Security News Digest
August 15, 2017

Instead of quiz questions, here is a fun game: Dog Days of Summer quiz

Free Wi-Fi Coming to B.C. Highway Rest Stops Including the Coquihalla

http://globalnews.ca/news/3668871/free-wi-fi-coming-to-highway-rest-stops-including-the-coquihalla/

The Britton Creek rest area at the summit of the Coquihalla Highway is the first rest area in B.C. to offer free Wi-Fi to the travelling public. "We are happy to bring free, public Wi-Fi to several rest areas in B.C. this year," Minister of Transportation and Infrastructure Claire Trevena said. "This helps motorists leave the phone alone while driving, and will give them the opportunity to check DriveBC and other sites at a rest area." The free Wi-Fi is being offered thanks to a partnership with ICBC and TELUS. Travelers will be able to identify which rest areas have Wi-Fi by the Wi-Fi graphic on the rest-area sign.

The free Wi-Fi is also expected to benefit the trucking sector by allowing commercial operators to rest, access washroom facilities and stay connected. The ministry has also added Wi-Fi to a number of commercial vehicle inspection centres throughout the province. The following rest area locations will offer the free Wi-Fi by the end of 2017: Britton Creek, Highway 5-67 kilometres south of Merritt, Glacier View, Highway 16-7 km north of Smithers, Taylor River, Highway 4-37 km west of Port Alberni, Galena Bay, Highway 23-49 km north of Nakusp, Mount Terry Fox, Highway 16-6km east of Tete Jaune, and Loon Lake, Highway 97C-40 km east of Merritt. More rest stop locations will be added to the list in the coming years.

6 Tips to Protect Your Personal Information When Using Public Wi-Fi

http://globalnews.ca/news/3652871/protect-personal-information-public-wi-fi-tips/

As the Internet has become a crucial part of everyday life, so too has the need to access it virtually anytime, anywhere. In fact, according to a recent survey completed by Symantec, over 66 per cent of Canadians consider access to public Wi-Fi when making travel or entertainment arrangements. Based on these numbers - and the risk of using public networks - it's important to know how to protect yourself. Here are six tips you can use to protect your personal information on public Wi-Fi networks, before and after you connect.

Before you log on:

Keep on top of security updates- As the world learned from the WannaCry ransomware attack, which started by delaying a Windows update and went on to affect hundreds of thousands of computers, staying on top of software updates is the most prudent way to protect yourself against hackers and cybercriminals. According to Forbes, "there's no magic bullet to data security," and diligently running updates for your operating system and web browser is one of the primary ways to protect yourself.

Turn off file-sharing and close shared folders on your laptop- While shared folders can be a great way to work collaboratively with colleagues, and share photos amongst family, make sure to close them and turn off file-sharing before logging onto a public network with your laptop or mobile device. A blog post from the online security company Zone Alert states that once your computer connects to a public Wi-Fi service, those folders can be viewed by anyone else on the network. To avoid any information falling into the wrong hands, users should adjust their privacy settings to ensure they are different for public and private networks.

Enable 2-factor authentication on any accounts that contain personal information- Two-factor authentication is a good option for anyone desiring a second layer of security on their physical electronic devices, including their mobile device and laptop. Enabling multiple layers of authentication on email, social networking and bank accounts can also act as an additional line of defence against cyber criminals lurking on public networks, reports The Next Web.

Use a VPN (virtual private network)- One of the most effective ways to protect your information while using public Wi-Fi is to use a Virtual Private Network (VPN). Simply download a VPN app on your phone or mobile device and log into your VPN before connecting to the Internet. A VPN reroutes your traffic

through a private, encrypted network. Kevin Haley, director of product management for security response at Symantec, explains exactly why a VPN is so useful. "What you're doing is, within a public network, creating a private network that's just for you, if you will," Haley says. "The other way it's referred to is a tunnel. It's really just making sure that your communication is surrounded by protection as you talk between where you are and wherever, the website that you're going to." According to PCMag, some of the best VPN services of 2017 include NordVPN and Private Internet Access for Android, or KeepSolid or NordVPN for iPhone.

After you log on:

Avoid signing in to accounts that contain personal information, including social media and online banking- Assuming that you've taken precautions beforehand, the next step is to be cautious after logging onto a public network. One of the best ways to play it safe is to avoid logging into any accounts that contain personal information, such as social media, work email and especially, online banking. Haley pointed out that even though a website itself might be reputable, personal information still isn't secure as long as the network is insecure. While email remains relatively low-risk, Stephen Neville, founder of the Centre for Advanced Security at the University of Victoria, noted in an email that any financial transactions should never be completed over a public network. "If you use encrypted transmissions, wireless access points offer reasonable security for low-risk activities, e.g. email, and security, that is more or less on par with a wired connection. But the security is insufficient for any higher-risk things like e-banking," Neville wrote.

Make sure the URL is encrypted- It's also helpful for users to know how to identify whether a website has taken steps to protect their information. Users can do this by checking the beginning of a URL to see whether it begins with HTTP or HTTPS. Haley explained that website URLs containing HTTPS use an SSL encryption to protect visitors to their site. Sites that use HTTPS will also show a small padlock next to the search bar. "Users just need to look for the little lock that's in the browser bar, and that tells you that your traffic is being encrypted," said Haley.

Canada Lags as Britain Moves to Give Citizens More Control Over Personal Data

http://globalnews.ca/news/3663210/social-media-posts-data-erased-britain/

The British government has proposed a bill that would allow individuals to ask for their old childhood posts to be completely erased from social media websites. The Data Protection Bill, introduced by Digital Minister Matt Hancock on Monday, seeks to give Britons more control and protection when it comes to their personal data. It's similar to the European Union's "right to be forgotten" rule, which also allows people to ask for their personal data to be removed from search engines such as Google. But one researcher says nothing similar is in the works in Canada, although it could happen in the future. "I think, in general, the European Union is ahead of us in terms of data policy," Anatoliy Gruzd, director of research at Ryerson Social Media Lab in Toronto, told Global News.

In an email, the Office of the Privacy Commissioner of Canada (OPC) told Global News that while no "right to be forgotten" law currently exists, the commission helps individuals who have concerns about their privacy being violated. It outlined its role in a January 2016 discussion paper called, "Online Reputation: What are they saying about me?" "Individuals have been turning to the OPC for assistance when they come across websites that have posted their personal information without consent," the paper reads. The OPC also launched consultations about online reputation last year, which it says will help form any future changes to rules.

The proposed U.K. law would ensure that sites such as Facebook will have to delete a user's posts if asked, unless there is a legal reason to keep it online. It would also require companies to disclose what personal data they have to the corresponding individual. In addition, it would create offences for those who break data rules. The country's information commissioner, Elizabeth Denham, praised the proposed changes in a press release.

Gruzd says there is a "lack of transparency" in the data industry, which lawmakers are trying to correct with more regulations on who is accessing data and how it's being used. "It's to give more power to people who actually created the data," he explained. While social media users can delete their posts from websites, Gruzd notes there's a "huge difference" in asking for data to be deleted. "When you delete your post, the data stays on multiple servers," Gruzd, who is also an associate professor at Ryerson University, said. He explained that most social media users have little information about who has access to their data, and the servers it exists on. While the information is disclosed in a website's terms and conditions, Gruzd points out that users rarely read it before clicking "accept." Social media websites can

then sell data to advertisers and other organizations. If these data protection rules are enforced, Gruzd says the social networks will have to adjust their policies and algorithms accordingly.

Hacker Helps Family Recover Minivan After Losing One-Of-A-Kind Car Key 

https://www.bleepingcomputer.com/news/technology/hacker-helps-family-recover-minivan-after-losing-one-of-a-kind-car-key/

After getting locked out of their Toyota Estima minivan for almost two months, a Canadian family has regained access to their car after a hacker agreed to help them. The story starts back in May this year, when John and Maria Higgins, a couple from the town of Surrey in Canada, bought a used Toyota Estima minivan imported from Japan from a local car dealership. When they picked up the car, the couple received only one car key, unlike most car owners who receive two or three. At the time, the couple didn't know the car utilized a one-of-a-kind unique car key.

A month later, on June 2, the couple went on a family road trip to the city of Victoria where they lost the key while walking around the city. John suspects he lost the keys while he bent down to tie one of his son's shoes. The family's vacation was cut short when they realized they had no keys. Things got an order of magnitude worse when their car dealership told them they couldn't replicate the lost key, and neither did their US and Japanese partners. In a desperate situation, the family turned to local press for help. Their story went viral when a local newspaper - Victoria Buzz - published their plea for help on Facebook.

"This vehicle is a Japanese import with a sophisticated immobilizer, and the key has a chip in it that can't be duplicated by North American Toyota dealers," Higgins wrote in the Facebook post. "I bought the vehicle a month ago from a dealer on the mainland who led me to believe they would be receiving another key for it from Japan in the few weeks following our purchase," Higgins also added. "This was not the case; as the manager just informed me, most cars sold by auction in Japan come with only one key and they haven't gotten anything else from the auction since."

Car remained stranded in Victoria for two weeks. The couple offered a 500 CAD reward (500 USD) for the return of their car key, but nothing came out of it. At one point, the family even tried dropping shiny objects on the ground so crows would pick them up and lead the Higgins to their nest, where they hoped to find their car key. The family's car remained stranded in a Victoria parking lot for almost two weeks before being towed back to a local mechanic's garage. Speaking to local press, the family said that several people offered to hack the minivan, but they declined their help without some kind of professional guarantee. Local mechanics advised against letting someone hack the car as there was a risk of permanently destroying the entire car. The problem came from the Toyota minivan's hybrid engine system.

It was the car dealership that provided the answer and connected the family with a trusted mechanic from the city of Richmond. The mechanic reached out to a local hacker who asked local press not to mention his real name. The hacker and the mechanic broke into the car, stripped its dashboard, and connected various wires and chips to the vehicle's main dashboard. Eventually, they were able to identify the immobilizer and reprogram it to work with new keys. The Higgins family received three new keys for their car, but not for free. In total, this whole ordeal cost the family nearly 4,500 CAD (3,500 USD) - 3,000 CAD for the manual labor, 770 CAD for programming new keys, and 760 CAD in towing costs. Fortunately for the family of four, Velocity Cars in Burnaby - the car dealership that imported and sold the used minivan - agreed to foot half the bill. The family told local press they stored one of the three new keys in a bank safety box, just to be sure this won't happen again.

Thousands of Android Apps Infected with SonicSpy Spyware

https://www.hackread.com/thousands-of-android-apps-infected-with-sonicspy-spyware/

Google Play is believed to be the best platform for downloading applications and users across the globe rely upon it. However, according to LookOut's cyber security researchers, in the past six months, over a thousand applications have been infected with spyware, and some of them are being distributed through Google Play. These infected applications are part of malware family called SonicSpy, which includes support for about 73 different remote instructions.

The deployment of infection started in February 2017. The perpetrators of this cyber-crime are based in Iraq since the account behind one of the infected Android apps Soniac was identified as iraqwebservice. It is the same account from where two other SonicSpy samples were posted on Play Store. LookOut's team found an app called Soniac available on Google Play, which appeared to be a harmless version of

Telegram messaging app but it also included malicious mechanisms. When an infected app is installed on a device, the cybercriminal behind the scheme immediately receives considerable control over it. Out of the 73 supports, some are identified in Soniac. Once the control is gained, the author of the threat can perform a variety of tasks such as discreetly recording audio, capture images/photos through the camera, send text messages to desired numbers, make outbound calls and extract information like contacts, call logs and Wi-Fi access points related info.
When installed, SonicSpy removes its launcher image and hides so that **the victim is unable to realize that the device has been infected**. Then it creates a connection to its C&C server and installs a customized version of Telegram app, which is titled su.apk and stored in the res/raw directory. Other sample apps analyzed by the research team contained similarities to another malware family SpyNote. This emerged in mid-2016, and it is believed that the same author developed both of the malware families because their coding is identical; these use dynamic DNS services and run on non-standard 2222 port. SpyNote uses customized desktop applications to inject malware into an app so that the victim can use the original functions of the infected app. It is also evident from the steady stream of SonicSpy apps that the threat actors are using similar automate-build process. Currently, researchers are not aware of the desktop tooling of the malware. It is clear that threat actors are now capable of launching spyware in official app store applications. Therefore, anyone using mobile for accessing sensitive information should be concerned.

Faulty Firmware Auto-Update Breaks Hundreds of 'Smart Locks'

http://thehackernews.com/2017/08/firmware-smart-locks.html

More features, more problems! Today, we are living in a digital age that is creating a digital headache for people by connecting every other unnecessary home appliance to the Internet. Last week, nearly hundreds of Internet-connected locks became inoperable after a faulty software update hit some models. Users of remotely accessible smart locks made by Colorado-based company LockState have taken to social media platforms including Twitter to complain that their **$469** LockState 6000i locks started to fail from last Monday, leaving the keypad entirely useless. LockState's RemoteLock 6i (6000i) is an Internet-connected smart lock that connects to your home Wi-Fi network for remote control and monitoring as well as firmware updates. LockState is even a partner with Airbnb, allowing Airbnb hosts' to give their guests entry code in order to get into hotel properties without having to share physical keys. However, last week many Airbnb customers were unable to use the built-in keypad on the smart lock devices to unlock the doors.
According to the company, **the issue occurred after its Wi-Fi enabled smart lock product range received a faulty over-the-air firmware update last week, which caused a "fatal error" in the locks, making them inoperable**. The error occurred because the firmware update was actually intended for 7000i model smart locks, but was instead mistakenly sent to 6000i products. What's worse? The smart locks now become unable to reconnect to the company's web servers, making a remote fix "impossible."

Hacker Creates Organization to Unmask Child Predators

http://money.cnn.com/2017/08/14/technology/business/innocent-lives-foundation-hackers-child-predators/index.html

Ethical hacker and social engineer Chris Hadnagy has helped get child predators off the streets. Now, he's recruiting other hackers to do the same. Last month, Hadnagy launched a non-profit organization called the Innocent Lives Foundation that works to unmask anonymous child predators online. It uses legal hacking techniques to identify these individuals and shares that information with law enforcement.
"Our goal is to locate people who produce and trade [child pornography]," he said. "Finding child pornography is sadly simplistic in itself on the open and dark web. We are trying to locate the people who are producing it. If we can get rid of the producers, and unmask them, then we can minimize the trading of it."
Hadnagy, 44, has worked in IT and security for almost two decades. He educates people on various types of social engineering, like phishing or impersonating people to try and access computer systems. Hadnagy, a father of two, said the work can take an emotional toll but he feels drawn to do something to stop what's happening online. In previous work with clients, he uncovered a handful of child exploitation cases and turned this information over to law enforcement. It led to multiple arrests, he said. "The ability to work on a couple cases where the end result is imprisonment and [protecting] children is an eye-opening experience," he said. He is currently working on 10 cases with the foundation. There are more

than six local law enforcement agencies in contact with ILF right now and three Fortune 500 companies looking to support it, Hadnagy said.
The ILF uses data from open-source intelligence, which connects the dots on publicly available data to find out someone's identity. For example, it can find an anonymous username that matches a public Instagram account. Child predators often use social media aliases to target victims. According to releases from the Department of Justice, convicted child pornographers have used platforms like Instagram, Kik, and Facebook. Many operate and distribute photos on the dark web - sites only accessible with Tor software, and not cached by search engines like Google. ILF looks for aliases and people - not images - associated with the distribution.
During the course of one current investigation, Hadnagy found a public collection of 51,000 images of child erotica. He reported it to the FBI and found the usernames of the people who published the collection. He was able to match usernames with real identities. The images are no longer online.
Hadnagy is looking for other hackers and companies to join in the mission, either by donating data, time, or money. The donations will go toward paying hackers for the time spent working to identify child predators. ILF will provide training on how to legally collect and hand over data to law enforcement.
"When I have really hard times, and there are a lot of things you can't unsee, I take a lot of time with my family," he said. "And I have a very strong belief in God, and I attach myself to that to help combat any of the negative influences of this crap."

Google Deploys Important Anti-Phishing Security Checks for iOS Gmail Users

https://hotforsecurity.bitdefender.com/blog/google-deploys-important-anti-phishing-security-checks-for-ios-gmail-users-18742.html

Google has started deploying anti-phishing security checks for users of its iOS Gmail app, the Internet giant has announced. When users tap on a link Gmail believes to be suspicious, a warning is displayed, advising users to think twice before proceeding. The rollout includes similar security checks to those offered to Android users in May, reveals the G Suite team, which provides information about new features and improvements for G Suite customers. When users receive the warning [pictured in the article], the team recommends that "you use caution before proceeding, because the link is likely unsafe. Only proceed if you're confident there's no risk." "These warnings are intended to prevent harmful phishing attacks and help you keep your account safe," the team adds.
Phishing has taken a back seat to ransomware in recent years, but that's not to say it is any less dangerous. In fact, like most other forms of malware, phishing attacks are becoming more sophisticated and harder to catch by the day. In May this year, Google users were hit with an advanced phishing scheme involving a fake Google Docs application. The spoof posed as a regular email from someone the receiver knew, like a friend or family member. It included a fake Google Docs link that, when clicked, gave hackers full access to the user's account. Then, using worm-like behavior, the fake Docs app used the account to send the same email to all the user's contacts, replicating itself.
Phishing schemes involving file-sharing and cloud storage services soared in the first quarter of 2016, taking the lead as the most-targeted sector, ahead of the retail and payment industries. Research by Bitdefender's Antispam Lab revealed at the time that one in five malicious URLs used a file-sharing service to deliver malicious payloads. **"Phishing remains a highly effective attack vector that is responsible for an increasingly significant percentage of data loss incidents affecting both end users and companies,"** Adrian Popescu, Team Leader of Bitdefender Antimalware Lab, said at the time.
In July, at the Black Hat hacker convention in Las Vegas, a security engineer working at a mobile payment company, showed how phishing scams are getting so good they can even trick tech-savvy users.
Typically, a phishing scheme impersonates a widely known website or service, like Facebook, or an email from companies like PayPal, Apple or Google, asking users to enter their credentials to download a certain file, or to validate their account. Hackers then capture the data and use it for financial gain.
Users should only click on links they can trust. If in doubt, simply hovering with the mouse pointer over the URL can reveal whether the source is what it claims to be.

Tech Firm is Fighting a Federal Demand for Data on Visitors to an Anti-Trump Website

https://www.washingtonpost.com/world/national-security/tech-company-is-fighting-a-federal-order-for-ip-addresses-to-find-visitors-to-an-anti-trump-website/2017/08/14/a65b7544-8152-11e7-b359-15a3617c767b_story.html

A Los Angeles-based tech company is resisting a federal demand for more than 1.3 million IP addresses to identify visitors to a website set up to coordinate protests on Inauguration Day - a request whose breadth the company says violates the Constitution. "What we have is a sweeping request for every single file we have" in relation to DisruptJ20.org, said Chris Ghazarian, general counsel for DreamHost, which hosts the site. "The search warrant is not only dealing with everything in relation to the website but also tons of data about people who visited it."

The request also covers emails between the site's organizers and people interested in attending the protests, any deleted messages and files, as well as subscriber information - such as names and addresses - and unpublished photos and blog posts that are stored in the site's database, according to the warrant and Ghazarian. The request, which DreamHost made public Monday, set off a storm of protest among civil liberties advocates and within the tech community. "What you're seeing is pure prosecutorial overreach by a politicized Justice Department, allowing the Trump administration to use prosecutors to silence critics," Ghazarian said.

A spokesman for the U.S. attorney's office in the District of Columbia, which sought the warrant, declined to comment. But prosecutors, in court documents, argued that the request was constitutional and there was no reason for DreamHost not to comply. The search warrant was issued July 12 by a Superior Court judge in the District of Columbia and served on DreamHost on July 17. The request marked an escalation from January when prosecutors investigating the protests asked DreamHost to preserve records and issued a subpoena for a limited set of data on the site. The company complied with both requests, Ghazarian said.

….The company said that the warrant would require them to turn over data on potentially tens of thousands of law-abiding website visitors. Mark Rumold, staff attorney for the Electronic Frontier Foundation, said that no plausible explanation exists for a search warrant of such breadth, "other than to cast a digital dragnet as broadly as possible." He said that the government appears to be investigating a conspiracy to riot, "but it's doing it in a blunt manner that does not take into account the significant First Amendment interests." Even people who were nowhere near Washington on Inauguration Day who visited the website will have their data "swept into a criminal investigation," he said. A hearing is scheduled for Friday in Superior Court before Judge Lynn Leibovitz.

North Korea-Linked Hackers Target U.S. Defense Contractors

http://www.securityweek.com/north-korea-linked-hackers-target-us-defense-contractors

The North Korea-linked cyber espionage group known as Lazarus is believed to be behind attacks targeting individuals involved with United States defense contractors, Palo Alto Networks reported on Monday. The threat actor, which has been active since at least 2009, is said to be responsible for several high-profile attacks, including the 2014 attack targeting Sony Pictures. Links have also been found to the recent WannaCry ransomware attacks. The Lazarus group, tracked by the U.S. government as Hidden Cobra and known by security firms for its Operation Blockbuster, Dark Seoul and Operation Troy campaigns, continues to be active. Recent attacks observed by Palo Alto Networks against U.S. defense contractors appear to have been launched either by this group directly or in cooperation with other cyberspies.

According to researchers, the hackers have sent out spear phishing emails containing weaponized Microsoft Office documents written in English that use macros to deliver a piece of malware. Specifically, Palo Alto has seen decoy documents describing job openings at some U.S. defense contractors. The text in these documents appears to be an exact copy, including typos, of job descriptions available on the legitimate company's website.

There are several links between these attacks and other recent campaigns, including very similar macros, decoy document details, command and control (C&C) servers, and payloads. "This reuse of macro source code, XOR keys used within the macro to decode implant payloads, and the functional overlap in the payloads the macros write to disk demonstrates the continued use of this tool set by this threat group. The use of an automated tool to build the weaponized documents would explain the common but not consistent reuse of metadata, payloads, and XOR keys within the documents," researchers explained.

Palo Alto Networks pointed out that the tools and tactics used by the group have changed only little compared to previous campaigns, despite the numerous reports describing its activities. This has led experts to believe that the Lazarus group will continue to launch targeted attacks. While the gang has been tied to several espionage and destruction campaigns, many of its recent attacks appear to have focused on financial institutions, including Bangladesh's central bank and banks in Poland.

HBO Hackers Leak Episodes for Insecure and Curb Your Enthusiasm

https://www.hackread.com/hbo-hackers-leak-episodes-for-insecure-curb-your-enthusiasm/

It looks like for now there is no end to the HBO hacking spree as earlier today [Aug14] the group of hackers behind breaching the Network's system and stealing a trove of data has leaked unaired episodes of Curb Your Enthusiasm, Insecure, Ballers, Barry and The Deuce TV series, reports the Associated Press. The latest leak does not include any new episodes of Game of Thrones but an episode of Insecure which was due to be released on Sunday. Another bad news for the network is that the leaked data also contains episodes belonging to Curb Your Enthusiasm, a popular TV series created by Larry David and due to make a comeback in October this year. Curb Your Enthusiasm was first aired back on October 15, 2000, and finished in 2011 after eight seasons.

It all started in July 2017, when hackers claimed to steal 1.5TB of data from the network and threatened to leak it online. After a few days, hackers started leaking sensitive documents belong to the company including an unreleased episode of Game of Thrones. The data also contained personal, financial and social media login credentials of HBO's Executive Vice President of Legal Affairs Viviane Eisenberg and phone numbers of GOT stars Emilia Clark, Lena Headey, and Peter Dinklage.

Furthermore, hackers demanded a multimillion dollar ransom from HBO and warned if their demands weren't met they would end up leaking more data. In reply, according to Variety; HBO was willing to pay a sum of $250,000 "bounty payment" offer to the hackers. However, after the latest leak, the media giant said that "The hacker may continue to drop bits and pieces of stolen information in an attempt to generate media attention. That's a game we're not going to participate in." It is unclear what's next from the hackers but based on their previous leaks it's easy to conclude that HBO is in big trouble.

Four Arrested in India for Leaking 'Game of Thrones' Episode

http://www.securityweek.com/four-arrested-india-leaking-game-thrones-episode

Four people have been arrested in India for leaking an episode from HBO's "Game of Thrones" television series before it was aired in the country, police said Monday. Already the most pirated show in TV history, the popular fantasy drama - which tells the story of noble families vying for the Iron Throne - has been plagued by leaks in recent weeks following the premiere of the seventh season. After receiving a complaint for a company "we investigated the case and have arrested four individuals for unauthorised publication of the fourth episode from season seven," Deputy Commissioner of Police Akbar Pathan told AFP. He said the four - accused of criminal breach of trust and computer-related offences - would be detained until August 21 amid an investigation.

The case was filed by a Mumbai-based company responsible for storing and processing the TV episodes for an app, local media said. The four arrested were company employees who possessed official credentials giving them access to the episodes, the reports added. Game of Thrones has more Emmy Awards than any narrative show in history and airs in 170 countries, with viewership figures shattering records across the world. As well as being a hit globally, it has a massive fan base in South Asia.

Vets Group Sues Pentagon for Not Protecting Private Military Records of Millions of Troops

http://www.miamiherald.com/news/nation-world/national/article166754722.html

A veterans organization is suing the Pentagon for exposing private details about troops' military service on "a truly massive scale" due to lax security on one of its websites. The lawsuit filed by Vietnam Veterans of America charges that a Defense Department website "is currently exposing private details about the military service of millions of veterans to anybody at all, anonymously, for any purpose." The shoddy security measures allow virtually anyone to access sensitive data about veterans' records by typing in a name and date of birth, which are easily available on the internet, alleges the suit, which was filed last week in federal court in New York. This gives "easy access to information about essentially all veterans or service members in the system" and thus violates the Federal Privacy Act, the lawsuit says.

The Servicemembers Civil Relief Act website, which according to the Pentagon receives more than 2.3 billion searches a year, is meant to be used by authorized institutions like banks to confirm the active duty status that entitles service members to certain protections. Instead, the information is available to con artists and scammers who can use it to impersonate government or other officials and gain veterans' trust by discussing details of their service that only authorized organizations would have.

…..Impostor fraud and identity theft aside, the group says that Vietnam veterans in particular want to keep details of their military record private, having "experienced the sting of rejection and public scorn on account of their service." Since they draw a steady, guaranteed income from the government, veterans are an attractive target for scammers. The numbers have increased in recent years, from 58,175 complaints by veterans in 2014 to 69,801 in 2016, according to the Federal Trade Commission's Consumer Sentinel Network. "Veterans are disproportionately targeted by scammers and identity thieves," Vietnam Veterans of America President John Rowan said in a statement. The Pentagon "is fueling the problem by leaving veterans' private information easily accessible on the internet (and) has refused to properly secure veterans' information," he said. "We are asking a court to order them to do so."
The Defense Department has refused to make any changes since being alerted about the problems with the site, the suit says. It points out that the Defense Department could implement a strict user registration or online verification system, which are used by the Social Security Administration and the Department of Homeland Security.