Security News Digest
July 18, 2017

For Canada's 150th anniversary of Confederation, check out
Canada's Security Scene Quiz

From a security awareness perspective, the following article is Highly Recommended for Everyone!

Why We Keep Falling for Online Phishing Scams and Downloading Viruses

http://www.cbc.ca/news/technology/phishing-online-scams-ramona-pringle-1.4205512

Why do so many of us fall prey to phishing attacks and online scams? We hear warnings about the dangers of opening untrusted files and cautionary tales of the repercussions of falling for nefarious internet hoaxes. And yet, the problem persists.

Take, for example, the opening of this viral message that spread like wildfire across Facebook last weekend: *"Please tell all the contacts in your messenger list not to accept Jayden K. Smith friendship request. He is a hacker and has the system connected to your Facebook account."* While it turned out to be a harmless hoax, what's notable is how many people fell for it and passed it on. "There have always been large scale untruths. The internet hasn't changed that," says Daniel Berkal, an ethnographer with the Palmerston Group, a boutique market research firm in Toronto. "What's really amazing here is the speed with which rumours spread."

From rumours to fake news to hoaxes like Jayden K. Smith, our social networks favour the fast, encouraging users to repost and retweet content before it passes them by in an ever-updating timeline.

The heightened pace at which untruths spread has to do with the ubiquity of the internet and the way content can be shared from one person to the next with a simple swipe or click - often without the sender even being fully aware of what he or she is sending. What's especially concerning is how often people are falling for these kinds of scams - and in some cases, with far more alarming outcomes.

According to a 2017 data breach investigation report by Verizon, 80 per cent of hacking-related breaches leveraged either stolen or weak passwords. One in 14 users were tricked into following a link or opening an attachment, without giving a second thought to what they're clicking on. The irony in the Jayden K. Smith hoax is that while the Facebook users who were fooled into passing on the message were concerned with the possibility of a dangerous hacker on the loose, they also leapt to share the message without stopping to question its validity. While no harm was done this time, often these kinds of hoaxes can be far more nefarious. **"If one does not critically think about each opportunity to click a link online, one could absolutely open oneself up to malware or other viruses,"** warned Jaigris Hodson, an assistant professor and head of the Interdisciplinary Studies program at Royal Roads University in Victoria.

Why so gullible? We hear about them all the time: the phishing scam where someone pretending to be from your company's IT department emails to notify you about a system upgrade, saying all they need to finalize the process is your password. It's the easiest way to breach a system, because the victim is fooled into literally handing over the password. Then there's malware, which could be disguised as an invoice, a receipt for a purchase from Apple, or even a LinkedIn request.

These attachments are made to look legitimate by masking as official communication from trusted sources, including banks and social networks. But once opened, they can compromise an entire computer system, in some cases by encrypting files so that the owner no longer has access to them.

"The systems that hackers use to infect your computer often rely primarily on psychological tricks - that is, tricking people into clicking on a particularly compelling link," says Hodson.

Perhaps that's partly why people fell for this particular hoax: we're so inundated by phishing attempts and malware attacks that these kinds of scams are front of mind. When a friend passes on an alert, it's understandable that someone's first instinct would be to consider the message credible and assume that their friend is passing on good information. "What we call 'gullible' is actually a combination of several interesting human traits," says Berkal. "On the simplest level, it's a way of showing that we are part of a community and that we have a genuine interest in protecting others. It communicates a helplessness to

others that is disarming and unthreatening. It showcases our honest fear for 'the unknown' and the unfamiliar."

Desire to please. It turns out that context is also key to why we fall for scams. In fact, research shows that it's not technological illiteracy that causes people to fall prey to these kinds of hoaxes. **Rather, the more regularly people use Facebook, the more likely they are to fall for a phishing scam and give away their personal information, thanks to a mixture of complacency and a desire to please**. Amy Cuddy, a business professor at Harvard University, told Business Insider in an interview last year that our decision to trust someone comes down to just two criteria: their warmth and their competence. And while her research pertains to the way we size people up when we meet them face to face, it's telling as to why we fall for hoaxes online, too.

The fact that the Jayden K. Smith hoax was passed from friend to friend through Facebook messenger was part of what lent it credibility. After all, we're inclined to trust the people we know. We may be wary of a billion dollar email offer from a Nigerian prince, but because of a feeling of warmth toward our relatives, friends and colleagues, there is a natural inclination to assume the information they pass on is credible.

And as for competence, the more legitimate something looks, or sounds, the more likely we are to be fooled. *If something looks official, with for instance, the branding of a trusted company like LinkedIn or iTunes, we're less inclined to question its validity*. Proof to that point: *"Invitation to Connect on LinkedIn" is one of the most widely used subject lines in phishing scams*. All to say, it's up to users to be vigilant and be on the lookout for tell-tale signs that something may not be what it seems. "It's important when you see anything online that you feel emotionally compelled to share, that you first exercise caution and critical thinking," Hodson said.

The following article is referred to in the article above. It was published in The Washington Post in June 2016 and is just as relevant today.

6 in 10 of You Will Share This Link Without Reading It, a New, Depressing Study Says

https://www.washingtonpost.com/news/the-intersect/wp/2016/06/16/six-in-10-of-you-will-share-this-link-without-reading-it-according-to-a-new-and-depressing-study/

On June 4, the satirical news site the Science Post published a block of “lorem ipsum” text [placeholder text only, used for layout purposes] under a frightening headline: “Study: 70% of Facebook users only read the headline of science stories before commenting.” *Nearly 46,000 people shared the post*, some of them quite earnestly - an inadvertent example, perhaps, of life imitating comedy.

Now, as if it needed further proof, the satirical headline’s been validated once again: *According to a new study by computer scientists at Columbia University and the French National Institute, 59 percent of links shared on social media have never actually been clicked: In other words, most people appear to retweet news without ever reading it*.

Worse, the study finds that these sort of blind peer-to-peer shares are really important in determining what news gets circulated and what just fades off the public radar. So your thoughtless retweets, and those of your friends, are actually shaping our shared political and cultural agendas. “People are more willing to share an article than read it,” study co-author Arnaud Legout said in a statement. “This is typical of modern information consumption. People form an opinion based on a summary, or a summary of summaries, without making the effort to go deeper.”

To verify that depressing piece of conventional Internet wisdom, Legout and his co-authors collected two data sets: the first, on all tweets containing Bit.ly-shortened links to five major news sources during a one-month period last summer; the second, on all of the clicks attached to that set of shortened links, as logged by Bit.ly, during the same period. *After cleaning and collating that data, the researchers basically found themselves with a map to how news goes viral on Twitter. And that map showed, pretty clearly, that “viral” news is widely shared - but not necessarily, you know, read. (I’m really only typing this sentence for 4 in 10 people in the audience.)*

The researchers made a few other telling observations, as well: *Most clicks to news stories, they found, were made on links shared by regular Twitter users, and not the media organization itself*. The links that users clicked were much older than we generally assume - some had been published for several days, in fact. *But most interesting, for our purposes, is this habit of sharing without clicking - a habit that, when you think about it, explains so much of the oft-demoralizing cesspool that is Internet culture*. Among the many phenomena we’d tentatively attribute, in large part, to the trend: the rise of sharebait (nee clickbait) and the general BuzzFeedification of traditional media; the Internet hoax-industrial complex, which only

seems to be growing stronger; and the utter lack of intelligent online discourse around any remotely complicated, controversial topic.
This was, incidentally, the Science Post's inspiration for its recent "lorem ipsum" gag on the subject. The editor of the site, who writes anonymously, told The Washington Post that *he had tired of seeing the sheer number of misunderstood, misrepresented or straight-up fictitious bunk that people gleefully signal-boost across the Internet*. The Science Post is run by professors and doctors, he explained: It pains them to see bad information spread this way. Unfortunately for them - and indeed, for all of us - it wouldn't seem the practice is going away.

Did You Receive a WhatsApp Subscription Ending Email or Text? Watch Out!

http://securityaffairs.co/wordpress/61057/cyber-crime/whatsapp-subscription-ending-scam.html
Researcher Graham Cluley is warning of bogus 'WhatsApp subscription ending' emails and texts. Internet users are receiving an email pretending to be from WhatsApp and warning them of the ending for an alleged WhatsApp subscription. *Although the company stopped requesting any payment since January 2016, crooks are attempting to exploit the fact that in the past, WhatsApp used to ask users to pay a fee after they had been using the service for a year*. Using this social engineering attack, crooks aim to trick users into clicking links including in the messages that might result in them handing their payment information over to attackers.
"Have you received an email claiming to come from WhatsApp that warns that you have been using the service for more than one year and that it's time to take out a subscription?" "Beware! The emails are, of course, a scam designed to trick you into clicking links that might result in you handing your payment information over to fraudsters." states the blog post published by Graham Cluley on the ESET blog. .. As usual, you should always be wary of unsolicited email messages and SMS text messages claiming to come from WhatsApp demanding payments or the verification of your account's credentials.
"You ultimately decide what links you click on, and whether you hand over your passwords and payment card details. Always think twice, because the wrong decision could prove costly." Concluded Graham Cluley.

22,000 People Agree to Clean Toilets Because Nobody Reads Terms & Conditions

https://www.bleepingcomputer.com/news/technology/22-000-people-agree-to-clean-toilets-because-nobody-reads-terms-and-conditions/
Over 22,000 users unwittingly agreed to clean public toilets when they connected to free WiFi hotspots at various UK establishments. *This was both a prank and experiment orchestrated by UK-based WiFi hotspot provider Purple. The experiment was to show that people rarely read privacy policies or terms & conditions, and usually agree to everything you put in front of them*.
Only one person noticed the quirky clauses. Purple ran the experiment for two weeks and had set up a prize for anyone who noticed the hidden clauses in the terms and conditions that users agree to before connecting to its public WiFi hotspots. Only one person noticed out of over 22,000.
Below are the clauses that Purple hid in its terms & conditions: (1) Cleansing local parks of animal waste, (2) Providing hugs to stray cats and dogs, (3) Manually relieving sewer blockages, (4) Cleaning portable lavatories at local festivals and events, (5) Painting snail shells to brighten up their existence, and (6) Scraping chewing gum off the streets.
It was only a media stunt. Purple said it does not plan to enforce any of the clauses, as this was only a media stunt to announce that they have become the first UK-based GDPR-compliant WiFi provider. The EU's GDPR (General Data Protection Regulation) is a new European law that will come into effect on May 25, 2018. The GDPR adds many provisions that protect user privacy and consumer rights for citizens of EU member states. Some of the GDPR clauses include provisions that companies active in the EU must obtain "unambiguous consent" from users before collecting any personal data that will be used for marketing purpose. Furthermore, the GDPR also dictates that companies that collect this data must provide means for users to review it at any time, and even withdraw their consent. The company must then remove the user's data.

Nasty Bug Left Thousands of Internet of Things Devices Open to Hackers

https://motherboard.vice.com/en_us/article/gybm4b/internet-of-things-camera-axis-bug
Security researchers have found a new bug that would allow hackers to take full control of several types of Internet of Things devices. Hackers could hijack thousands of Internet of Things devices

around the world, *such as security cameras, due to a flaw in a piece of software used by several major manufacturers*.
Security researchers found a bug in an open source software library that, when tested on an Internet of Things camera, allows hackers to remotely access the video feed of a camera, install a backdoor in the device, or block the camera's owner from accessing it. Researchers say it would work on other IoT devices as well - in other words, hackers would have total control over the vulnerable products, they said.
"We basically have complete control of the camera as if it was our own computer," said Stephen Ridley, founder of security startup Senrio in a phone call with Motherboard.
Ridley and his colleagues, led by a researcher who goes by M. Carlton, found the bug - which they're calling Devil's Ivy - while probing a camera manufactured by Axis, a Sweden based multinational that sells more than 200 different products to millions of customers around the world, according to its website. Axis confirmed the existence of the bug and told Motherboard that it classified it as a "critical vulnerability" that affected almost all its products.
"They were all affected, basically," Fred Juhlin, Axis's global senior consultant, told Motherboard in a phone call, adding that the company sells "millions" of devices. The researchers discovered the flaw in an open source software library called gSOAP, made by a company called Genivia. *The software is used by some members of ONVIF, an electronics industry consortium that includes Axis, as well as other giants such as Canon, Siemens, Cisco, Hitachi, and many others*. "I bet you all these other manufacturers have the same vulnerability throughout their product lines as well," Ridley told Motherboard. **"It's a vulnerability in virtually every IoT device [...] "Every kind of device you can possibly think of."**
An ONVIF spokesperson said in a statement sent via email that the consortium has notified its members of the flaw, but it's now "up to each member to handle this in the way they best see fit. Also, gSOAP "is not in any way mandated by the ONVIF specifications, but as SOAP is the base for the ONVIF API, it is possible that ONVIF members would be affected," according to the statement. HD Moore, a well-known security researcher who works for security firm Atredis Partners, estimates that the vulnerability might affect "hundreds of thousands of devices," as he told Motherboard in a direct message on Twitter." *A simple search for the term "Axis" on Shodan, an engine that scours the internet for vulnerable devices, returns around 14,000 results*. Robert van Engelen, the CEO of Genivia, said in an email that the company knows of 34 manufacturers who use their software. The good news is that, in theory, most Axis cameras should sit behind a firewall, making it harder for hackers to reach and exploit them. But it's likely that other devices made by other companies also contain the bug and could be exposed on the internet.
Still, according to van Engelen, some of the devices using gSOAP should have a setting that limits the amount of data that can be uploaded to them - a defense against distributed denial of service attacks. This setting should prevent the exploitation of the devices, something that Moore confirmed as well.
Axis issued a patch and alerted its customers through a newsletter on July 6. The problem, however, is that Axis sells to distributors who then sell the devices to the end customers, so it's now up to the customers to install the patch - if they even know about the bug. "It's very hard to reach to everyone," Juhlin admitted. And remember, while the researchers discovered the flaw in an Axis camera, the bug could be in countless other devices, made by different companies.
"Without security for all the little computerized devices that we rely on, we are standing on a house of cards." That's one of the biggest issues with the Internet of Things (IoT). Bugs exist in all kinds of software and hardware. Manufacturers have become pretty good at pushing patches to computer and cellphone users, but many IoT devices never get patches. **"IoT devices don't have standard update procedures," Ridley said. "When these devices get deployed they stay vulnerable, they don't get fixed."**
While the actual damage created by this flaw will hopefully be limited, this is yet another cautionary for the future of IoT. In the last couple of years, malicious hackers and security researchers have abused and exposed countless of vulnerable devices, showing that the companies who are taking a plunge into the IoT market might not be ready or willing to secure their own products.

Didn't Get Your Oreo Cookie Shipment? Last Month's Global Cyber Attack May Be to Blame

https://hotforsecurity.bitdefender.com/blog/didnt-get-your-oreo-cookie-shipment-last-months-global-cyber-attack-may-be-to-blame-18484.html

More and more details are emerging of the financial impact that last month's malware attack has had on major businesses. As everyone who works in IT security is all too aware, a massive malware attack crippled organisations and critical infrastructure in late June, after being distributed via a malicious automatic update in an accounts package called MeDoc. The malware (variously named as Petya, NotPetya or GoldenEye by security vendors) didn't confine itself to disrupting Ukrainian businesses, however, as it spread rapidly beyond the country's borders to impact multinational organisations across the globe.

In its annual SEC filing, international courier delivery service FedEx admitted that its systems were affected by the NotPetya/GoldenEye outbreak, with computers at TNT Express – a transportation company FedEx acquired last year – particularly badly hit:

*As of the date of this filing, all TNT Express depots, hubs and facilities are operational and most TNT services are available. Nevertheless, customers are still experiencing widespread service delays, including invoicing, and manual processes are being used to facilitate a significant portion of TNT Express operations and customer service functions…*At this time, we cannot estimate how long it will take to restore the systems that were impacted and it is reasonably possible that TNT Express will be unable to fully restore all of the affected systems and recover all of the critical business data that was encrypted by the virus. FedEx says that it is "still evaluating" the financial impact of the attack, but "it is likely that it will be material" and the company says its full-year financial results will be impacted. *FedEx says it did not have any insurance in place that would cover the impact of the malware attack*.

It's a similar story from confectionary giant Mondelez, the makers of Oreo Cookies and Cadbury chocolates, which found its offices as far away as Tasmania had fallen foul of NotPetya/GoldenEye, forcing production to halt. In its most recent update on the security incident, Mondelez said that the malware attack had been contained, but the company's revenues might be harmed: Given the timing of this significant global attack, despite our best efforts, we experienced disruption in our ability to ship and invoice during the last four days of our second quarter. There are a few markets where we have permanently lost some of that revenue due to holiday feature timing, but we expect we will be able to recognize the majority of these delayed shipments in our third quarter results.

As I discussed in an article on the Bitdefender Business Insights blog, other large businesses such as advertising giant WPP, household goods manufacturer Reckitt Benckiser, and shipping company Maersk, continued to feel the pain long past the initial impact of the GoldenEye malware outbreak. There may be no such thing as 100% security, but I really hope that more companies are adopting a layered approach to security, examining closely how they have set up their networks, whether they are controlling who has local admin rights, *and taking steps to ensure that they are able to recover quickly should disaster strike*.

751 Domains Hijacked to Redirect Traffic to Exploit Kits

https://www.bleepingcomputer.com/news/security/751-domains-hijacked-to-redirect-traffic-to-exploit-kits/

On July 7, French domain registrar Gandi lost control over 751 customer domains, which had their DNS records altered to point incoming traffic to websites hosting exploits kits. *The domain hijacking was active for only a few hours*, between 12:50 UTC and 13:30 UTC, albeit the DNS records of some domains propagated slower and they still redirected user traffic up until 18:02 UTC.

Attacker obtained one of Gandi's passwords. In a report detailing the incident, Gandi's staff say the hijack was possible because an attacker was able to get their hands on one of the passwords for a backend provided by one of Gandi's technical partners. The compromised credentials allowed Gandhi's staff and other automated systems *to connect to a backend and manage DNS details for 34 TLD extensions*. The full list of affected TLDs includes: .ASIA, .AT, .AU, .CAT, .CH, .CM, .CZ, .ES, .GR, .HK, .IM, .IT, .JP, .LA, .LI, .LT, .LV, .MG, .MS, .MU, .NL, .NU, .NZ, .PE, .PH, .PL, .RO, .RU, .SE, .SH, .SI, .SX, .UA, .XN–P1AI.

Gandi was adamant that they didn't suffer a breach, and suspect that the technical partner was to blame. "We strongly suspect they were obtained from an insecure connection to our technical partner's web portal," the Gandi team said, "the web platform in question allows access via http."

Traffic redirected to exploit kits. Email traffic left alone. Swiss cyber security firm SCRT was one of the affected entities, whose domains were hijacked by the attacker. According to its own report, traffic from its domain was redirected to exploits kits. A report from SWITCH, the national domain registrar for Switzerland and Liechtenstein, hijacked traffic reached servers hosting the Neutrino and RIG exploit kits. The attacker(s) also hijacked email DNS MX and SPF records. SCRT and Gandi say the attacker never

set up servers to intercept any email messages. The domain hijacking event also broke incoming HTTPS traffic to the affected domains.
Following the incident, Gandi reset all passwords for all the accounts it uses to manage TLD entries at country and domain-specific registrars. Last week, a security researcher discovered that he could have hijacked all .IO domains just by registering a crucial .IO domain. In April, security researchers from Kaspersky revealed that on October 22, 2016, an unknown attacker had hijacked the DNS records for a Brazilian bank's entire domains in order to steal login credentials from its customers.

Intel, Defense Bills Amended to Include Russian Hacking

http://www.securityweek.com/intel-defense-bills-amended-include-russian-hacking

Intelligence and defense policy legislation passed last week shows that the United States government is increasingly concerned about cyberattacks, particularly attacks coming from Russia. The National Defense Authorization Act (NDAA), which the House of Representatives passed on Friday, specifies the budget and expenditures of the U.S. Department of Defense (DoD). *The list of amendments for the fiscal year 2018 includes several issues related to cyber capabilities*. One of the adopted amendments requires the DoD to update its cyber strategy, to require the president to create a strategy for using offensive cyber capabilities, and providing technical assistance to NATO members. Other amendments include improvements to training, recruitment and retention of cyber personnel; the possibility to request additional resources if the House of Representatives is the victim of a cyberattack; and banning the DoD from working with telecoms firms that were "complicit" with cyberattacks attributed to North Korea. Another amendment requires the DoD to help Ukraine improve its cyber security capabilities. This comes after the country's energy sector was hit two times by damaging cyberattacks believed to have been sponsored by the Russian government.
Russia is the focus of several amendments, including the cyberattacks believed to have been launched by state-sponsored actors and the country's propaganda and disinformation initiatives. The Secretary of Defense and the Director of National Intelligence will be required to provide Congress a report on all attempts to hack DoD systems in the past two years by threat groups linked to Russia. The Intelligence Authorization Act for Fiscal Year 2018, which the House Permanent Select Committee on Intelligence unanimously advanced on Thursday, also references Russia. The Intelligence Authorization Act, which authorizes funding for the U.S. intelligence community, requires the Director of National Intelligence to submit a report assessing the most significant Russian influence campaigns aimed at foreign elections. Without specifically naming Russia, the bill also requires an unclassified advisory report on foreign counterintelligence and cybersecurity threats to federal election campaigns. This comes after the U.S. officially accused Russia of attempting to interfere with last year's presidential election. There have been several incidents recently involving the leakage of classified information from the intelligence community, including the Vault7 files by WikiLeaks. *An amendment to the Intelligence Authorization Act requires officials to submit semiannual reports on investigations into unauthorized public disclosures of classified information*.
Another hot topic covered by the Intelligence Authorization Act is related to the retention of vulnerabilities. This has been a highly debated subject, particularly after the recent WannaCry ransomware attacks, which leveraged an exploit developed by the NSA. Following the attacks, a group of lawmakers introduced a new bill, the PATCH Act, whose goal is to help the government decide whether or not it should release vulnerability details to non-federal entities.

White House Releases Sensitive Personal Information of Voters Worried about Their Sensitive Personal Information

https://www.washingtonpost.com/news/wonk/wp/2017/07/14/white-house-releases-sensitive-personal-information-of-voters-worried-about-their-sensitive-personal-information/

The White House on Thursday made public a trove of emails it received from voters offering comment on its Election Integrity Commission. The commission drew widespread criticism when it emerged into public view by asking for personal information, including addresses, partial social security numbers and party affiliation, on every voter in the country. It further outraged voters by planning to post that information publicly.
Voters directed that outrage toward the Trump White House and the voter commission, often using profanity-laced language in the 112 pages of emails released this week. "You will open up the entire voting population to a massive amount of fraud if this data is in any way released," one voter wrote.

“Many people will get their identity stolen, which will harm the economy,” wrote another. “I respectfully request, as an American-born citizen legally eligible to vote for two decades, that you leave my voter data and history alone, do not publish it, and do nothing with it,” said another.

Unfortunately for these voters and others who wrote in, the Trump administration did not redact any of their personal information from the emails before releasing them to the public. In some cases, the emails contain not only names, but email addresses, home addresses, phone numbers and places of employment of people worried about such information being made available to the public. The Washington Post is not publishing any of this information because *in most cases it does not appear that the individuals were aware their comments would be shared by the White House*. The emails were sent to the Election Integrity Commissions' email address that the administration asked U.S. secretaries of state to send data files to.

“This request is very concerning,” wrote one. “The federal government is attempting to get the name, address, birth date, political party, and social security number of every voter in the country.” That email, published by the White House, contained the sender's name and home address. “DO NOT RELEASE ANY OF MY VOTER DATA PERIOD,” wrote one voter whose name and email address was published by the White House. “Beefed up the security on this email address yet?” asked another voter whose name and email address were also published by the White House. “The request for private voter information is offensive,” wrote one voter whose name, home address and email address were published by the White House. “I removed my name from voter rolls. And I'm a Republican!” wrote one voter whose name was published by the White House.

Federal agencies often solicit and release public comments on proposed legislation. Regulations.gov, the federal government's clearing house for public comments, includes a detailed set of guidelines explaining how to submit comments, what type of personal information is collected and how that information may be used. “Some agencies may require that you include personal information, such as your name and email address, on the comment form,” the website explains. The Securities and Exchange Commission, for instance, warns commenters to “submit only information that you wish to make available publicly.” Similarly, the Federal Trade Commission tells commenters that “published comments include the commenter’s last name and state/country as well as the entire text of the comment. Please do not include any sensitive or confidential information.”

The White House does not appear to have issued any such public guidelines or warnings before many of the emails were sent. "These are public comments, similar to individuals appearing before commission to make comments and providing name before making comments," said Marc Lotter, Press Secretary to Mike Pence, in an email. "The Commission’s Federal Register notice asking for public comments and its website make clear that information 'including names and contact information' sent to this email address may be released." The Federal Register notice soliciting comments was published on July 5. The White House page was published on July 13. Approximately half of the emails published by the White House were dated prior to July 5.

Hacked Dating Site Ashley Madison Agrees to Pay $11m to US-Based Users

https://www.theguardian.com/technology/2017/jul/17/hacked-dating-site-ashley-madison-parent-company-ruby-life-inc-pay-11m-dollars-us-based-users

The parent company of hacked extramarital dating site Ashley Madison has agreed to pay an $11.2m (£8.57m) settlement to US-based users of the site, ending a two-year court battle. Ruby Life Inc agreed to pay the settlement following a number of class-action lawsuits “alleging inadequate data security practices and misrepresentations regarding Ashley Madison”. It will pay for, among other things, “payments to settlement class members who submit valid claims for alleged losses resulting from the data breach and alleged misrepresentations as described further in the proposed settlement agreement”.

In a statement, Ruby Life Inc said that it denies any wrongdoing, and reiterated that “merely because a person’s name or other information appears to have been released in the data breach does not mean that person actually was a member of Ashley Madison”.

The plaintiffs, a collection of three separate class-action lawsuits consolidated together, alleged that the company “misrepresented that they had taken reasonable steps to ensure AshleyMadison.com was secure and that the data breach resulted in the public release of certain personal information contained in AshleyMadison.com accounts and included account information of some users who had paid a fee to delete their information from the AshleyMadison.com website”.

Ruby Life Inc, formerly known as Avid Life Media, has new leadership following the departure of the executive team in April 2016. In July last year, it confirmed it was under FTC investigation for an unrelated issue, brought to light only as a result of the breach: the claim that the company used a "fembot army" to create the impression of widespread female membership.

Privacy Campaigners Criticise UK Plan for Age Checks on Porn Websites

https://www.theguardian.com/technology/2017/jul/17/age-checks-introduced-porn-websites-uk-credit-card-details

Privacy and free speech campaigners have criticised the government's plans to force pornography websites to use age checks or face being blocked. Websites flouting the new rules, which are part of the Digital Economy Act, could reportedly find that a regulator has told internet service providers to prevent access to them. Those who provide payment and other services to such sites could also be asked to impose restrictions.

Porn site users will have to provide details from a credit card, which cannot be legally issued to anyone under 18, according to the Mail on Sunday. Gambling websites use the same system of verification. The government is also expected to announce plans to appoint a regulator to police the sex websites. It is believed this could be the British Board of Film Classification - which sets age limits on films, DVDs and video games. The aim is for all online pornography to have age verification controls by April 2018 along with the appointment of a new regulatory body to oversee and enforce it, the Department for Digital, Culture, Media and Sport said.

But the plans have faced a backlash from privacy and free speech campaigners. Jim Killock, the executive director of campaign body Open Rights Group, said: "Age verification could lead to porn companies building databases of the UK's porn habits, which could be vulnerable to Ashley Madison-style hacks. "The government has repeatedly refused to ensure that there is a legal duty for age verification providers to protect the privacy of web users. "There is also nothing to ensure a free and fair market for age verification."

Killock said Open Rights was concerned that MindGeek – one of the world's biggest pornographic website operators, which owns PornHub, YouPorn and other brands and has its headquarters in Luxembourg - would become the Facebook of age verification, dominating the UK market. "They would then decide what privacy risks or profiling take place for the vast majority of UK citizens," Killock said. "Age verification risks failure as it attempts to fix a social problem with technology. In their recent manifestos, all three main political parties called for compulsory sex and relationship education in schools. Sex education would genuinely protect young people, as it would give them information and context."

Jerry Barnett, author of the book Porn Panic! and a free speech campaigner, said: "This law is the culmination of years of lobbying by a wide variety of state and private interests, and will fundamentally change the internet in the UK and possibly globally. For the first time, the government has the power to block websites, en masse, without court orders. This is a first in a democracy. "Although this appears to be just about protecting children from porn, it isn't. It will block any site that doesn't comply with strict UK content rules. Any nude image at all risks being categorised as porn, and the entire site being blocked. Current filtering systems class up to 4m websites as sexual. It's likely this regime will block the vast majority of these. And doubtless, the censorship regime will then be extended to other crimes against decency.

"Although much attention has been paid to the very dangerous snooper's charter, this law is at least as dangerous, and has had far less attention." The digital minister, Matt Hancock, who is to set to formally start the process with a written statement to the House of Commons on Monday, insisted that the measures were vital. "Now we are taking the next step to put in place the legal requirement for websites with adult content to ensure it is safely behind an age verification control," he said. "All this means that while we can enjoy the freedom of the web, the UK will have the most robust internet child protection measures of any country in the world."

Online pornography, which experts say can damage a child's development and decision-making, has been seen by 65% of 15 to 16-year-olds and 48% of 11 to 16-year-olds, according to an NSPCC report in 2016. The study also found that 28% of children may have stumbled across pornography while 19% had searched for it deliberately. Will Gardner, the chief executive of internet safety charity Childnet, said: "Protecting children from exposure, including accidental exposure, to adult content is incredibly important, given the effect it can have on young people. "Steps like this to help restrict access, alongside the provision of free parental controls and education, are key. "It is essential to help parents and careers, as

well as young people, be more aware of this risk and what they can do to prevent exposure and also to make sense of exposure if it happens."

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 Technology, Innovation and Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****