Security News Digest
August 22, 2017

Relax and Take
Dog Days of Summer quiz

Beware Phony iCloud Hacking Calls

https://www.bbb.org/vancouver-island/news-centre/bbb-scam-alerts/2017/08/beware-phony-icloud-hacking-calls/
[Aug17] Have an Apple device and iCloud account? Don't let this new scam fool you. Con artists are calling people across the United States and Canada and claiming that their iCloud accounts have been hacked. BBB [Better Business Bureau] Scam Tracker has gotten numerous reports of this scam in the past few weeks, and some targets say they've gotten 10 or more calls a day!
How the Scam Works: You get a robocall claiming to be from Apple Support. Your Caller ID may say "Apple Inc." or the name of your local Apple store. The message informs you that your iCloud account was hacked and prompts you to stay on the line and speak to an Apple support "technician." If you stay on the line, this "technician" will offer to fix your account. But first, they will need remote access to your computer. Unfortunately, allowing a scammer to access your computer can open you up to the risk of identity theft. Scam artists can install malware that records passwords or hunts for personal information, such as bank account numbers, on your computer.
Protect yourself from tech support scams: (1) **Don't ever give a stranger remote access to your machine**: Granting someone remote access to your computer permits them to install malware and access your files. Don't do it! (2) **Don't believe Caller ID:** Victims report falling for this scam because the calls appear to come from Apple Support. Scammers often spoof phone numbers, so don't believe what you see on your phone. (3) **Check out BBB Tips**: Many tech support scams use similar techniques; see bbb.org/techsupportscam/ for more advice.
For More Information: Learn more about scams impersonating Apple by visiting this page on support.apple.com.

Minor Leak Balloons Into Major Web Outage at StatsCan: Documents

http://www.cbc.ca/news/politics/statistics-canada-web-outage-shared-services-memory-it-leak-1.4249945
An incident involving a leaky air conditioner at Statistics Canada's Ottawa data centre in June mushroomed into a major outage that, among other problems, left some exporters' trucks stuck at the American border. The rapid escalation of a minor spill into a 30-hour crisis was no accidental series of escalating events, says the former head of the agency. Instead, it was the result of obsolete equipment that's the responsibility of Shared Services Canada (SSC) - the government's troubled IT department.
"The kind of careless error that brought down the data centre on June 9 is hard to excuse," said Wayne Smith, former chief statistician. "The repeated outages of Statistics Canada's internet site, now its primary method of dissemination, are becoming a national embarrassment."
Through the Access to Information Act, CBC News obtained internal emails and other documents detailing the scramble to get key systems back online over two days in June, Statistics Canada's second major outage this year. The latest chain of events began Thursday, June 8, when a contractor did routine maintenance on an air conditioner inside the data centre at the agency's Tunney's Pasture complex, about four kilometres west of Parliament Hill. Faulty work left the unit leaking overnight, and by Friday morning the water caused a small short-circuit that triggered a smoke alarm shortly before 9 a.m. ET. (The monthly Labour Force Survey, a jobs report, had been successfully posted at 8:30 a.m. ET.)
The smoke alarm, in turn, activated a power shutdown to protect the roomful of servers and other IT equipment used to run Statistics Canada's major systems, including its web services and main email. The contractor was called back to fix the leak, and at 10:15 a.m. ET technicians restored power to the data centre. Aging IT equipment, however, is susceptible to damage from sudden power fluctuations and abrupt loss of cooling. Flipping the "on" switch blew out several memory units, leaving the data centre completely non-functional again. There wasn't enough replacement memory on hand for repairs, so new

memory units had to be ordered from a supplier in Pennsylvania and trucked into Canada - a 24-hour process. The units arrived Saturday, and the data centre was finally declared functional again at 4:15 p.m. that day, or more than 30 hours after the minor leak. During the outage, the agency's heavily used web services were dark, some of its data collection was shut down, and among other services, the main email system was not available. Altogether, six key systems were out of commission, including the Canadian Automated Export Declaration (CAED) system, which Canada's exporters use to file key export documents electronically.

Winnipeg Couple Slams Walmart Canada Bank for Not Reversing $6,600 in Fraudulent Charges

http://www.cbc.ca/news/canada/manitoba/walmart-credit-card-mexico-1.4256154

A Winnipeg couple who say they were pickpocketed in Mexico are out $6,600 after someone apparently used the PIN on their credit card to make fraudulent purchases, and their credit card company says that's enough reason to not reverse the charges. Rick and Andree Jolicoeur were in Cancun in February when a routine bus trip to get groceries ended with him realizing his wallet had been stolen sometime during their travels. Since then, they've been in a months-long fight with Walmart Canada Bank, which issued their MasterCard. The company says it won't reverse the charges because it appears the person who used the card knew the four-digit PIN, and the cardholder agreement states a consumer must protect the code. "If someone has a MasterCard, they won't realize that this can happen to them - this is atrocious," Rick Jolicoeur told CBC News. "We did everything that we are supposed to do."

Credit card PINs can be stolen. Frances Lawrence, who's with the Credit Counselling Society, said a PIN can be stolen with the use of a pinhole camera at an ATM or other bank machines. Credit card information can be accessed using a device such a **"shimmer"** - a new smaller, more powerful and practically impossible to detect kind of skimmer. Shimmers fit inside a card reader and can be installed quickly by a criminal who slides it into the machine while pretending to make a purchase or withdrawal. **Once installed, the microchips on the shimmer record information from chip cards, including the PIN**. "All of the information has to be stored somewhere," she said. "Be vigilant and always make sure you know where your card is."

The Jolicoeurs say they didn't notice the wallet was missing until about two hours after they left their hotel, and when they tried to pay for groceries.

They quickly made calls to their credit card companies, cancelling their Visa and MasterCard. Rick Jolicoeur said Visa had already flagged a suspicious double charge on his card and had put a hold on it. His MasterCard had already racked up almost $7,000 in charges, including two of $3,300 from what he was later told was an "equipment rental" business. Rick Jolicoeur said the company told them to "enjoy their vacation" and "everything would be taken care of."

After they returned to Winnipeg, they learned Walmart Canada Bank refused to reverse the charges. Several phone calls to the call service centre revealed that because the card has a chip and the purchaser used the correct PIN to make the charge, Walmart Canada Bank was not liable. Walmart Canada Bank stands by its decision to not reverse the charges. "Unfortunately many consumers believe they are fully insulated from credit card fraud. The fact is the cardholder agreement holds the account holder responsible for the protection of their PIN," said spokesperson Alex Roberton in a prepared statement. "The majority of fraudulent chip and PIN transactions are not reversed if a correct PIN is used, particularly on the first try."

How Hackers are Hijacking Mobile Phone Numbers to Grab Wallets

http://nationalpost.com/news/world/how-hackers-are-hijacking-mobile-phone-numbers-to-grab-wallets/wcm/e4f75c03-6a0e-4e25-a07a-8099e02279e3

Hackers have discovered that one of the most central elements of online security - the mobile phone number - is also one of the easiest to steal. In a growing number of online attacks, hackers have been calling up Verizon, T-Mobile U.S., Sprint and AT&T and asking them to transfer control of a victim's phone number to a device under the control of the hackers. Once they get control of the phone number, they can reset the passwords on every account that uses the phone number as a security backup - as services like Google, Twitter and Facebook suggest.

"My iPad restarted, my phone restarted and my computer restarted, and that's when I got the cold sweat and was like, 'OK, this is really serious,'" said Chris Burniske, a virtual currency investor who lost control of his phone number late last year. A wide array of people have complained about being successfully

targeted by this sort of attack, including a Black Lives Matter activist and the chief technologist of the Federal Trade Commission. The commission's own data shows that the number of phone hijackings has been rising. In January 2013, there were 1,038 such incidents reported; by January 2016, that number had increased to 2,658. **But a particularly concentrated wave of attacks has hit those with the most obviously valuable online accounts: virtual currency fanatics like Burniske**. Within minutes of getting control of Burniske's phone, his attackers had changed the password on his virtual currency wallet and drained the contents - some US$150,000 at today's values.

Most victims of these attacks in the virtual currency community have not wanted to acknowledge it publicly for fear of provoking their adversaries. But in interviews, dozens of prominent people in the industry acknowledged that they had been victimized in recent months. "Everybody I know in the cryptocurrency space has gotten their phone number stolen," said Joby Weeks, a bitcoin entrepreneur. Weeks lost his phone number and about $1 million worth of virtual currency late last year, despite having asked his mobile phone provider for additional security after his wife and parents lost control of their phone numbers.

The attackers appear to be focusing on anyone who talks on social media about owning virtual currencies or anyone who is known to invest in virtual currency companies, such as venture capitalists. And virtual currency transactions are designed to be irreversible. Accounts with banks and brokerage firms and the like are not as vulnerable to these attacks because these institutions can usually reverse unintended or malicious transactions if they are caught within a few days. But the attacks are exposing a vulnerability that could be exploited against almost anyone with valuable emails or other digital files - including politicians, activists and journalists. ..The vulnerability of even sophisticated programmers and security experts to these attacks sets an unsettling precedent for when the assailants go after less technologically savvy victims. **Security experts worry that these types of attacks will become more widespread if mobile phone operators do not make significant changes to their security procedures**. "It's really highlighting the insecurity of using any kind of telephone-based security," said Michael Perklin, chief information security officer at the virtual currency exchange ShapeShift, which has seen many of its employees and customers attacked. Mobile phone carriers have said they are taking steps to head off the attacks by making it possible to add more complex personal identification numbers, or PINs, to accounts, among other steps. But these measures have not been enough to stop the spread and success of the culprits. ..A spokesman for Verizon, Richard Young, said that the company could not comment on specific cases, but that **phone porting** was not common.

… The vulnerability of phone numbers is the unintended consequence of a broad push in the security industry to institute a practice, known as two-factor authentication, that is supposed to help make accounts more secure. Many email providers and financial firms require customers to tie their online accounts to phone numbers, to verify their identity. But this system also generally allows someone with the phone number to reset the passwords on these accounts without knowing the original passwords. A hacker just hits "forgot password?" and has a new code sent to the commandeered phone. Pokornicky was online at the time his phone number was taken, and he watched as his assailants seized all his major online accounts within a few minutes. "It felt like they were one step ahead of me the whole time," he said. The speed with which the attackers move has convinced people who are investigating the hacks that the attacks are generally run by groups of hackers working together. ..Perklin and other people who have investigated recent hacks said the assailants generally succeeded by delivering sob stories about an emergency that required the phone number to be moved to a new device [social engineering] - and by trying multiple times until a gullible agent was found. "These guys will sit and call 600 times before they get through and get an agent on the line that's an idiot," Weeks said.

Tuesday: Spammers' Favorite Day of the Week

http://www.darkreading.com/endpoint/tuesday-spammers-favorite-day-of-the-week/d/d-id/1329678?

If you've ever wondered when spammers are most active, take a look at your work schedule. More than 83% of spam is sent on weekdays, with activity at its highest on Tuesday. Researchers at IBM X-Force Kassel, which operates spam honeypots and monitoring, dug into six months of data to learn about the days and times when spammers and their spam bots do the most work. The team has access to data from billions of unsolicited emails sent each year.

This research focused on data from December 2016 to June 2017. During this timeframe, the biggest day for spam was Tuesday, followed by Wednesday and Thursday. Activity dropped on weekends across geographies, which were determined using spam senders' IP addresses. Spammers have been

consistently shifting their operating hours to align with potential victims, says Limor Kessem, executive security advisor for IBM Security. As more attackers target businesses, they also adopt the traditional 9-to-5 corporate work schedule. "It goes hand-in-hand with the fact that a lot of malware spam is directed at company employees," says Kessem of the trend. "More are going after company accounts, it only makes sense they're going to be more integrated into the business week." The workday starts around 5AM UTC (1AM EST) as spammers start hitting European targets and gradually follow the sun to the United States. It wraps up around 8PM UTC (4PM EST). Some spam continues afterwards but is "likely only in the US," researchers estimate. They also noticed an "undercurrent" of spam ongoing for 24 hours per day across time zones.

While most spam is sent during the week, there are spammers and spam bots operating on weekends, Kessem notes. Those working weekends are active around the clock. Spam peaks begin at midnight, hit a second peak around 1PM (UTC), and dies down around 11PM before starting up again one hour later. India was the top spam originator in this dataset, with 30% of messages in six months, followed by South America (25%) and China (11%), respectively. Spammers tended to be more active during the day, and drop off at night, across Europe, India, and South America.

Russian spammers were most active on Thursday and Saturday, and didn't change much throughout the week. North America and China had the most consistent spam with no significant drops.

Researchers did consider that criminals could be spamming from a different country while contracting services from overseas. Spam origin is significant because threat actors typically target victims in their own country to appear legitimate and bypass spam filters. The changes in spammers' schedules coincide with another trend: the use of different malware families, such as banking Trojans and ransomware, to target businesses as opposed to sending spam to indiscriminate users' email accounts. The gangs behind Dridex, TrickBot, Qakbot, and other gang-owned malware, spam employees at times they're likely to be opening email.

Researchers detected an increasing level of sophistication as attackers bypass spam filters to target new victims. Kessem points to the Necurs botnet, which was active earlier in 2017 and generated a wealth of automated spam. Necurs has shifted its tactics in the past few months, from lacing Office documents with malicious exploits to delivering fake DocuSign files. "Typically spammers will strive to use botnets as much as they can," says Kessem of automation. "It depends on the resources they have available to them, and it depends on the botnets out there servicing spammers." Botnets are primarily used among cybercrime groups, but spammers employ a variety of techniques including mailers, traffic distribution systems, and hijacked computers to accelerate and broaden the spread of their campaigns. "The important thing is to understand the adaptation of cybercriminals," Kessem says. Spam is an old threat, but attackers are innovating and changing their tactics to keep it relevant.

The Guy Who Invented Those Annoying Password Rules Now Regrets Wasting Your Time

https://gizmodo.com/the-guy-who-invented-those-annoying-password-rules-now-1797643987

We've all been forced to do it: create a password with at least so many characters, so many numbers, so many special characters, and maybe an uppercase letter. Guess what? The guy who invented these standards nearly 15 years ago now admits that they're basically useless. He is also very sorry.

The man in question is Bill Burr, a former manager at the National Institute of Standards and Technology (NIST). In 2003, Burr drafted an eight-page guide on how to create secure passwords creatively called the "NIST Special Publication 800-63. Appendix A." This became the document that would go on to more or less dictate password requirements on everything from email accounts to login pages to your online banking portal. All those rules about using uppercase letters and special characters and numbers - those are all because of Bill.

The only problem is that Bill Burr didn't really know much about how passwords worked back in 2003, when he wrote the manual. He certainly wasn't a security expert. And now the retired 72-year-old bureaucrat wants to apologize. "Much of what I did I now regret," Bill Burr told *The Wall Street Journal* recently, admitting that his research into passwords mostly came from a white paper written in the 1980s, well before the web was even invented. "In the end, [the list of guidelines] was probably too complicated for a lot of folks to understand very well, and the truth is, it was barking up the wrong tree."

Bill is not wrong. **Simple math shows that a shorter password with wacky characters is much easier to crack than a long string of easy-to-remember words**. This classic XKCD comic shows how four simple words create a passphrase that would take a computer 550 years to guess, while a

nonsensical string of random characters would take approximately three days: This is why the latest set of NIST guidelines recommends that people create long passphrases rather than gobbledygook words like the ones Bill thought were secure.
Inevitably, you have to wonder if Bill not only feels regretful but also a little embarrassed. It's not entirely his fault either. Fifteen years ago, there was very little research into passwords and information security, while researchers can now draw on millions upon millions of examples. Bill also wasn't the only one to come up with some regrettable ideas in the early days of the web, either. Remember pop-ads, the scourge of the mid-aughts internet? The inventor of those is super sorry as well. Oh, and the confusing, unnecessary double slash in web addresses? The inventor of that idea (and the web itself) Tim Berners-Lee is also sorry. **Technology is often an exercise of trial and error**. If you get something right, like Jeff Bezos or Mark Zuckerberg have done, the rewards are sweet. If you screw up and waste years of unsuspecting internet users' time in the process, like Bill did, you get to apologize years later. We forgive you, Bill. At least some of us do.
For reference, the new NIST guidelines for passwords:
https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Skilled Bad Actors Use New Pulse Wave DDoS Attacks to Hit Multiple Targets

http://www.csoonline.com/article/3216548/security/skilled-bad-actors-using-new-pulse-wave-ddos-attacks-to-pin-down-multiple-targets.html
In a new report, Incapsula warns about a new type of ferocious DDoS attack that uses "pulse waves" to hit multiple targets. Pulse wave DDoS is a new attack tactic designed by skilled bad actors "to double the botnet's output and exploit soft spots in 'appliance first cloud second' hybrid mitigation solutions."
Comprised of a series of short-lived bursts occurring in clockwork-like succession, pulse wave assaults accounted for some of the most ferocious DDoS attacks we mitigated in the second quarter of 2017. In the most extreme cases, they lasted for days at a time and scaled as high as 350 gigabits per second (Gbps). The lack of a gradual ramp-up to peak traffic first caught Incapsula's attention, as it took only a few seconds to peak. The pattern of the attack is "highly repetitive" and consists "of one or more pulses every 10 minutes." The attacks are persistent, lasting at least an hour, but "usually for several hours or even days at a time."
The firm had "never before seen attacks of this magnitude peak with such immediacy, then be repeated with such precision." The attackers were able "to mobilize a 300Gbps botnet within a matter of seconds. This, coupled with the accurate persistence in which the pulses reoccurred, painted a picture of very skilled bad actors exhibiting a high measure of control over their attack resources."
How pulse wave DDoS attacks work and who's vulnerable. Incapsula says "pulse wave DDoS events most likely result from skilled bad actors portioning their attack resources to launch multiple assaults at the same time." The time between each pulse is likely "being used to mount a secondary assault on a different target. With effective DDoSing it's likely even more simultaneous attacks can be launched - further boosting resource utilization and the offenders' bottom line." Appliance-first hybrid mitigation solutions are vulnerable to pulse wave attacks. In fact, Incapsula said the attacks are a "worst case scenario" for networks defended by hybrid solutions.
Most DDoS attacks ramp up slowly, giving "appliance first hybrid mitigation" solutions the required several minutes to complete the cloud activation and the traffic failover. However, the first burst from a pulse wave DDoS attack immediately cuts off all syncing and congests the network pipe. After traffic spikes, the appliance and cloud cannot communicate; the appliance cannot signal the cloud to start diverting traffic. "For the pulse duration, the entire network shuts down completely. By the time it recovers, another pulse shuts it down again, ad nauseam." The lack of communication also means the appliance cannot provide the information needed to create an attack signature.
…Over the last several months, Incapsula saw pulse wave DDoS attacks used against high-value targets such as gaming and fintech companies. Unfortunately, other bad actors will grasp the benefit of splitting up attack traffic and pinning down multiple targets and then be inspired to imitate the attack; expect the range of targets to expand.

Autistic Man Hacked Sports Direct Website To Get Employment

https://www.hackread.com/autistic-man-hacked-sports-direct-website-to-get-job/

UK - The retail giant Sports Direct's website went down for 30 minutes which cost them the loss of sales of approx. £48,000 (USD 61,540) to £50,000 (USD 64,105). We already informed you that the retail giant suffered the data breach in February this year, but the latest report is quite surprising. Jason Polyik, the hacker responsible for shutting down Sports Direct, states that he did so because he wanted the firm to employ him. The loss for the company wasn't restricted to sales only as the company had to spend £15,000 in consultancy fees to get the vulnerability in their system fixed. Joe Harvey, mitigating, told Derby Telegraph that the 27-year old Polyik probably was searching for a vulnerability in their site believing that just like Google and Amazon, where hiring people who successfully identified flaws in computer systems, Sports Direct will also offer him employment. *"He is a talented graphic artist, but no-one wanted to work with him because of his social issues. He is socially awkward and on the autism spectrum. He has honed and shaped his skills over a number of years," explained Harvey.*
Sports Direct isn't the only company targeted by Polyik, but he also exploited another firm's system. In that particular hack attack, Polyik exploited the system in a way that when its chief executive turned his laptop on, a sinister laughter welcomed him with an image of The Joker from the movie Batman. The motive behind the hacking was to show how easy it was to hack the system that they have been using. Polyik conducted the hacking spree between July and September 2016.
However, his hacking obsession has landed him in jail as Polyik has been sentenced to a 10-month long prison term and also received a suspension for a year. According to Judge Peter Cooke, Polyik carried out "determined hacking" by shutting down the Sports Direct website because of which the company had to bear the loss of thousands of pounds and pay a "significant" amount for getting the problem fixed. Simon Ash, prosecution attorney, stated that Polyik accessed more than one systems on Sports Direct website due to which the site went down for 30 minutes while the second firm targeted by the 27-year old had to make changes to its server in Montreal, Canada. Mr. Ash further noted that after performing the hacks, Polyik left his mobile number and email address on both targeted websites believing that the companies would consider employing him after realizing his hacking skills. However, the companies alerted the law enforcement, and resultantly, Polyik was arrested. The Central Drive, Shirebrook resident Polyik pleaded guilty to a charge of unauthorized accessing of computer material.

Information Security Spending to Reach $93 Billion in 2018: Gartner

http://www.securityweek.com/information-security-spending-reach-93-billion-2018-gartner

Gartner has predicted that worldwide information security spending will reach $86.4 billion in 2017; a seven percent growth over the year. Spending is expected to increase to $93 billion in 2018. The fastest growing sector is security services; especially in IT outsourcing, consulting and implementation services. The only area where growth is likely to slow down is hardware support services, which are becoming less necessary with the continuing adoption of virtual appliances, public cloud and Security as a Service (SaaS) solutions. Much of the growth is thus expected to come from upgrading the IT infrastructure to a perceived more secure posture than by simply buying additional security products. "Improving security is not just about spending on new technologies," said Sid Deshpande, principal research analyst at Gartner. "As seen in the recent spate of global security incidents, doing the basics right has never been more important. Organizations can improve their security posture significantly just by addressing basic security and risk related hygiene elements like threat centric vulnerability management, centralized log management, internal network segmentation, backups and system hardening," he said.

Faster growth is likely to come from the security testing market, particularly in relation to application security testing as part of DevOps. This is no surprise to RJ Gazarek, Product Manager at Thycotic. "Thycotic research on DevOps security practices," he told *SecurityWeek*, "has shown that more than 60% of DevOps organizations are not managing credentials in scripts in any way. This is a major security problem that needs to be addressed immediately, especially as more breaches are making the news, and people realize that the way into an organization is to find the department with the weakest security practice and get to work infiltrating." Neither the growth nor the areas of growth surprise Nathan Wenzler, chief security strategist at AsTech. "If we watch how the trend of attacks has gone over the past several years, we see more and more criminals moving away from targeting servers and workstations, and toward applications and people," he explained.

…There is, however, one area in which Gartner sees actual product growth: data leak prevention (DLP). The belief is that fears over the far-reaching and severe implications of the EU General Data Protection Regulation (GDPR) is spurring, and will continue to spur, DLP purchasing through 2018. GDPR will come

into force in May 2018. From that date onward, any company anywhere in the world that handles the personal information of European citizens could be liable for a fine of up to 4% of global turnover if they do not adequately protect that data. "The EU General Data Protection Regulation (GDPR) has created renewed interest, and will drive 65 percent of data loss prevention buying decisions today through 2018," says Gartner.

How Facebook Prioritizes Privacy When You Die

https://techcrunch.com/2017/08/18/facebook-after-death/

Should your parents be able to read your Facebook messages if you die? Facebook explained why it won't let them in a post in its Hard Questions series today [Aug18] about social networking after death. Facebook admits it doesn't have all the answers, but it has come up with some decent solutions to some issues with what it calls Memorialized Profiles and a "Legacy Contact." When you pass away, once Facebook is informed, the word "Remembering" appears above your name on your profile and no one else can sign in to your account.

The Legacy Contact is a friend you select in your Manage Account Settings while you're still alive, though they're not informed until your profile is memorialized. They can pin a post atop your profile, change your profile pic, respond to friend requests or have your account removed. But Facebook explains they can't log into your account, change or delete old posts, remove friends or read your messages. Similarly, Facebook won't allow parents or anyone else to read your messages after you die. That's because "In a private conversation between two people, we assume that both people intended the messages to remain private," writes Monika Bickert, Facebook's Director of Global Policy Management. The Electronic Communications Privacy Act and Stored Communications Act may also prohibit it from sharing private communications even with parental consent.

Facebook also tries to minimize the emotional impact of losing a loved one by no longer sending birthday reminders about writing on their wall. But there are still plenty of opportunities for hurt feelings. Facebook's On This Day feature and others can surface old content from when that person was still alive, creating an unexpected experience of having to think about their death. The company has built features to enhance empathy with its users, allowing them to avoid unnecessarily seeing their exes on the app after a break-up. But it's tough to know what will be a sweet nostalgic reminder and what will be a heart-wrenching spiral into the past.

What's important is that Facebook is at least thinking and talking about these issues. Now at 2 billion users, Facebook has become a ubiquitous utility that impacts every phase of our lives. "There's a deep sense of responsibility in every part of the company," says Facebook CPO Chris Cox. "We're getting to the scale where we have to get much better about understanding how the product has been used."

Tech Companies Banishing Extremists After Charlottesville

http://www.vancouversun.com/business/tech+companies+banishing+extremists+after+charlottesville/14244863/story.html

It took bloodshed in Charlottesville to get tech companies to do what civil rights groups have been calling for for years: take a firmer stand against accounts used to promote hate and violence. In the wake of the deadly clash at a white-nationalist rally last weekend in Virginia, major companies such as Google, Facebook and PayPal are banishing a growing cadre of extremist groups and individuals for violating service terms.

What took so long? For one thing, tech companies have long seen themselves as bastions of free expression. But the Charlottesville rally seemed to have a sobering effect. It showed how easily technology can be used to organize and finance such events, and how extreme views online can translate into violence offline. "There is a difference between freedom of speech and what happened in Charlottesville," said Rashad Robinson, executive director of Color of Change, an online racial justice group. The battle of ideas is "different than people who show up with guns to terrorize communities."

Tech companies are in a bind. On one hand, they want to be open to as many people as possible so they can show them ads or provide rides, apartments or financial services. On the other hand, some of these users turn out to be white supremacists, terrorists or child molesters.

Keegan Hankes, analyst at the Southern Poverty Law Center's intelligence project, said his group has been trying for more than a year to get Facebook and PayPal to shut down these accounts. Even now, he said, the two companies are taking action only in the most extreme cases. "They have policies against violence, racism, harassment," said Hankes, whose centre monitors hate groups and extremism. "The

problem is that there has been no enforcement." Case in point: The neo-Nazi website Daily Stormer has been around since 2013. But it wasn't effectively kicked off the internet until it mocked the woman killed while protesting the white nationalists in Charlottesville.

SHIFTING LINE PayPal said groups that advocate racist views have no place on its service, but added that there is a "fine line" when it comes to balancing freedom of expression with taking a stand against violent extremism. Other companies like Facebook, Twitter and Google struggle with the same balancing act. The fine line is constantly moving and being tested. Ahead of the rally, Airbnb barred housing rentals to people it believed were travelling to participate. Before and after Charlottesville, PayPal cut off payments to groups that promote hate and violence. GoDaddy and Google yanked the domain name for Daily Stormer following the rally. Facebook, Twitter and Instagram are removing known hate groups from their services, and the music streaming service Spotify dropped what it considers hate bands.

"Companies are trying to figure out what the right thing is to do and how to do it," said Steve Jones, a professor at the University of Illinois at Chicago who focuses on communication technology. What happens from here is "partly going to depend on the individual leadership at these companies and company culture — and probably resources, too."

CAT AND MOUSE While traditional brands such as Tiki had no way of knowing that their torches were being bought for the rally, tech companies have tools to identify and ban people with extremist views. That's thanks to the troves of data they store on people and to their ability to easily switch off access to users. Airbnb users can link to social media profiles, and the company said it used its existing background checks and "input from the community" to identify users who didn't align with its standards. Yet these services also allow for anonymity, which makes their jobs more difficult. Banned people can sign up again with a different email address, something they can easily obtain anonymously.

Facebook spokeswoman Ruchika Budhraja said hate groups also know the site's policies and try to keep things just benign enough to ensure they are not in violation. For instance, the event page for the "Unite the Right" rally in Charlottesville looked fairly innocuous. Budhraja said there was nothing on the page that would suggest it was created by a hate organization. It has since been removed. Facebook's technology is designed to automatically flag posts that are on the absolute extreme and clearly violate the company's policies. They are sometimes removed before users can even see them. What Facebook can't leave to automation are posts, events and groups in that ever-growing grey area.

…The Daily Stormer and other banned groups could move to darker corners of the web, where extreme views are welcome. But this won't help with recruitment and won't allow them to disseminate their views as broadly as they could on Facebook or Twitter. "These are the platforms everyone is using," Hankes said. "They don't want to be pushed to the margins because they want influence." Because of that, the industry's efforts might just be a game of whack-a-mole, with extremist views returning, perhaps in different guises, once public outrage dies down. [article has more discussion]

Petya Ransomware Cost World's Biggest Container Ship Company Up to $300M

http://www.cbc.ca/news/technology/maersk-petya-ransomware-cyber-incident-300-million-1.4249283

The June cyberattack that paralyzed the computer systems in companies around the world is estimated to have cost the world's biggest container shipping line between $200 million and $300 million US, A.P. Moller-Maersk said Wednesday. The Copenhagen-based group, which was particularly severely affected by the attack, says the impact will first be reflected in its third-quarter results as revenue was mainly lost in July. The company says the June 27 malware attack was distributed through Ukrainian accounting software with back doors into the networks of users. It was contained the following day.

"In the last week of the quarter, we were hit by a cyberattack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July," CEO Soeren Skou said. The businesses "were significantly affected," but there was "no data breach or data loss." It said it made a loss of $264 million in the second quarter, against a profit of $118 million a year earlier. Revenue rose to $9.6 billion from $8.7 billion.

Hacker Steals $475,000 Worth of Ethereum After Breaching Enigma Project

https://www.bleepingcomputer.com/news/security/hacker-steals-475-000-worth-of-ethereum-after-breaching-enigma-project/

An unidentified hacker (or hackers) has taken control of the Enigma Project website, Slack channel, and mailing list, and tricked users into sending funds to a wrong Ethereum account. The hack took place during the company's ICO. An ICO (Initial Coin Offering) is similar to a classic IPO (Initial Public

Offering), but instead of stocks in a company, buyers get tokens in an online platform. Users can keep tokens until the issuing company decides to buy them back, or they can sell the tokens to other users for Ethereum. During the last few days, Enigma was holding an ICO pre-sale in preparation for the main token sale, set for September 11.

Hacker takes control of website, mailing list, Slack channel. The hacker took over the Enigma Project website yesterday and replaced the Ethereum pre-sale address where users had to send money to buy their ICO tokens. The attacker also gained access to the company's mailing list and sent out emails to some of Enigma's mailing list subscribers. A copy of this email is available [in the article]. In addition, the hacker also appears to have compromised the account of a Slack admin and used this access to send messages to users via the company's official Slack channel, urging users to visit the compromised site and buy tokens in the ongoing pre-sale event. A copy of the message is available [in the article], and appears to belong to Guy Zyskind, the Enigma Project's CEO. The company tried to warn users about the hack via Twitter, Facebook, and a message on its site. Users also tried to warn each other on Twitter, Reddit, and personal blogs. Hours later, the company's IT staff managed to regain access over the hacker servers. In a statement on Twitter, the Enigma Project admitted the hack.

In Ukraine, a Malware Expert and FBI Witness Who Could Blow the Whistle on Russian Hacking

http://nationalpost.com/news/world/in-ukraine-a-malware-expert-and-fbi-witness-who-could-blow-the-whistle-on-russian-hacking/wcm/9bad167c-fc65-430c-9a5d-1645de2f33a6

KIEV, Ukraine - The hacker, known only by his online alias “Profexer,” kept a low profile. He wrote computer code alone in an apartment and quietly sold his handiwork on the anonymous portion of the internet known as the dark web. Last winter, he suddenly went dark entirely. Profexer’s posts, already accessible only to a small band of fellow hackers and cybercriminals looking for software tips, blinked out in January - just days after U.S. intelligence agencies publicly identified a program he had written as one tool used in Russian hacking in the United States. U.S. intelligence agencies have determined Russian hackers were behind the electronic break-in of the Democratic National Committee.

But while Profexer’s online persona vanished, a flesh-and-blood person has emerged: a fearful man who Ukrainian police said turned himself in early this year and has now become a witness for the FBI. “I don’t know what will happen,” he wrote in one of his last messages posted on a restricted-access website before going to the police. “It won’t be pleasant. But I’m still alive.” It is the first known instance of a living witness emerging from the arid mass of technical detail that has so far shaped the investigation into the election hacking and the heated debate it has stirred. Ukrainian police declined to divulge the man’s name or other details, other than that he is living in Ukraine and has not been arrested. There is no evidence that Profexer worked, at least knowingly, for Russia’s intelligence services, but his malware apparently did.

That a hacking operation that Washington is convinced was orchestrated by Moscow would obtain malware from a source in Ukraine - perhaps the Kremlin’s most bitter enemy - sheds considerable light on the Russian security services’ modus operandi in what Western intelligence agencies say is their clandestine cyberwar against the U.S. and Europe. It does not suggest a compact team of government employees who write all their own code and carry out attacks during office hours in Moscow or St. Petersburg, but rather a far looser enterprise that draws on talent and hacking tools wherever they can be found.

….Security experts were initially left scratching their heads when the Department of Homeland Security on Dec. 29 released technical evidence of Russian hacking that seemed to point not to Russia, but rather to Ukraine. In this initial report, the department released only one sample of malware said to be an indicator of Russian state-sponsored hacking, though outside experts said a variety of malicious programs were used in Russian electoral hacking. The sample pointed to a malware program, called the PAS web shell, a hacking tool advertised on Russian-language dark web forums and used by cybercriminals throughout the former Soviet Union. The author, Profexer, is a well-regarded technical expert among hackers, spoken about with awe and respect in Kiev. He had made it available to download, free, from a website that asked only for donations, ranging from $3 to $250. The real money was made by selling customized versions and by guiding his hacker clients in its effective use. It remains unclear how extensively he interacted with the Russian hacking team.

After the Department of Homeland Security identified his creation, he quickly shut down his website and posted on a closed forum for hackers, called Exploit, that “I’m not interested in excessive attention to me

personally." Soon, a hint of panic appeared, and he posted a note saying that, six days on, he was still alive.

Unpatchable Flaw Affects Most of Today's Modern Cars

https://www.bleepingcomputer.com/news/security/unpatchable-flaw-affects-most-of-todays-modern-cars/

A flaw buried deep in the hearts of all modern cars allows an attacker with local or even remote access to a vehicle to shut down various components, including safety systems such as airbags, brakes, parking sensors, and others. The vulnerability affects the CAN (Controller Area Network) protocol that's deployed in modern cars and used to manage communications between a vehicle's internal components. The flaw was discovered by a collaborative effort of Politecnico di Milano, Linklayer Labs, and Trend Micro's Forward-looking Threat Research (FTR) team.

Researchers say this flaw is not a vulnerability in the classic meaning of the word. This is because the flaw is more of a CAN standard design choice that makes it unpatchable. Patching the issue means changing how the CAN standard works at its lowest levels. Researchers say car manufacturers can only mitigate the vulnerability via specific network countermeasures, but cannot eliminate it entirely.

"To eliminate the risk entirely, an updated CAN standard should be proposed, adopted, and implemented," researchers say. "Realistically, it would take an entire generation of vehicles for such a vulnerability to be resolved, not just a recall or an OTA (on-the-air) upgrade." Researchers say that almost any modern car in circulation today is likely affected. Bosch developed the CAN protocol in 1983, and it became an ISO standard in 1993. Nearly all modern cars use it to interconnect components. The vulnerability researchers describe is a denial of service attack. The issue can be exploited with local access by default, but if any of the car's components contains a remotely-exploitable flaw, then the CAN vulnerability can also be exploited from a remote location.

…The Department of Homeland Security's ICS-CERT has issued an alert regarding this flaw, albeit there is little to be done on the side of car makers. "The only current recommendation for protecting against this exploit is to limit access to input ports (specifically OBD-II) on automobiles," said ICS-CERT experts in an alert released last month. In the long term, researchers recommend that standardization bodies, decision makers, and car manufacturers get together to revise and improve existing standards or issue new ones in tune with our times.

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