Security News Digest
March 28, 2017

- March is Fraud Prevention Month -
Take the Top Ten Scams Quiz

Visit the Information Security Branch Fraud Prevention Month Page:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/fraud-prevention-month

B.C. Government Facebook Page Restored After Brief Hacking Monday
http://vancouversun.com/news/local-news/b-c-government-facebook-page-restored-after-brief-hacking-monday
The provincial government has tweeted an apology after its Facebook page was hit by hackers. In separate tweets posted Monday night, the government apologized for any inconvenience and said its *Facebook page had been vandalized and compromised*. A partial photo of a person in camouflage and what appeared to be Arabic script was briefly posted. The site was quickly restored and was operating normally Tuesday. *No other government sites were involved*. A statement from the government says its staff worked with Facebook to resolve the problem as quickly as possible.

Carleton University Students, Staff Urged to Change Passwords After Key-Logging Devices Found
Carleton University [Ottawa] is urging caution among staff and students after discovering potential hacking tools on a handful of classroom computers. The university says it discovered USB key-logging devices on six classroom computers across three university buildings. Carleton says staff discovered the devices last week during what it called a routine classroom inspection, but did not indicate how long they had been in place. *Keystroke-loggers capture information typed into a computer and can record usernames and passwords people use to log into various websites and programs*. The university says it will inspect classroom computers every morning and throughout the day, adding it's taking additional steps to strengthen classroom security. Carleton says it's not aware of anyone having their personal information breached because of the devices, but urges people to change passwords all the same. "These computers are used solely for instructional purposes in classrooms and do not store any university, personal or confidential information," Carleton said in an internal note to staff.

Nova Scotia Boy, 14, Charged with Sharing Child Pornography on Facebook
http://www.timescolonist.com/nova-scotia-boy-14-charged-with-sharing-child-pornography-on-facebook-1.12805237#sthash.bl1M4INX.dpuf
A 14-year-old Nova Scotia boy has been charged with sharing child pornography on Facebook. Const. Lindsey Donovan said RCMP officers arrested the young teen at home in Kingston, N.S., on Thursday after Facebook informed them that the image had been shared. The person shown in the image was not a local resident, he said. "It's not a known victim," said Donovan of the RCMP's Internet Child Exploitation Unit. "I've actually seen that image in different files before - just something someone would have got off the Internet and just gave it to somebody else. And since they gave it to somebody else on Facebook, they called us and reported it. "The boy was charged with possession and distribution of child pornography, and was released following an appearance in Kentville provincial court. He will return April 6. Donovan says it is uncommon for a youth to be charged in such cases.

Five to Survive
http://itincanadaonline.ca/index.php?option=com_content&view=article&id=2078:five-to-survive&catid=100:eric-jacksch&Itemid=629&utm_source=newsletter_3242&utm_medium=email&utm_campaign=itc-daily

Thousands of leaked CIA documents published by Wikileaks earlier this month have yet again *highlighted how much we still have to learn about protecting confidential information*. Many news articles have focused on the details of the documents, and in doing so, have missed the forest for the trees. *Here are five things Canadians need to know*.

(1) The insider threat is grossly underestimated. The vast majority of government and private-sector organizations ignore the principle of least privilege. *Many employees and contractors are granted carte blanche access to far too much information*. To make matters worse, *insider access to corporate data, especially file shares, is often not logged*. An insider copying thousands of files to their local PC should result in alarm bells, but in practice most organizations are unable to even audit access after the fact. *The belief that insiders are inherently trustworthy, and the assumption that employees are somehow less likely to leak information than contractors, defies logic*. Organizations of all sizes must start taking the insider threat seriously.

(2) Cryptography works. …According to Let's Encrypt, in December 2015, 39.5 per cent of page loads on the Web used HTTPS as measured by Firefox telemetry. By June 2016, that number was up to 45 per cent. Google continues to prod site owners to migrate to HTTPS by using it as a ranking signal, and announcing that their Chrome browser will eventually flag all HTTP sites as "insecure." While state-sponsored actors may be able to spoof targeted sites, increased TLS adoption drives up the cost and difficulty of intercepting communications.

(3) The primary target is the endpoint. ..Traditional anti-malware software is not up to the challenge, execution control products are too expensive to implement, and weak administration procedures make it too easy for intruders. *Until better solutions are developed, businesses should reflect on why employees read email, surf the web, and process sensitive corporate information on the same computers given how frequently those computers are compromised*.

(4) Software vulnerabilities are critical. ..While zero-day exploits receive a lot of attention, the reality is that *most organizations, in both public and private sectors, regularly fail to address known vulnerabilities for which patches and upgrades already exist*. Mature products make it easy to obtain technical details and enterprise-wide vulnerability metrics. All organizations need to *stop making excuses and start managing vulnerabilities*.

(5) Protecting metadata is the next challenge. Canadian law has traditionally provided protection against the unauthorized interception of communications, but *it has become increasingly clear that governments believe metadata deserves little protection*. Many encryption systems, including PGP and HTTPS, focus on protecting content, but leave metadata exposed. While content protection is important, metadata can reveal sensitive information and patterns, and it is generally easier to automatically collect and analyze. *Canadians need to start paying much more attention to protecting metadata*.

Bot Attacking Gift Card Accounts

http://www.csoonline.com/article/3184771/fraud/bot-attacking-gift-card-accounts.html

It's the gift that keeps on giving for cybercriminals. *The accounts connected to gift cards are being wiped out as quickly as a teenager with cash at a shopping mall*. *Luxury retailers, supermarkets, and major coffee distributors with gift card processing capabilities are all the target of a new widespread cybersecurity attack*.

Hackers are using a bot [botnet], dubbed GiftGhostBot, to test a list of potential gift card account numbers at a rate of 1.7 million gift card numbers per hour. *It is believed that once they correctly identify gift card numbers, they are draining balances for resale on the Dark Web*. On one retail customer site, there have been peaks of over 4 million requests per hour, nearly 10 times their normal level of traffic. The company that identified the attack, Distil Networks, has tracked activity on nearly 1,000 customer websites. In several instances, over half of the traffic on the website was on the gift card page alone, *indicating a very targeted attack*.

Fraudsters are using automation to test a list of potential account numbers and requesting each balance. If successful in obtaining the balance, fraudsters can resell the account number on the dark web or use them to purchase goods. Distil wrote on its site: "If the balance is provided, the bot operator knows that the account number exists and contains funds. *For a cyber thief, the beauty of stealing money from gift cards is that it is typically anonymous and untraceable once stolen*." GiftGhostBots are being distributed across worldwide hosting providers, mobile ISPs, and data centers, *executing JavaScript to avoid detection*.

"Like most sophisticated bot attacks, GiftGhostBot operators are moving quickly to evade detection, and any retailer that offers gift cards could be under attack at this very moment," said Rami Essaid, CEO of Distil Networks. "While it is important to understand that retailers are not exposing consumers' personal information, consumers should remain vigilant. Check gift card balances, contact retailers and ask for more information. In order to prevent resources from being drained, individuals and companies must work together to prevent further damage." ..Distil said consumers' personal identifiable information is not at risk in this scam. *The research company recommends consumers check their gift card balances regularly, and use the gift cards frequently and if they see this kind of activity to contact authorities*. [note: studies on gift cards have shown that some are never used, or carry balances for long periods, even though the gift cards were already purchased = waste of money…]

Personally Identifiable Information Found on 40 Percent of Used Devices in Largest Study To-Date

http://www.naidonline.org/nitl/en/consumer/news/5845.html

The National Association for Information Destruction (NAID) announced today [March24] the results of the largest study to date of the presence of personally identifiable information (PII) on electronic devices sold on the second hand market. *The study showed that 40 percent of devices resold in publicly-available resale channels contained PII. NAID commissioned CPR Tools, Inc. to analyze the used devices, which included used hard drives, mobile phones and tablets*.

The current state of electronic storage has made it possible for nearly every adult to carry a form of data storage device. "As data storage is included in nearly every aspect of technology today, so is the likelihood of unauthorized or unintended access to that data" states CPR Tools CEO, John Benkert. He goes on to say, **"Auction, resell, and recycling sites have created a convenient revenue stream in used devices; however, the real value is in the data that the public unintentionally leaves behind."** While there have been similar studies over the past decade, the NAID study is unique insofar as the recovery process used to locate the data on more than 250 devices was, by design, not sophisticated nor was advanced forensic training required. All methods leveraged downloadable shareware.

Robert Johnson, NAID CEO, points out that while this study's results show a decrease in data found compared to past studies, "NAID employed only basic measures to extract data; imagine if we had asked our forensics agency to actually dig!" He goes on to surmise that "40 percent is horrifying when you consider the millions of devices that are recycled annually." *PII recovered included credit card information, contact information, usernames and passwords, company and personal data, tax details, and more*. ..The study included devices that had been previously deployed in both commercial and personal environments.

Following London Attack, UK Wants WhatsApp Backdoor

http://www.pcmag.com/news/352638/following-london-attack-uk-wants-whatsapp-backdoor

Following the terror attack in London last week, UK Home Secretary Amber Rudd says government intelligence services must be able to access messages from apps like WhatsApp. "We need to make sure that organizations like WhatsApp, and ... plenty of others ... don't provide a secret place for terrorists to communicate with each other," she said in a video posted by *The Guardian*. "It used to be that people would steam open envelopes or just listen in on phones when they wanted to find out what people were doing, legally." *The individual responsible for the attack on Westminster Bridge last week reportedly used WhatsApp shortly before carrying it out*. In a statement, a WhatsApp spokesperson said: "We are horrified at the attack carried out in London and are cooperating with law enforcement as they continue their investigations."

WhatsApp and other similar services "cannot get away with saying 'we are a different situation,' they are not," according to Rudd, who has reportedly invited reps from popular messaging services to a March 30 meeting. Rudd argued for a "carefully thought through, legally covered arrangement" rather than a mandate, but did not rule out legislation if the companies refuse to comply, *The Guardian* says. That would likely require WhatsApp to lessen its security and create a backdoor for government officials, something it and its rivals have thus far refused to do. Last year, WhatsApp turned on full end-to-end encryption by default, meaning WhatsApp does not have access to specific messages.

…"Encryption is one of the most important tools governments, companies, and individuals have to promote safety and security in the new digital age. While we recognize the important work of law enforcement in keeping people safe, efforts to weaken encryption risk exposing people's information to

abuse from cybercriminals, hackers, and rogue states," WhatsApp co-founders Jan Koum and Brian Acton wrote in a 2016 blog post.

Microsoft Handed Over Email Data to UK Authorities After London Attack

http://globalnews.ca/news/3339689/microsoft-handed-over-email-data-to-uk-authorities-after-london-attack/

Microsoft revealed Monday it gave British authorities email information relating to last week's deadly attack outside the U.K. Parliament in London. Though the tech giant did not disclose how much, or what kind of information was provided, Microsoft admitted it took swift action to comply with the request, responding to authorities within 30 minutes. "Our team responded in under 30 minutes last week to verify that the legal order was valid and provided law enforcement the information that was sought," Microsoft President Brad Smith said in a statement published to the company's website. "Our global team is on call 24/7 and responds when it receives a proper and lawful order."

The revelation comes on the heels of British interior minister Amber Rudd's calls for technology companies to cooperate with law enforcement agencies to provide data related to investigations, suggesting that tech companies should stop offering "secret places for terrorists to communicate" using encrypted messages.

Local media have reported that British-born Khalid Masood sent an encrypted message via WhatsApp moments before killing four people by ploughing his car into pedestrians and fatally stabbing a policeman as he tried to get into parliament.

Google Outlines Plan to Reject Symantec's Digital Certificates

http://www.cuinfosecurity.com/google-outlines-plan-to-reject-symantecs-digital-certificates-a-9795

Google has run out of patience with Symantec's digital certificate business. It has outlined a plan that over time will have its Chrome browser reject all of Symantec's existing digital certificates. *The web giant alleges Symantec has issued thousands of digital certificates without proper verification, undermining the safety of its users*. *Google says that an investigation it launched on Jan. 19 has turned up findings that have caused "us to no longer have confidence in the certificate issuance policies and practices of Symantec over the past several years," writes Ryan Sleevi, a Google staff software engineer*.

The move holds vast and possibly costly implications for Symantec, as well as those who have bought certificates from the company. It means either new certificates would have to be purchased from other suppliers, or Symantec would have to issue replacements. **It's a big deal for organizations and businesses because of the security implications**. *Digital certificates, also referred to as Secure Sockets Layer /Transport Layer Security [SSL] certificates, are a cornerstone of internet security*. They're used to encrypt data traffic and also to verify the owner or operator of a domain name.

Symantec has grown its digital certificate business through acquisitions of VeriSign, Thawte and Equifax, among others. Two years ago, Symantec had issued 30 percent of SSL certificates by volume worldwide, according to Google.

Symantec is contesting Google's claims. In a short blog post on March 24, Symantec says that Google's public statement was "unexpected" and "irresponsible." "Google's statements about our issuance practices and the scope of our past mis-issuances are exaggerated and misleading," it says. Mozilla, which develops the Firefox browser, is mulling whether it should go the same route as Google.

…Certificate Authorities, or CAs, issue digital certificates. CA certificates are "trusted" by web browsers, *with successfully encrypted connections indicated by a green padlock or "https" in the URL window*.

Some CAs have lost their trusted status due to abuses of their systems or lax security practices. Hackers have often tried to obtain digital certificates for domains they do not own. *If an unauthorized certificate is obtained, it would be possible to intercept and decrypt traffic destined for a major web service as part of a* ***man-in-the-middle attack***. With its vast technical resources, Google has been able to react quickly when problems occur. ..Google says that its latest investigation has uncovered more than 30,000 certificates erroneously issued by Symantec. Symantec, however, contends that it only issued 127 such certificates.

…Because invalidating all certificates that fall under Symantec's purview at once would be too disruptive to those running websites and services, Google is planning a phased rejection of all of the company's certificates. [article has more details]

Apple: If Hackers Have Our Customers Passwords, They Didn't Steal Them From Us

https://hotforsecurity.bitdefender.com/blog/apple-if-hackers-have-our-customers-passwords-they-didnt-steal-them-from-us-17844.html

If you were worried that hackers might wipe millions of iPhones, Macs and iCloud accounts there's some good news today. If you remember, a group calling itself the "Turkish Crime Family" was claiming to have a stolen database of millions of Apple customer credentials, and threatening to wipe them remotely unless Apple agreed to pay a ransom demand by April 7th. As news of the Turkish Crime Family's threats began to make headlines there was a worrying silence from Apple, which can't have done much to reassure its customers. *But now, in a statement issued to Fortune, Apple has declared that its systems had not been hacked: "There have not been any breaches in any of Apple's systems including iCloud and Apple ID. The alleged list of email addresses and passwords appears to have been obtained from previously compromised third-party services."*

All of which, of course, does not necessarily mean that hackers don't have their sweaty paws on Apple customers' usernames and passwords. After all, they may have grabbed them courtesy of one of the other high profile mega-breaches (LinkedIn and Yahoo spring instantly to mind). But don't worry, if the extortionists do still follow through with their threats Apple isn't leaving its users high and dry: "Apple is actively monitoring to prevent unauthorized access to user accounts and are working with law enforcement to identify the criminals involved. *To protect against these type of attacks, we always recommend that users always use strong passwords, not use those same passwords across sites and turn on two-factor authentication*." …two-factor authentication (2FA) is the arch enemy of account hackers, because it means that they'll need more than just your password to gain access. In all likelihood, anyone attempting to break into your 2FA-protected account will simply find it too difficult - and attempt to find someone else who has been less diligent about defending their online lives. ..If you adopt best password practices you will have dramatically reduced the chances of having your account compromised and - if it ever does happen - reduced the impact that it will have on the rest of your online existence.

Meanwhile, it remains to be seen if the Turkish Crime Family follow through with their threats. Until we see evidence to the contrary, I think it might be wise to be a little skeptical – whilst still ensuring that our accounts are properly secured.

Weaponized Word Document Targets MacOS, Windows

http://www.securityweek.com/weaponized-word-document-targets-macos-windows

A recently uncovered malware campaign was found to be using a weaponized Word document that can be used to target both macOS and Windows machines, Fortinet researchers warn. The campaign relies on a macro-enabled Word file designed to execute a malicious VBA (Visual Basic for Applications) code. Up to a certain point, the code execution follows the same steps, but then it takes a different path, depending on whether it runs on macOS or Windows. *Similar to a typical macro attack, as soon as the user opens the malicious document, they are prompted to enable macros, which automatically causes the VBA code to be executed* (the VBA uses slightly modified code taken from a Metasploit framework). …[article provides the technical details on this attack] Although macro malware has been hitting Windows users for a very long time, *this is only the second attack to date to abuse malicious macros in an attempt to compromise Macs*, after another was detailed in early February. *However, this is the first time the same macro-enabled Word document has been used to target both macOS and Windows users*.

Twitter Suspended 377,000 Accounts for Promoting Terror and Extremism

https://www.hackread.com/twitter-suspends-377-000-accounts/

Twitter announced on Tuesday (20th) that it has deleted 377,000 accounts in the second half of 2016 as part of its fight against content related to extremism and terrorism. The number is 60% higher than the profiles deleted in the first half of last year, according to its transparency report. In total, the social network giant removed 636,248 accounts for the same reason in the period from August 1, 2015, to December 31, 2016. The social media networks are being urged by governments and law enforcement authorities to use their platforms to tackle individuals promoting extremism and religious violence.

The report further reveals that from the prior six-month period there has been a 7 percent increase in government requests for user data since *the company received 88 requests from governments all over the world with suspension requests, including accounts of journalists and "recognized" media organizations. However, no further action was taken in most cases*, with some exceptions for Germany and Turkey, where 88% of these requests came from.

…Lately, the social media companies are taking actions against pro-terrorism content. Facebook and Google are using automated tools to identify and remove extremist videos. Facebook is also encouraging "counter-speech," or creating and distributing content that contradicts hate speech messaging. This is a great achievement for Twitter since the company was being accused of not doing enough to take down terrorism-related content.

[US] Senate Votes to Undo Internet Privacy Rules

http://money.cnn.com/2017/03/23/technology/senate-internet-privacy/index.html

Regulations designed to give consumers more control over their online privacy appear to be dead before it was even set to begin. The Republican-controlled Senate voted along party lines Thursday to repeal Internet privacy protections that were approved by the Federal Communications Commission just days before Donald Trump won the election. *The rules, which had not yet gone into effect, would have required Internet service providers to get your permission before collecting and sharing your data on everything from web browsing history to geo-location information*. *Providers would also have been required to notify customers about the types of information collected and shared*. Jeff Flake, the Republican Senator who introduced the resolution to repeal, criticized the rules this month as "unnecessary" and "innovation-stifling regulation."

Democrats, however, argued the repeal effectively hands over the customer's personal information to the highest bidder. Many broadband providers already share some of their customers' browsing behavior with advertisers. To avoid that, customers typically have to opt out - and they might not even be aware that their information is being shared. "The American people do not want their sensitive information collected, used and sold by any third party, whether that be your broadband provider or a hacker," Sen. Edward Markey said in a speech on the floor of the Senate hours before the vote. *"This is the first action of Congress on tech policy [and] it's to take away your privacy rights with Internet service providers," says Chris Lewis, VP of Public Knowledge, a tech advocacy group*. ..The repeal is a big win for providers like AT&T and Verizon. They have bet billions on content acquisitions, which can potentially be paired with subscriber data to build up online advertising businesses to compete with the likes of Google and Facebook.

Five Ways Cybersecurity Will Suffer If Congress Repeals the FCC Privacy Rules

https://www.eff.org/deeplinks/2017/03/five-ways-cybersecurity-will-suffer-if-congress-repeals-fcc-privacy-rules

Back in October of 2016, the Federal Communications Commission [FCC] passed some pretty awesome rules that would bar your Internet provider from invading your privacy. The rules would keep Internet providers like Comcast and Time Warner Cable from doing things like selling your personal information to marketers, inserting undetectable tracking headers into your traffic, or recording your browsing history to build up a behavioral advertising profile on you - unless they got your permission first. The rules were a huge victory for U.S. Internet users who value their privacy. But last Thursday, Republicans in the Senate voted to repeal those rules. If the House of Representatives votes the same way [this week] and the rules are repealed, *it's pretty obvious that the results for Americans' privacy will be disastrous*.

But what many people don't realize is that Americans' cybersecurity is also at risk. That's because privacy and security are two sides of the same coin: privacy is about controlling who has access to information about you, and security is how you maintain that control. You usually can't break one without breaking the other, and that's especially true in this context. To show how, here are five ways repealing the FCC's privacy rules will weaken Americans' cybersecurity.

Risk #1: Snooping On Traffic (And Creating New Targets for Hackers)

In order for Internet providers to make money off your browsing history, they first have to collect that information - what sort of websites you're browsing, metadata about whom you're talking to, and maybe even what search terms you're using. Internet providers will also need to store that information somewhere, in order to build up a targeted advertising profile of you. So where's the cybersecurity risk? .. Imagine what could happen if hackers decided to target the treasure trove of personal information Internet providers start collecting. People's personal browsing history and records of their location could easily become the target of foreign hackers who want to embarrass or blackmail politicians or celebrities. To make matters worse, FCC Chairman (and former Verizon lawyer) Ajit Pai recently halted the enforcement of a [security] rule that would require Internet providers to "take reasonable measures to protect customer [personal information] from unauthorized use, disclosure, or access" - *so Internet providers won't be on the hook if their lax security exposes your data*. This would just be the fallout from passive data collection

- where your Internet provider simply spies on your data as it goes by. An even scarier risk is that Internet providers want to be able to do much more than that.

Risk #2: Erasing Encryption (And Making it Easier for Hackers to Spy On You)

Right now, your Internet provider can only spy on the portion of your traffic that *isn't* encrypted - in other words, whenever you visit a site that starts with http***s*** (instead of just http), your Internet provider *can't* see the contents of what you're browsing. ..[see article for tech explanation]

Translating from engineer-speak, that means many of the systems designed to decrypt and then re-encrypt data actually end up weakening the security of the encryption, which exposes users to increased risk of cyberattack. Simply put, if Internet providers think they can profit from looking at your encrypted data and start deploying these systems widely, we'll no longer be able to trust the security of our web browsing - and that could end up exposing everything from your email to your banking information to hackers.

Risk #3: Inserting Ads Into Your Browsing (And Opening Holes In Your Browsing Security)

One of the major threats to cybersecurity if the FCC's privacy rules are repealed comes from Internet providers inserting ads into your web browsing. Here we're talking about your Internet provider placing additional ads in the webpages you view (beyond the ones that already exist). Why is this dangerous? *Because inserting new code into a webpage in an automated fashion could break the security of the existing code in that page*. ..In other words, *security features in sites and apps you use could be broken and hackers could take advantage of that* - causing you to do anything from sending your username and password to them (while thinking it was going to the genuine website) to installing malware on your computer.

Risk #4: Zombie Supercookies (Allowing Hackers to Track You Wherever You Go)

Internet providers haven't been content with just inserting ads into our traffic - they've also tried inserting unique tracking tags as well (the way Verizon did two years ago). *For Internet providers, the motivation is to make you trackable, by inserting a unique ID number into every unencrypted connection your browser makes with a website. Then, a website that wants to know more about you (so they can decide what price to charge you for a product) can pay your Internet provider a little money and tell them what ID number they want to know about, and your Internet provider will share the desired info associated with that ID number*.

At first you might be tempted to file this one away as purely a privacy problem. But *this is a great example of how privacy and security really are two sides of the same coin*. If your Internet provider is sending these tracking tags to *every* website you visit (as Verizon did originally), then *every website you visit, and every third party embedded in websites you visit, can track you* - even if you've deleted your browser's cookies or enabled Incognito mode.

Risk #5: Spyware (Which Opens the Door for Malware)

The last risk comes from Internet providers pre-installing spyware on our devices - particularly on mobile phones, which most of us purchase directly from the company that provides our cell service, i.e. our Internet provider. …But some apps transmit those logs off of your phone as part of standard debugging procedures, assuming there's nothing sensitive in them. As a result, "keystrokes, text message content and other very sensitive information [was] in fact being transmitted from some phones on which Carrier IQ is installed to third parties." Depending on how that information was transmitted, eavesdroppers could also intercept it - meaning hackers might be able to see your username or password, without having to do any real hacking.

But the even bigger concern is that for spyware like Carrier IQ to function effectively, it has to have fairly low-level access to your phone's systems - which is engineer-speak for saying it needs to be able to see and access all the parts of your phone's operating system that would usually be secure. Thus, if hackers can find a vulnerability in the spyware, then they can use it as a sort of tunnel to get access to almost anything in your phone.

Sextortion is Scarily Common, New Study Finds

http://money.cnn.com/2016/05/11/technology/brookings-institution-sextortion-study/index.html

[from 2016] Children and women [and men] are being manipulated online in a common, scary phenomenon called 'sextortion.' *It's the practice of using personal information - often photos obtained by illicit means - to extort victims into providing more sexually explicit photos and videos*.

Take Luis Mijangos, *a sextortion offender who managed to trick women and teenage girls into downloading malware that would allow him to remotely take control of their computers. He could turn on*

their webcams and microphones and spy on them, as well as see everything they typed. Sometimes, he'd pretend to be their boyfriends in order to get them to send him pornographic materials of themselves - and then he used that to extort them more. It's a vicious cycle.
In all, Mijangos had at least 230 victims, 44 of whom were under the age of 18. He was eventually caught and got six years in prison. He has one year left of his sentence. His story is detailed in one of two new [2016] Brookings Institution [a non-profit public policy group in Washington DC] reports released Wednesday on the topic of sextortion. "It's a new form of sexual assault because you can do it without being in the person's presence - and you can do it at scale," said Senior Fellow Benjamin Wittes during a webcast discussing his findings.
He examined 78 recent cases with more than 3,000 victims, in a first-of-its-kind report on the issue. The *victims are overwhelmingly minors* (78%), and the offenders tend to have not one, but many victims. The perpetrators are all male. "This is really a men problem," Wittes said. *"Beyond the fact that they're all men, I have not been able to find any common thread."* The adult victims are women, while the child victims are both boys and girls. **Teens are particularly vulnerable, said Wittes, because of the prevalence of "sexting." This creates digital files that, if obtained by the wrong person, can be used against them**. They also don't tend to use two-step authentication or have strong passwords. But whereas revenge porn is often about public humiliation, *sextortion victims are privately being controlled. They fear coming forward to law enforcement in case images and content are publicly disclosed by perpetrators*. [they are also afraid to tell their parents]
"It's the tip of a much, much larger iceberg. We are certain that the data is incomplete .... that the problem is more widespread than we are able to capture," said Wittes. "*It's a remarkably common form of sex crime* ...These are cases of remote coercion of sex in a fashion that's closer to a sexual assault than it is to anything you would call innocent." According to his findings, there could be more than 6,000 sextortion victims. ..*Part of the intention in releasing the reports is to not only raise awareness, but also to propose a federal law to ensure that all perpetrators are charged with at least one crime*. As with other forms of internet harassment like revenge porn, there aren't specific laws against sextortion, meaning there's no uniform sentencing either.

$100 Million Phishing Scam Lands Lithuanian Man in Prison

https://hotforsecurity.bitdefender.com/blog/100-million-phishing-scam-lands-lithuanian-man-in-prison-17837.html
A 48 year-old Lithuanian man was arrested for carrying out a sophisticated phishing scam on two multinational companies, which landed him more than $100 million in banking transactions. The scam involved tricking the two companies into thinking he was representing a legitimate hardware manufacturer in Asia *and convincing them to wire money into accounts he controlled*. Forging contracts, invoices, and letters, Evaldas Rimasauskas convinced the two companies that they owed his company money and demanded payment via wire transfers. Through multiple bank accounts he controlled in Latvia, Cyprus, Slovakia, Lithuania, Hungary and Hong Kong, Rimasauskas moved the money around to avoid detection. His arrest was possible due to the cooperation of banks and the FBI that also lead to recovering an undisclosed amount of the wired transactions.
"This case should serve as a wake-up call to all companies – even the most sophisticated – that they too can be victims of phishing attacks by cyber criminals," said Acting U.S. Attorney Joon H. Kim. "And this arrest should serve as a warning to all cyber criminals that we will work to track them down, wherever they are, to hold them accountable."
The report claims that Rimasauskas's scam ran from 2013 through 2015, and he only targeted companies that dealt with multimillion-dollar transactions. While it's unclear if more than two companies fell victim to Rimasauskas's scam, he has been charged with one count of wire fraud and three counts of money laundering. ..Each of those charges carries a maximum sentence of 20 years, but it up to the judge to rule how much jail time Rimasauskas could serve, if convicted.

US Suspects North Korea in $81 Million Bangladesh Theft: Report

http://www.securityweek.com/us-suspects-north-korea-81-million-bangladesh-theft-report
US federal prosecutors suspect the North Korean government directed last year's theft of $81 million from Bangladesh's account at the New York Federal Reserve Bank, according to a media report Wednesday [March22]. Citing unnamed sources, *The Wall Street Journal* said prosecutors were developing cases showing Chinese middlemen helped the North Korean government orchestrate the enormous theft from the Bangladesh central bank. *In February 2016, thieves transferred the funds from Bangladesh's account*

at the New York Fed to accounts in the Philippines using authenticated international bank access codes in the SWIFT system, not by hacking the bank. It was unclear when or if any charges would be filed but any case might implicate North Korea without charging North Korean officials. The Justice Department and the New York Fed declined to comment on the report. The New York Fed over the past year has issued several statements, including joint statements with the central bank of Bangladesh and SWIFT, pledging to recover the stolen funds and enhance security of the payments system.

And Now, This:

Toilet Paper Hoarding Pushes Chinese Park to Install Dispensers that Recognize Faces

http://globalnews.ca/news/3324968/toilet-paper-hoarding-pushes-chinese-park-to-install-dispensers-that-recognize-faces/

A UNESCO World Heritage site in Beijing is tackling a toilet paper theft problem head-on [pun intended?] by installing machines that automatically dispense the sheets of paper after it scans the face of the user. The facial-recognition machines at the Temple of Heaven Park in Beijing dole out around 60 centimetres [24 inches] of toilet paper per person. *The same person cannot get more toilet paper until at least nine minutes have passed. The move is an effort by authorities to curb excessive toilet paper use by park visitors*. Local media reported that some people witnessed others stuffing their bags with the toilet paper – a problem the park has been facing since 2007, according to the BBC.

The *New York Times* reported that the six machines installed for a 15-day trial run, cost about $960 each and were met with both frustration and positivity by locals at the park. "It's a very bad habit," said Qin Gang of *the propensity for people to "exploit public goods" due to a history of poverty*. "Maybe we can use technology to change how people think." The BBC quoted a park spokesperson as saying visitors suffering from diarrhea or in desperate need for more toilet paper can flag ground staff, who can provide more toilet paper. In the meantime, the older manual toilet paper dispensers have been kept in place throughout the trial period. Another change for the park is that *the toilet paper has been upgraded to two ply, instead of one ply*.

According to the *Beijing Evening News*, *the trial has been successful so far, with the park seeing a 20 per cent drop in daily toilet paper use*. But the technology isn't without some sore spots. There were reports of the machines taking up to 10 times longer than they are supposed to take to scan faces, leading to user confusion. And when some local reporters went to take a look over the weekend, two of the machines were broken. *The novelty of the machines may have more people visiting the restrooms to try the machines out for themselves, which may, for the short term, outweigh the toilet paper savings*.