others – but good luck trying to find out how.**

Major Accounting Firm Deloitte Reports Extensive Cybersecurity Breach

https://www.engadget.com/2017/09/25/deloitte-reports-extensive-cybersecurity-breach/

Deloitte, a major US and global accounting firm, revealed that it was hit with a cybersecurity breach that may have extended from October of last year through this past March, the *Guardian* reports. The company - one of the world's Big Four accounting firms - which works with large banks, global firms and government agencies, among others, provides tax and auditing services, operations consulting, merger and acquisition assistance and, wait for it, cybersecurity advice.
It's currently unclear who was behind the attack, but for the past six months, Deloitte has been investigating the breach of its email server, which exposed some five million emails. Along with emails and their sometimes sensitive attachments, the hackers may have gotten their hands on usernames, passwords, IP addresses, business information and workers' health records. The breach apparently stemmed from an administrator's account that was protected by a password and not two-step verification.
The *Guardian* reports that six of Deloitte's clients have been notified that their information was affected. A Deloitte spokesperson told the newspaper, "In response to a cyber incident, Deloitte implemented its comprehensive security protocol and began an intensive and thorough review including mobilising a team of cybersecurity and confidentiality experts inside and outside of Deloitte." The review of the breach is ongoing and the company is working to retrace the hacker's steps to see exactly what information was accessed. "The review has enabled us to understand what information was at risk and what the hacker actually did, and demonstrated that no disruption has occurred to client businesses, to Deloitte's ability to continue to serve clients, or to consumers," said the spokesperson.
Deloitte hasn't stated which of its clients, which include US government agencies, have been impacted, but said, "As part of the review, Deloitte has been in contact with the very few clients impacted and notified governmental authorities and regulators. We remain deeply committed to ensuring that our cybersecurity defences are best in class, to investing heavily in protecting confidential information and to continually reviewing and enhancing cybersecurity. We will continue to evaluate this matter and take additional steps as required."

CCleaner Backdoor Attack: A State-Sponsored Espionage Campaign

https://www.hackread.com/ccleaner-backdoor-attack-a-state-sponsored-espionage-campaign/

Previously we informed you about hacking of anti-virus maker firm Avast’s CCleaner software and embedding of a malicious malware payload in two of the software’s versions namely CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 (both are 32-bit versions). An initial investigation carried out by security researchers at Cisco Talos revealed that with this attack, hackers managed to compromise Avast’s servers as well as embed a backdoor and a multi-stage malware payload, which got installed automatically whenever CCleaner was installed.
Reportedly, the infected CCleaner software was distributed to nearly 700,000 customers between 15th August and 12th September. **Newest details related to this hack attack reveal that a state-sponsored hacker group might be involved in the attack while mainstream tech giants were the real targets of hackers**. Previously Avast maintained that the malware payload was never delivered to customers and therefore, there was no damage caused. However, **latest revelations point out that the**

scope of the damage is far greater than what we have been told so far because it is indeed true that the payload was delivered effectively. Unarguably, the objective of distributing malware at such a massive scale was to gain access to the servers and networks of high-profile tech firms including Google, Microsoft, Intel, Vodafone, SinTel, VMware, HTC, Sony, Samsung, D-Link, Akamai, Linksys, and Cisco.
It must be noted that CCleaner software removes unwanted data like temporary files and cookies and scans for malware and other data monitoring software on Windows-based systems. As per researchers, the malicious code was added to the software before its compilation, which means the hackers had access to Piriform, CCleaner's development infrastructure providing firm. Avast acquired Piriform in July.
Cisco's research team got hands on a copy of the C&C server of the hackers where they discovered detailed logs of over 700,000 computers. These computers had communicated with the hackers earlier in September. Further investigation revealed that the hackers weren't at all interested in a majority of the infected customers, which led the researchers to believe that this was actually a well-designed, state-sponsored attack. **The attack was targeted towards major tech firms, and the motive was to access and copy trade secrets and internal data of these organizations**. Thus, Cisco's researchers concluded that what they have been treating as a "run-of-the-mill mass cybercrime scheme" was a "state-sponsored spying operation" in reality.
Security experts are divided regarding which group could be involved. Cisco Talos highlighted that the presence of malware in CCleaner software has the same code that is linked with a notorious yet sophisticated hacking group called Group 72 or Axiom. As cited by Motherboard, the group was noted to be involved by security firm Novetta in a Chinese government operation back in 2015. Another security firm FireEye hasn't named any particular hacker group as yet but believes that state actors are involved: "FireEye found infrastructure overlap with a nation-state threat actor. CCleaner is used in lots of orgs (even if primarily consumer-focused). Supply chain compromise is a perfect vector for a nation-state to use," says Christopher Glyer, FireEye's chief security officer.
One of the configuration files present on the server, claims Cisco, was set in China's time zone but this couldn't be regarded as solid evidence against China. Nonetheless, after the emergence of new information, Avast finally conceded that what they have been claiming so far that the multi-stage payload was never delivered was a false claim, however, **now the company states that the second stage payload was sent to nearly 8 companies, and affected machines are in "the order of hundreds**."
"The server logs indicated 20 machines in a total of 8 organizations to which the 2nd stage payload was sent, but given that the logs were only collected for little over three days, the actual number of computers that received the 2nd stage payload was likely at least in the order of hundreds." Cisco has warned targeted tech firms that the problem cannot be fixed by deleting CCleaner software because the payload might have installed the second payload on their networks and the C&C server might still be actively communicating with it.

7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks

https://www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/

During the past year, there has been a surge in data breach reporting regarding Amazon S3 servers left accessible online, and which were exposing private information from all sorts of companies and their customers. In almost all cases, the reason was that companies, through their staff, left Amazon S3 "buckets" configured to allow "public" access. This means that anyone with a link to the S3 server could access, view, or download its content.
The problem is that most companies believe that if they're the only ones knowing the database's URL, they are safe. This is not true. Attackers can obtain these URLs using MitM attacks on corporate networks, accidental employee leaks, or by brute-forcing domains for hidden URLs.
While this sounds complicated, there are open-source available on GitHub that simplify the discovery of public S3 buckets, putting a large number of companies at risk.
According to statistics by security firm Skyhigh Networks, 7% of all S3 buckets have unrestricted public access, and 35% are unencrypted, meaning this is an endemic problem of the entire Amazon S3 ecosystem. These lapses in security best practices have resulted in some serious breaches, from army contractors to big-time US ISPs.
Below is a (most likely incomplete) list of all the major data leaks caused by companies leaving Amazon S3 buckets configured with public access during the past few months. (1) Top defense contractor **Booz Allen Hamilton** leaks 60,000 files, including employee security credentials and passwords to a US

government system. (2) **Verizon partner** leaks personal records of over 14 million Verizon customers, including names, addresses, account details, and for some victims - account PINs. (3) An AWS S3 server leaked the personal details of **WWE fans [World Wrestling]** who registered on the company's sites - 3,065,805 users were exposed. (4) Another AWS S4 bucket leaked the personal details of over 198 million **American voters**. The database contained information from three data mining companies known to be associated with the Republican Party. (5) Another S3 database left exposed only leaked the personal details of job applications that had Top Secret government clearance. (6) **Dow Jones**, the parent company of the Wall Street Journal, leaked the personal details of 2.2 million customers. (7) Omaha-based voting machine firm **Election Systems & Software** (ES&S) left a database exposed online that contained the personal records of 1.8 million Chicago voters. (8) Security researchers discovered a Verizon AWS S3 bucket containing over 100 MB of data about the company's internal system named **Distributed Vision Services** (DVS), used for billing operations. (9) An auto-tracking company leaked over a half of a million records with logins/passwords, emails, VIN (vehicle identification number), IMEI numbers of GPS devices and other data that is collected on their devices, customers and auto dealerships.

Companies that want to avoid situations like the above should review the following Amazon documentation pages [go to article for the links] and make sure they fully understand their server's permissions level: Overview of Managing Access; Introduction to Managing Access Permissions to Your Amazon S3 Resources; and Managing Access Permissions to Your Amazon S3 Resources. In addition, Mark Nunnikhoven, Vice President of Cloud Research at Trend Micro, also has a simple guide on how to secure an Amazon S3 buckets.

Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks

https://gizmodo.com/equifax-has-been-sending-consumers-to-a-fake-phishing-s-1818588764

Equifax's response to its data breach has been a total shitshow, something the company seems determined to remind us of each and every day. For nearly two weeks, **the company's official Twitter account has been directing users to a *fake* lookalike website, the sole purpose of which is to expose Equifax's reckless response to the breach**. After announcing the breach, Equifax directed its customers to equifaxsecurity2017[dot]com, a website where they can enroll in identity theft protection services and find updates about how Equifax is handling the "cybersecurity incident."

But the decision to create "equifaxsecurity2017" in the first place was monumentally stupid. The URL is long and it doesn't look very official - that means it's going to be very easy to emulate. Fake versions of the site could be used to phish Equifax customers and steal their personal information, again. **A much safer choice would have been to create a subdomain on the Equifax website (equifax.com) and direct users there.**

To illustrate how idiotic Equifax's decision was, developer Nick Sweeting created a fake website of his own: securityequifax2017[dot]com. (He simply switched the words "security" and "equifax" around.) Sweeting's website looks slightly different than the official Equifax website, as you can see below [in the source article], but only because he isn't actually trying to dupe anyone.. Sweeting's intentions clearly aren't malicious. If anything, he's trying to demonstrate why Equifax needs to shut down its website, or at least transfer it elsewhere, so it isn't further exposing consumers to risk.

As if to demonstrate Sweeting's point, Equifax appears to have been itself duped by the fake URL. The company has directed users to Sweeting's fake site sporadically over the past two weeks. Gizmodo found eight tweets containing the fake URL dating back to September 9th: Each of the tweets containing Sweeting's URL is signed by someone at Equifax named "Tim." The latest tweet was sent out September 19th. (Equifax deleted this tweet Wednesday morning, but at the time of writing the other seven tweets were still live.)

"It's in everyone's interest to get Equifax to change this site to a reputable domain," Sweeting told Gizmodo. "I knew it would only cost me $10 to set up a site that would get people to notice, so I just did it." The real Equifax site is dangerous, he said, because of how easy it is to impersonate. "It only took me 20 minutes to build my clone. I can guarantee there are real malicious phishing versions already out there." [definitely, there are phishing versions set up by scammers offering people the opportunity to learn if their information was compromised – they just have to provide their personal identifying information!]

Amazon Reviewing Sales Algorithm after Suggestions in U.K. that Bomb-Making Ingredients Be Bought Together

http://www.cbc.ca/news/business/amazon-bomb-making-1.4300136
Amazon says it is reviewing its website after a British news channel found that the online retailer's product algorithm was suggesting customers buy products that when used together could build an explosive device. Britain's Channel 4 News reported on Monday that the website was recommending that people who bought one product may want to buy another.
That's a common practice for the company, but the type of items being sold raised eyebrows. By themselves, none of the products are illegal or worthy of suspicion, but when they are used together, items such as ball bearings, battery connectors, cables and switches can be used to make explosives. The website was recommending that people who bought one of the items should buy others, too, because they are "frequently bought together."
The discovery comes days after someone made such a device and left it on a London tube train on Sept. 15, injuring more than two dozen people when it went off. Amazon said it was reviewing its policies in the wake of the TV channel's report. "In light of recent events, we are reviewing our website to ensure that all these products are presented in an appropriate manner," Amazon said in a statement, while adding that everything the company sells is well within the bounds of legality. "All products sold on Amazon must adhere to our selling guidelines and we only sell products that comply with UK laws," Amazon said.

Facebook Will Hand Over 3,000 Russia-Linked Ads to Congress

https://www.cnet.com/news/zuckerberg-vows-to-protect-election-integrity/
Facebook CEO Mark Zuckerberg is digging more into the possible role his social network - as well as covert Russian agents - may have played in the 2016 US election. The world's largest social network said Thursday it's handing over 3,000 Russia-linked ads to the Senate and House intelligence committees as investigators delve into what happened.
Earlier this month, Facebook disclosed it sold $100,000 worth of ads to inauthentic accounts likely linked to Russia during the election. Last week, the company said it's working with investigators as Special Counsel Robert Mueller and his team examine alleged Russian meddling into the election. "This has been a difficult decision. Disclosing content is not something we do lightly under any circumstances," Colin Stretch, Facebook's general counsel, said in a blog post. "We believe the public deserves a full accounting of what happened in the 2016 election, and we've concluded that sharing the ads we've discovered, in a manner that is consistent with our obligations to protect user information, can help."
Facebook has been in the spotlight as it tries to grapple with its scale and influence. The social network faces continued criticism for its handling of false news spreading on the site, as well as accusations that Facebook adds to division in the country by splitting people up over their ideologies.
As part of the announcement, Zuckerberg also outlined ways Facebook would try to protect the integrity of elections. He said the company would be more transparent around political ads - with added requirements like disclosures about who paid for them, as well as strengthening the review process around them. "We are in a new world," Zuckerberg said during a live broadcast on his Facebook page. "It is a new challenge for internet communities to deal with nation states attempting to subvert elections." He also said the company is doubling the number of workers on its team for "election integrity." Facebook will also add 250 people across all its teams working on safety and security.
Zuckerberg said Facebook is conducting its own investigation into Russian interference, as well as cooperating with investigators on the federal probe. The CEO also said Facebook has been working to make sure the upcoming German election has not been compromised. Zuckerberg's comments are a stark contrast from the stance he took days after the election. He said at the time it was a "pretty crazy idea" that fake news circulating on Facebook influenced the outcome. Since then, Zuckerberg hasn't been shy about wading into political debate. For example, he sharply criticized President Donald Trump's executive order on immigration. He's also embarked on a tour of the US to meet people in rural areas, in what he's said is an attempt to understand the people in this country better.
While he tried to offer up solutions on Thursday, he was quick to emphasize that Facebook won't be able to prevent all wrongdoing on its site. "There will always be bad people in the world, and we can't prevent all governments from all interference," Zuckerberg said. "But we can make it harder. We can make it a lot harder."

Adobe's Product Security Team Accidentally Posted Its Private PGP Encryption Key To Its Blog

https://www.gizmodo.com.au/2017/09/adobes-product-security-team-accidentally-posted-its-private-pgp-encryption-key-to-its-blog/

The past few weeks have been a nightmare for data breaches, so good news: Here's another easily preventable security problem. Adobe's Product Security Incident Response Team accidentally posted the private PGP encryption key - necessary to decrypt encoded messages transmitted to them using their public PGP key - associated with their psirt@adobe.com email account this week, Ars Technica reported. The mistake was first noticed on Friday afternoon by security researcher Juho Nurminen, who posted it to Twitter with the caption "Oh shit Adobe". PGP, which stands for Pretty Good Privacy, is a method for sending encrypted messages with close to government-grade security. PGP users receive two keys: a public PGP key tied to an email address or username, which encrypts incoming messages, and a private key which should be known only to the recipient used to decrypt said messages. Just knowing the private PGP key would not in and of itself allow a malicious user to breach Adobe's associated email account, which would have its own layers of security. But as the Register noted, the leak of the key could cause other problems for Adobe, since the email address was used to report critical security flaws with their products: Armed with the private key, an attacker could spoof PGP-signed messages as coming from Adobe. Additionally, someone (cough, cough the NSA) with the ability to intercept emails - such as those detailing exploitable Flash security vulnerability reports intended for Adobe's eyes only - could use the exposed key to decrypt messages that could contain things like, say, zero-day vulnerability disclosures. According to Ars Technica, the mistake appeared to emerge when an Adobe staffer posted a text file containing the public PGP key using Mailvelope, a common browser extension. They then forgot to trim the section of the exported text file containing the private key. The PGP system is not exactly user-friendly - it's frankly pretty cumbersome - but this is still a relatively major mistake. The original post has since been deleted and replaced with a new key, so hopefully no damage was done in the brief period of time it was live on the site. Certainly the recent weeks have seen much, much worse problems with digital security than this little incident, so probably cut Adobe a break on this one.

And Now, This:

TV Broadcasts in California Interrupted to Show “End of the World” Alert

https://www.hackread.com/tv-broadcasts-in-california-interrupted-to-show-end-of-the-world-alert/

Television viewers across the Orange County area were in for a surprise on the morning of 21st September. Most of the Californians enjoy their breakfast with TV shows, but this Thursday was different as a majority of the regular, scheduled programs were disrupted with strange, mysterious warning messages informing viewers about the upcoming invasion of extra-terrestrials and the onset of Armageddon.

According to Orange County, these weird warning messages appeared on mainstream TV channels and affected Spectrum and Cox cable users. Some of the warning videos have been uploaded on YouTube. In one of the videos, we can hear a breathless voice stating that the “space program” has been contacted with and “they are not what they claim to be.” The whole message read: “The space program made contact with… They are not what they claim to be. They have infiltrated a lot of, uh, a lot of aspects of military establishment, particularly Area 51. The disasters that are coming - the military - I’m sorry the government knows about them…”

According to Gizmodo, the audio sound has been taken from a call received back in 1997 by the host Art Bell of popular radio show Coast to Coast AM. The call was made by a person who claimed to be an ex-employee at Area51. It is amusing that this was a conspiracy-theory-themed show. There are other videos available on YouTube as well, but the warning voice is different while the emergency alert is somewhat the same as all of them inform about the onset of “extremely violent time.”

As far as the scope of impact is concerned in the latest of such cases, Cox spokesperson Todd Smith claimed that the company is not sure regarding the number of affected customers and they are trying to identify the location from where the mysterious messages were aired. As per Smith’s understanding, their system received the signals after one or more radio stations caught them while carrying out regular, monthly emergency testing. When radio stations conduct such tests, they usually send out an end tone to inform cable networks about the completion of the alerts, but it is apparent that no such signal was transmitted in this situation. Nevertheless, the emergency alert videos interrupted scheduled programming for about a minute, and viewers were stunned when they heard that the end of the world is approaching. …. However, since in the Orange County case it is unclear whether it was a hack attack or

a glitch, the story can relate to the 1987 incident in which a mysterious apocalyptic message interrupted TV broadcasts in California with ‘Violent Times Will Come’ message.

Feel free to forward the Digest to others that might be interested.
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

****