Security News Digest
September 05, 2017

New Month, New Quiz:
September Living Mobile Quiz

Victoria Police Warn of Extortion that Coaxes Victims Into Sending 'Compromising' Photos

http://globalnews.ca/news/3711885/victoria-police-warn-of-extortion-that-coaxes-victims-into-sending-compromising-photos/

The Victoria Police Department (VicPD) has issued a warning following a "disturbing online trend" in which individuals have been extorted into sending compromising pictures of themselves. Police said victims are contacted by an anonymous person via social media who claims to have a lot of money. The individual then promises large sums of money in exchange for compromising pictures. The anonymous person then uses those images to extort more pictures out of victims. The extortion involves threats to send the pictures to friends and family, using information found on the victims' social media profiles. Police said the suspect has successfully obtained pictures in some cases but that no money is known to have been exchanged in this scheme. "The anonymity provided by the internet means that these investigations are often very complex and difficult to investigate," said Det. Cst. Justin Munro of the Special Victims Unit. **"We encourage anyone who receives this type of request to ignore it and to report it to their local police department."** Police are urging people to ensure that their online identities are secure, to restrict the personal info they put on social media, and to ignore any "unsolicited requests for any information from unknown parties." They also urged parents to be involved in their kids' social media activities.

Is It Ever OK to Snoop On Your Child's Social Media? It Depends

http://globalnews.ca/news/3620411/is-it-ever-ok-to-snoop-on-your-childs-social-media-it-depends/

In an age where nearly one in five young Canadians (ages 15 to 29) report having experienced cyberbullying according to Statistics Canada, parents of young children and teens continue to struggle to ensure their child's safety online. And one way many parents feel is an effective method of doing so is by spying on their child's social media and Internet activity, also known as "cyber snooping." But is it something parents should be doing?

According to parenting expert Ann Douglas, there's a difference between spying and overseeing, and parents have every right to be doing the latter. "I think overseeing is a good word," she says. "I don't think we want to be sneaking around. Instead, we want to be upfront about our intentions and keeping tabs on what's going on online because that's part of our job as parents." But seeing as the issue of children and teens and cyber safety remains a baffling subject to many parents, it can be difficult for moms and dads to find that balance between spying and monitoring. So to help, Douglas offers a few tips on what adults can - and should - do to effectively and safely oversee their child's online activities.

The appropriate age. But when is it an appropriate time or age for a child to get their own social media account? Douglas says that the decision will often depend on a kid-by-kid basis, but that during the pre-teen years is often the most fitting. "Use your judgment, just like you would in deciding if your child is old enough to go to the store by themselves or hang out with friends at a mall," Douglas says. "Do you think they have the judgment, and do you think they're going to be somebody who gets in over their head or are they going to come to you for guidance if something starts to go wrong? Those are the kinds of questions I would ask."

"Even if you're worried that the pre-teen years might be a little young, it's better for them to go on social media with your guidance and supervision as opposed to sneaking online behind your back and then you not have that opportunity to help them learn," she adds.

Be honest with your child. Rather than spying on your child, be upfront with them. Being sneaky, Douglas says, can actually backfire. In fact, it can drive kids and teens to go underground, meaning they create two profiles: one for the family, and the other for friends. So it's best to set an honest tone. This starts with creating two things: your own social media profile, and house rules on social media use, Douglas says. And once you've created your own social media accounts, have your child add you as a friend.

"Be connected to them as their mom or dad but that doesn't mean you become that annoying and overbearing parent who 'likes' every single post or writes comments under everything," Douglas says. "You're there in the background, monitoring." But when creating rules, don't rush in and create a long list of rules, Douglas says. Start with a few basic rules, see how things go and then take off from there.

Don't overreact. If your child posts something that you aren't happy about, refrain from overreacting, Douglas says. "Maybe they think it's a funny joke and you don't, or they make a snarky comment that you don't like, just realize that's it's a learning process from them," she says. "They're going to have to figure some of this stuff out. So there will be times where they post something that wasn't a great choice, but that's why you're there to help guide them. They will make mistakes." While some parents may feel compelled to address their feelings on their child's social media page or elsewhere online, Douglas advises parents to refrain from doing so. ..Douglas adds not to go on the attack when you hear the child's answer. Instead, try to understand their intentions and then express your concerns and explain to them in a calm manner what they did wrong without a judging tone.

Police Seize Domain of Online Store That Stole User's Card Data

https://www.bleepingcomputer.com/news/security/police-seize-domain-of-online-store-that-stole-users-card-data/

Canadian police have seized the domain of Fazny.ca, an online electronics store that stole users' payment card data and used it to make fraudulent purchases. According to a statement from the Edmonton Police Service (EPS), its Cyber Crimes Investigation Unit started looking into the website after a user complained of fraudulent purchases appearing in his bank statements in May this year. The complainant said the victim received repeated errors while trying to buy products via the Fazny.ca store, indicating that the payment could not be processed. The victim said that shortly after, several suspicious purchases appeared on his bank account's financial statements. EPS says that following "a complex investigation," detectives "determined the complainant's information had been stolen at fazny.ca."

With a court order in hand, officers seized the site's domain to prevent other users from falling victim. EPS says the website used Facebook ads to draw in users to its store. Police says the site was a fake and crooks used computer accessory product images stolen from legitimate sites. The investigation is still ongoing, and authorities say they are trying to determine the number of affected users. Police are also asking users to step forward and make complaints if they've been on the site and seen suspicious transactions on their cards.

"Seizing the domain serves two purposes; to identify further victims and to prevent further fraud," said Const. Phil Hawkins of the Cyber Crimes Investigation Unit. "We believe others may also have been defrauded by this website and want to encourage them to report the incident(s) to their local law enforcement agency." Police only seized the site's domain, and not its server, which most likely contains the clues they're looking for.

Clark Builders Identified as Company Targeted in $11.8M MacEwan University Phishing Scam

http://globalnews.ca/news/3713350/clark-builders-identified-as-company-involved-in-11-8m-macewan-university-phishing-scam/

Clark Builders, an Edmonton construction and contracting company, said it was the company fraudsters posed as in the $11.8-million MacEwan University phishing scam. "We're not pleased with the fact that somebody was fraudulently using our logo and our brand and our information," Clark Builders president and CEO Paul Verhesen said Friday.

On Thursday, MacEwan University revealed it was defrauded of $11.8 million in an online scam. The university said a company posing as Clark Builders - a company the university has worked with for more than a decade - sent a series of fraudulent emails to the university that "convinced university staff to change electronic banking information for one of the university's major vendors." Three separate payments, ranging from $22,000 to $9.9 million, were made to the fraudsters between Aug. 10 and Aug. 19. More than $11.4 million has been traced to accounts in Canada and Hong Kong. The university said

the funds have been frozen while it works with lawyers in an attempt to recover the money. The remaining $400,000 is still unaccounted for.
The Edmonton Police Service said it became involved in the investigation on Aug. 24. Police said the MacEwan incident appears to be part of a "much larger BEC scam." BEC, or Business Email Compromise, scams are typically conducted in two ways, police said: (1) A request to change an account payable for a vendor, or (2) An e-mail is received from an executive requesting a rush wire transfer. In a rush wire transfer request, employees are typically contacted when the executive is away and the messaging implies urgency, suggesting they are unavailable by telephone.
Verhesen said Clark Builders has a very good relationship with MacEwan and contacted the university when it missed a payment. "They've always been very diligent in paying their bills on time so that's how we became aware of it," Verhesen said. "Our project team was wondering why we weren't getting paid, because it was very uncharacteristic of MacEwan to do that." Verhesen said the company came forward to make its name known publicly as a way to alert other companies of the dangers of online scams.
"There are people out there who are fraudulently trying to defraud businesses and individuals. So the message is: we should all be way more diligent in how we conduct business and transfer money and information. It's a powerful lesson for all of us to learn."

Massive Locky Ransomware Strain Hits US with Over 23 Million Emails

https://www.hackread.com/massive-locky-ransomware-strain-hits-us-with-over-23-million-emails/

Cybercriminals are becoming more and more skilled regarding technological advancement and sophisticated planning techniques. The latest ransomware campaign is a true case of how hackers can trap users and cause widespread damage by simple tweaking of an already lethal malware. According to security experts at AppRiver, the notorious Locky ransomware is back in action with utmost evilness. In the latest campaign attackers have sent out malicious Locky ransomware via a whopping 23 million infected emails.
AppRiver has posted a sample email that shows how effortlessly attackers managed to affect so many devices at once. The email has just a single sentence "download it here" and the sender's name while the subject line is also chosen randomly from a standard list. There are simple terms used in the whole email such as documents, images, photos, pictures, and scans while 'please print' is the most complex phrase.
The attackers have tried to benefit from the naivety and unsuspicious nature of a large number of internet users. When one is launching ransomware to 23 million potential targets, then the campaign is bound to claim some victims. Those who did fell prey to this trap had to pay a considerable sum to regain access to their files, which at the time of this writing was about .5 Bitcoin (more than $2300) for a single device. You can easily imagine if there were even one or two thousand compromised devices out of the 23 million then the attackers would have easily made a few million dollars.
Do not open unknown and/or spam emails The latest attack is quite dangerous. The malware traffic outrage started on Monday at around 7 a.m. CST, exactly when workers in the US arrive at offices. They were welcomed by malicious, 'extremely vague' emails sitting in their inboxes, stated AppRiver security research manager Troy Gill. The email contained a ZIP file attachment, which was a VBS (Visual Basic Script) file. Inside this attachment was another ZIP file. When the user clicked this second file, a downloader was executed, and the modified version of Locky was unleashed via "greatesthits[dot]mygoldmusic[dot com]" stated the AppRiver post.
Once downloaded, Locky ransomware starts encrypting entire data on the infected device and adds [.]lukitus to them. When encryption stage is completed, the attackers change computer's desktop background with another image on which the instructions for decryption are noted and an HTML file named "Lukitus[dot]htm" is uploaded. Unsurprisingly, the victim is asked to install TOR browser first and then sent a Darkweb link for paying the demanded ransom. When the payment is received, the victim is redirected to decryption service.
A post from AppRiver informed that the campaign was launched all across the US earlier this week and it is reportedly one of the largest ransomware attacks in 2017's second half. It is worth noting that ransomware remains the biggest cyber-threat since 2016 and its intensity has only increased over time with a 600% increase in ransomware attacks in comparison to last year. Last year Locky was the dominating malware while this year the top slot has been claimed by Cerber variants so far until Locky made a full throttle come back recently. According to Gill, the attacks haven't subsided or stopped yet, as

per the post, AppRiver detected over 5.6 million messages on Monday and still there is no information about any method to reverse the Locky ransomware strain.
Therefore, to help out the users, AppRiver suggest regular updating of their computers' software and hardware with security patches so that all the flaws and vulnerabilities are fixed timely, and ransomware or other malware exploits are prevented. In this regard, automatic software updates are your best bet, but you can also customize settings to get the newest updates regularly. Moreover, it is important to install email and web protection software too so that ransomware is prevented from entering the network. Lastly, creating data backup always works because it lets you restore your important data and you are spared from paying such hefty sum to cyber criminals.

Spambot Leaks More Than 700m Email Addresses in Massive Data Breach

https://www.theguardian.com/technology/2017/aug/30/spambot-leaks-700m-email-addresses-huge-data-breach-passwords

More than 700m email addresses, as well as a number of passwords, have leaked publicly thanks to a misconfigured Spambot, in one of the largest data breaches ever. The number of real humans' contact details contained in the dump is likely to be lower, however, due to the number of fake, malformed and repeated email addresses contained in the dataset, according to data breach experts.
Troy Hunt, an Australian computer security expert who runs the Have I Been Pwned site, which notifies subscribers when their data ends up in breaches, wrote in a blog post: "The one I'm writing about today is 711m records, which makes it the largest single set of data I've ever loaded into HIBP. Just for a sense of scale, that's almost one address for every single man, woman and child in all of Europe." It contains almost twice the records, once sanitised, than those contained in the River City Media breach from March, previously the largest breach from a spammer.
The data was available because the spammers failed to secure one of their servers, allowing any visitor to download many gigabytes of information without needing any credentials. It is impossible to know how many others besides the spammer who compiled the database have downloaded their own copies. While there are more than 700m email addresses in the data, however, it appears many of them are not linked to real accounts. Some are incorrectly scraped from the public net, while others appear to have been simply guessed at by adding words such as "sales" in front of a standard domain to generate, for example, "sales@newspaper.com".

It Still Takes 2 Minutes to Have Vulnerable IoT Devices Compromised Online

https://www.bleepingcomputer.com/news/security/it-still-takes-2-minutes-to-have-vulnerable-iot-devices-compromised-online/

Almost a year after the emergence of the Mirai botnet, smart devices are still facing a barrage of credential attacks, and a device left connected to the Internet with default credentials will be hijacked in about two minutes. This is the result of a recent experiment carried out by Johannes B. Ullrich, a member of the SANS Technology Institute. Ullrich bought an Anran DVR system and left it connected to the Internet for two days. Ullrich left the device in its default state, with the Telnet port open to external connections, and with its default credentials intact (root/xc3511). The researcher logged everything that happened on the device and connected the DVR to a remote-controlled power outlet that reset it every five minutes. Resetting the device was necessary because this action removed any malware from previous infections.
Experiment results: DVR hijacked every two minutes. Results showed that 10,143 "users" connected to the device from 1,254 different IPs during the two-day experiment. The device was left online for 45 hrs and 42 min, which meant that around every two minutes, someone connected to the device using the default credentials. Ullrich analyzed the IP addresses using Shodan, and to nobody's surprise, most of the IPs from where the logins originated were traced back to other IoT devices from vendors such as TP-Link, AvTech, Synology, and D-Link, the usual suspects when it comes to botnet cannon fodder. These devices were most likely infected with IoT malware. Mirai and most of today's IoT malware families include Telnet or SSH scanners that select random IP addresses and attempt to log in via Telnet or SSH with a list of default credentials. This type of self-spreading mechanism has been used for years, but it became very popular after the large-scale DDoS attacks carried out with the Mirai malware. After the Mirai malware source code was released online, Telnet and SSH scanners became almost prevalent.

Results similar to 2016 experiment. Last year, in the middle of all the Mirai-powered DDoS attacks, security researchers carried out a similar test by putting an IP-based security camera with default credentials online. IoT malware took control over the camera in 98 seconds (1.5 minutes) on average. Almost a year after that experiment, the security of IoT devices hasn't improved at all, and IoT malware scanners are as aggressive as they were last year.
"This problem isn't going away anytime soon," Ullrich concluded. "If people haven't heard yet about vulnerable DVRs and default passwords, then they will not read this article either." Ullrich's experiment comes on the heels of another IoT security woe after last week security researchers discovered a Pastebin list containing thousands of fully working Telnet credentials.

Cyber-Flaw Affects 745,000 Pacemakers

http://www.bbc.com/news/technology-41099867

A total of 745,000 pacemakers have been confirmed as having cyber-security issues that could let them be hacked. The Food and Drug Administration **revealed that 465,000 pacemakers in the US** were affected, in an advisory note about a fix to the problem. The pacemaker's manufacturer, Abbott, told the BBC there were a further 280,000 devices elsewhere. The flaws could theoretically be used to cause the devices to pace too quickly or run down their batteries. However, Abbott said it was not aware of any cases of this happening, adding that it would require a "highly complex set of circumstances". The Department of Homeland Security has said that an attacker would need "high skill" to exploit the vulnerabilities.
Three-minute fix. The affected pacemakers are branded as having been made by St Jude Medical, which was acquired by Abbott earlier this year. Patients are being advised to ask their doctors about an available firmware update at their next scheduled appointment. The pacemakers can receive the revised code by being placed close to a radio wave-emitting wand in a process that lasts about three minutes. Pacemakers manufactured after 28 August will come with the new firmware pre-installed.
…The benefit of allowing the pacemakers to send and receive data wirelessly is that patients can pair them with a transmitter at home that monitors the devices as they sleep and can potentially alert them to medical problems.

New Social Media Scams: Can You Tell Friend From Foe?

http://www.csoonline.com/article/3202104/phishing/new-social-media-scams-can-you-tell-friend-from-foe.html

Most security organizations have long since lost the fight to keep employees from using social media on work computers; indeed, many people now have to be on Facebook or Twitter as part of their professional duties. **The goal now is to help contain any damage from social media attacks - keeping in mind that even an attack via someone's personal account can affect their work lives**. To that end, we spoke to some security pros about scams and attack vectors that are springing up on social medial. Here are their tips for avoiding social media scams.
Social media accounts aren't a shortcut to riches. The world of con artistry has seen endless variations of the get rich quick scheme. SEO expert Bradley Shaw points to one current example on Twitter, the "Twitter cash starter kit," which promises users that they can hit it rich on the platform in unspecified ways. The key to the scam? "Victims will pay an initial fee for the kit itself by entering their debit or credit card information," says Shaw. Once the scammer has access to that information, charges quickly mount: "Their cards are charged a hidden 'membership' fee of $50 each month after initial signup. They can also make further fraudulent charges."
You can't win a contest you never entered. There are plenty of "free" too-good-to-be true enticements that can woo the unwary as well. J.A. Hitchcock, president of WHOA and WHOA-KTD, a volunteer organization that fights online harassment, notes one scam becoming increasingly popular on Snapchat. "A user gets a graphic that claims they are a winner. When they click on the graphic and fill out requested info, they're asked to download an app in order to receive a prize. That app most likely contains a virus."
Beware of wolves in brands' clothing. One particularly devious scam involves imitating a business's social media presence. "Fraudsters step up and grab unclaimed businesses on social media and act as the owner," says Julian Wong, architect at fraud detection provider DataVisor. "Someone looking to book an appointment at a spa reaches the fraudster instead of the legitimate business owner, who then takes the caller's credit card info as a 'down payment' to book or hold the appointment and then runs off with the money."

...especially if they're offering help. One scam exploits an aspect of life we've come to expect and rely on - that sometimes brand accounts seek you out, not the other way around. Companies ranging from cable providers to airlines automatically search social media to find people complaining about their services and then use support accounts to reach out and try to resolve issues. But those complaint tweets are public and those search tools are available to anybody. Philip Tully, senior data scientist at ZeroFOX, a company that detects risk on social media, outlines how this can get scary: a fake "support" account, with graphics and a bio borrowed from a real one, reaches out to someone having problems, asking them to log into a phishing site where they give their account number and password.

You reveal more about yourself than you think. A variation on this scam involves trying to assess a user's public profile to determine potential commercial interests. "A hacker can scan a Twitter feed to find out that a user posts constantly about her new puppy," explains Keeper Security CEO Darren Guccione. "The hacker then creates a phishing scam that looks like a product announcement for a portable puppy crate and targets that Twitter account."

Social platforms can't keep up. Even things that seem to have a platform's seal of approval - like a paid advertisement - hasn't necessarily been vetted; the ad-buying process is wholly automated and usually pretty cheap, and offers a great chance to get phishing links in front of targeted user demographics. "Up-front cost to the perpetrator pales in comparison to their ROI," says Tully. "On Twitter, advertisers pay only when a user engages with a promoted Tweet, and the average cost of each engagement ranges between $0.50 and $2. Perpetrators in successful phishing campaigns make off in some cases with thousands to tens of thousands of dollars in profit from things like credit card fraud or direct money withdrawal, so it only takes a single victim to make a spray and pray attack worth it."

Think twice even when you see someone you know. Lindsay Satmary, a blogger at Paperclips and Pacis, warns about profile cloning - scammers creating a duplicate profile for a real person in the hopes of getting that person's acquaintances to accept friend requests, giving them a trusted position in their social networks. Kevin Lee, trust and safety architect at fraud prevention software provider Sift Science, says that some attackers go one step further, compromising real accounts to spread malware and spam.

Expect social espionage. Once attackers have infiltrated a circle of friends or professional associates, they're in a perfect position to monitor networks. **"Hackers can use social media to infect someone within an organization, then sit on the network and monitor their internal communications,"** says Asaf Cidon, VP of content security services at Barracuda Networks. "This can be carried out by impersonating a real individual, adding them as a friend on LinkedIn, or even joining an open forum or channel on a social platform like Slack."

The endgame is often a phishing attack. "Hackers can go on LinkedIn and create fake accounts posing as a current or former employee at your company," says Kurt Wescoe, chief architect at Wombat Security Technologies. "The hacker then attempts to contact multiple people at your business, collecting small amounts of data from each employee. Each bit of info on your company - location, office hours, hierarchy, email nomenclature - could potentially add up to enough info for a successful attack." Cidon describes a specific scenario: "If hackers know the exact timing of a deal that is underway and who's in charge of authorizing the wire transfer, they're able to initiate a spear-phishing attack at the most opportune time."

"With the adversary constantly evolving, together with the massive volume of new content pouring across their platforms, social networks only have so much control over these types of problems," says ZEROFox's Tully. The bottom line in all these scams: Keep your guard up. Social media sites are designed to be as friendly as possible, but you lose many of the cues that help you tell friend from foe in real life. Being aware of these techniques can help you and your co-workers stay suspicious enough to avoid them.

Massive Wave of MongoDB Ransom Attacks Makes 26,000 New Victims

https://www.bleepingcomputer.com/news/security/massive-wave-of-mongodb-ransom-attacks-makes-26-000-new-victims/

Ransom attacks on MongoDB databases rekindled last week and over the weekend with the emergence of three new groups that hijacked over 26,000 servers, with one group hijacking 22,000. The attacks, detected by security researchers Dylan Katz and Victor Gevers, are a continuation of the so-called MongoDB Apocalypse that started in late December 2016 and continued through the first months of 2017. During those attacks, multiple hacking crews scanned the Internet for MongoDB databases left open for external connections, wiped their content, and replaced it with a ransom demand. Most of these exposed

databases were test systems, but some contained production data and a few companies ended up paying the ransom only to later find out they've been scammed and the attacker never had their data.

New wave of MongoDB hijacks discovered. Several security researchers have tracked the attacks with the help of a Google Docs spreadsheet. In total, attackers ruined over 45,000 databases, if not even more. From MongoDB, ransom attacks also spread to other server technologies, such as ElasticSearch, Hadoop, CouchDB, Cassandra, and MySQL servers. Over the spring and summer, hacking groups involved in these attacks waned off, and the number of ransomed servers went down. Last week, three new groups emerged, identified based on the email address they used in the ransom notes.

Fewer attackers but larger impact. "The amount of (new) attackers went down compared with the beginning of the year, but the destructive reach (in regards to victims) per attack went up in numbers," Gevers told Bleeping Computer in a private conversation. "So it looks like there are fewer attackers but with a larger impact." To put it in perspective, it took attackers from the first wave of MongoDB attacks nearly a month to rack up 45,000 ransomed DBs. The Cru3lty group managed half of that only last week. Gevers says that he's seen cases where the group hijacks a user's DB, the user restores a database copy from backups, and the group ransoms the server again on the same day because the victim failed to properly secure his DB.

"Now we need to study exactly what is going on here because we are missing pieces of the puzzle to keep a complete picture," Gevers told Bleeping. "Is this a lack of knowledge? Did they mess up the [MongoDB] security settings without knowing it? Are they running on older version without safe defaults and other vulnerabilities?"

It's been a busy year for crooks and security researchers alike. Gevers also said he'll also have to bring in some outside experts to help him analyze this massive wave of MongoDB hijacks. This is not because Gevers and fellow security researchers can't investigate the attacks, but because they are already busy finding and reporting other types of vulnerable devices left connected online, such as cryptocurrency miners, Arris modems, or IoT devices. Gevers, who is the chairman of the GDI Foundation, a non-profit organization working to secure devices exposed online, has been busy all year securing all sorts of devices, from AWS S3 buckets to Jenkins instances, and from computers infected with EternalBlue to GitHub repos that contain sensitive credentials.

Stolen 6M Celebrities Data from Instagram Sold on Dark Web

https://www.hackread.com/stolen-6m-celebrities-data-from-instagram-sold-on-dark-web/

The data is available on a searchable website called DoxaGram. As reported on Thursday the social media giant Instagram suffered a massive data breach in which an unknown hacker or hackers stole a trove of personal data from verified accounts (top celebrities) and ended up trading them on underground hacking forums. The data was stolen when attackers exploited a bug in an Instagram API. Now it has been revealed that hackers have set up a website with a searchable database of 6 million Instagram account. This means one can simply search for the account they are interested in and buy its details for just $10 in Bitcoin.

The site is called DoxaGram which is offering to sell anyone the data including emails and phone numbers of high-profile celebrities. … their Dark Web domain is up and running allowing users to search and buy data. ..If you are wondering, since there are no passwords available, why would someone buy this data? Well, for social engineering attacks emails and phone numbers are worth everything as attackers can search for these emails in previous data breaches like MySpace, DropBox, and LinkedIn. And if the targeted account is in the list and luck is on the attacker's side, the victim might have never changed their old password and using the same password for their Instagram and other accounts.

This will allow an attacker to hack not only the Instagram account but also those linked with the email. Moreover, an attacker can conduct **smishing (phone phishing)** on a victim and trick them into giving away their personal, social media and banking details.

Instagram is still investigating the issue, but it must be noted that days before the news of the celebrities accounts being hacked surfaced, popular singer Selena Gomez had her account hacked in which hackers leaked nude pictures of Justin Bieber.

… If you have an Instagram account, make sure to enable Two-factor authentication (2FA), never click on a suspicious link, do not open a spam or unknown email and avoid downloading the files attached to those emails.

Taringa: Over 28 Million Users' Data Exposed in Massive Data Breach

https://thehackernews.com/2017/09/taringa-data-breach-hacking.html

If you have an account on Taringa, also known as "The Latin American Reddit," your account details may have been compromised in a massive data breach that leaked login details of almost all of its over 28 million users. Taringa is a popular social network geared toward Latin American users, who create and share thousands of posts every day on general interest topics like life hacks, tutorials, recipes, reviews, and art.

The Hacker News has been informed by LeakBase, a breach notification service, who has obtained a copy of the hacked database containing details on 28,722,877 accounts, which includes usernames, email addresses and hashed passwords for Taringa users. The hashed passwords use **an ageing algorithm called MD5** – which has been considered outdated even before 2012 – that can easily be cracked, making Taringa users open to hackers. Wanna know how weak is MD5? The LeakBase team has already cracked 93.79 percent (nearly 27 Million) of hashed passwords successfully within just a few days. LeakBase has shared a dump of 4.5 million Taringa users with The Hacker News to help us verify the authenticity of the leaked database. Using email addresses in the dump, we contacted a few random Taringa users with their plain text passwords, who acknowledged the authenticity of their credentials.

...Taringa is currently sending a password reset link via an email to its users as soon as they access their account with an old password.

Trove of Private Military Contractor Job Applicants Exposed Online

https://www.hackread.com/trove-private-military-contractor-job-applicants-exposed-online/

Another day, another trove of data goes public – This time, personal and sensitive data of American citizens who applied for jobs at North Carolina-based Private Military Contractor (mercenary and security firm) TigerSwan and hundreds of those claiming "Top Secret" US government security clearances.

According to Chris Vickery, director of cyber risk research at security firm UpGuard; Resumé files of 9,402 people were found available publically on an unprotected Amazon Web Services run by a third-party vendor TalentPen who used the files for recruitment purposes until February 2017. A look at the exposed files revealed applicant names, home addresses, phone numbers, email addresses, driver's license numbers and highly sensitive job history of US military veterans, mercenaries and even Iraqi and Afghan nationals who worked alongside US forces and government institutions back in their countries.

TigerSwan was founded in 2008 by retired US Army lieutenant colonel and Delta Force operator James Reese. Since then the international security and global stability firm have provided its services during the infamous Iraq war, 2014 Sochi Olympics and Standing Rock Protests (Dakota Access Pipeline protests, DAPL). However, in May 2017, The Intercept cited leaked documents indicating that the firm used counterterrorism tactics at standing rock to "defeat pipeline insurgencies." In 2011, the firm also won a one year contract in Saudi Arabia where it provided construction and security services for the South Gate Entry Control Point, Eskan Village, Riyadh.

In their official statement, the firm has acknowledged the issue and said that: "At no time was there ever a data breach of any TigerSwan server. All resume files in TigerSwan's possession are secure. We take seriously the failure of TalentPen to ensure the security of this information and regret any inconvenience or exposure our former recruiting vendor may have caused these applicants. TigerSwan is currently exploring all recourse and options available to us and those who submitted a resumé." It is unclear for how long the data remained unprotected or whether it was accessed by anyone else other than UpGuard researchers.

Denmark and Sweden Boost Defence Ties to Fight Russian Cyber-Attacks

https://www.theguardian.com/world/2017/aug/31/denmark-and-sweden-boost-defence-ties-to-fight-russian-cyber-attacks

Denmark and Sweden are to boost defence cooperation to counter what they described as a growing threat from Russia, including from "dangerous" fake news campaigns and cyber-attacks, the two countries' defence ministers have said. Peter Hultqvist of Sweden and Claus Hjort Frederiksen of Denmark said in a statement before a meeting in Stockholm that Russian hybrid warfare – cyber-attacks, disinformation and fake news – could create uncertainty. When nations "cannot clearly distinguish false news and disinformation from what is true, we become increasingly unsafe", the ministers said, adding: "We have both been exposed to forms [of this] and want to better defend our societies in this area." This year Stockholm's Institute of International Affairs accused Russia of using fake news, false documents and disinformation in a coordinated campaign to influence public opinion and decision-making in Sweden.

The study said Sweden had been the target of “a wide array of active measures” including misleading reports on Russian state-run news networks and websites, forged documents, fabricated news items and “troll armies”.
Moscow’s main aim was to “preserve the geo-strategic status quo” by minimising NATO’s role in the wider Baltic region and keeping Sweden out of the international military alliance, the study said. Hultqvist and Frederiksen said the two countries would also increase more traditional forms of military cooperation, citing the increased presence of Russian naval vessels in the Baltic and airspace violations by Russian military aircraft.
“We already have good cooperation with Sweden and the other Nordic countries, but believe we can expand this more,” Frederiksen said. “We need to stand together when we have an unreasonable Russia moving into the Crimea and building up in our immediate neighbourhood.” Joint exercises and more cross-border exchanges of military and intelligence expertise would follow, he added.
In January, after accusations that Russian hackers had interfered with the US presidential election, Sweden’s prime minister, Stefan Löfven, told a national defence conference that he could not rule out Russia trying to influence the next Swedish elections, due in 2018.