Chelsea Lovgren – “Home IoT Attacks” (September 29, 2020)

I learned of Internet of Things freshman year in my information technology class and never truly understood what it is. Lovgren helped define IoT by using examples. IoT refers to anything that has access to the internet and features a function that usually benefits people. Examples of IoT devices in homes include smart doorbells, smart thermostats, smart locks, and any other “smart” device. These devices are usually seen as harmless since they are meant to make the user's life easier. For example, a smart doorbell allows someone to view who is at the door without actually going to the door. It also allows both parties to communicate through the doorbell. Someone would find a smart doorbell useful if they are disabled, if they have package thieves, or if they just want to see who is at the door before they go to the door.

As helpful as these IoT devices may seem, they harvest tons of information. For example, most of these IoT devices require the user to register with an email, username, and password. This information can be used for marketing or be a target for bad actors. Smart doorbells may also collect audio data and video data. According to the Electronic Frontier Foundation (EFF) and BBC, the Amazon Ring doorbell collects data and sends it to third party trackers such as Facebook, Google, AppsFlyer, and MixPanel. In an EFF article by Bill Budington, he says, “Four main analytics and marketing companies were discovered to be receiving information such as the names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of paying customers.” (EFF). BBC also mentioned that “Ring logs every doorbell press and app action.” Although Ring doesn’t appear to be sending the video and audio recordings, they have it on record.

Other home IoT devices may collect temperature and environment information, light brightness, time, location, and IoT device status. Smart thermostats, smoke alarms, and air quality controls may fetch the temperature the user prefers and the environment the device is in. Smart locks track the time, location, and status of the devices themselves. The device could log when the user locks and unlocks their doors, where the door is located (bedroom, bathroom, entrance, backyard, etc.), and know whether the door is (un)locked. Although these data types may not be much of a big deal to the average user, it should concern them that the IoT device collects this information and potentially sells it to third party trackers. The information being collected tells the device what time they do certain actions, how social a person is, where they live, their IP address, and other things that are like fingerprints.

Additional types of attacks that bad actors can do to IoT devices are control the IoT device itself, control other devices or the network. A bad actor could attack a smart lock and unlock it, making the house unsafe and prone to further attacks. If one were to attack a smart thermostat, they could alter the temperature and torture the user by setting the temperature to super low or high. At this point, the user would have to uninstall the device and send it back for being “faulty.” With technologies becoming more prevalent in everyday lives, more people make their homes “smart,” and these technologies are sold worldwide. Most companies focus on the security of the application and network because that’s what they’ve been focusing on in the past few decades. Although there is some form of protection in IoT devices, it’s not as secure as a computer may be.

Throughout the past few years, people have expressed their security concerns, and companies such as Ring have spoken about the concerns. Earlier this year, Ring released a statement saying they will allow users to opt-out of sharing agreements where applicable (without clarifying what “where applicable” might mean). Many companies started allowing users to request the data that has been collected on them and opt-out of sharing data to third party trackers. In 2018, California passed the California Consumer Privacy Act (CCPA), which enhances the privacy rights and consumer protection for California residents. This act allows consumers to see what data has been collected by a business and how they use that data and where it is shared to. The act also allows the consumer to delete personal information collected and opt out of collecting and selling the data (oag.ca.gov).

Something I found most interesting was how I didn’t think of this type of data being collected. Although I don’t have these types of home IoT devices, it made me think of how many people do and what kind of information is out there. I know Facebook is a huge data collector and have many litigations over what they collect and how they use that information. As an average consumer, my first thought when buying something like a smart doorbell is I can protect myself from dangerous people before answering the door in person. I wouldn’t think about the company keeping a record of the video or audio, how many times the doorbell rings, and information about me. These seem like security violations, and I’m sure they are in some areas. Still, it’s fascinating to think about how companies can collect this data without much government suspicion.

Many people claim that home IoT devices are used to spy on people by the government. Although this may be true, the government also uses IoT devices. Some of the devices may be the same such as smart thermostats or smart locks that unlock with a fingerprint, but the devices the government employ are much costlier. Other devices may not be available to purchase publicly, but another example is a device that helps track stream levels that could lead to floods in the Colorado River. This device (sensors) was implemented years ago, and the users didn’t know it was an IoT device (govtech.com). They thought they were just using the tools that were available to them, which is like most home IoT users. They see a product available to them and use it because it will benefit them somehow and don’t care much about the security behind it because they don’t think about it. A bad actor could attack the Colorado River sensors and alter the data it emits and trick the government. Although IoT devices benefit many people, they have their security drawbacks and will likely never be hacker foolproof.

Stephanie Reid: Instagram Security

Instagram, among other social media platforms, brings a lot of risk with personal information. Companies like Instagram, Facebook, Twitter, and Snapchat are more likely to be hacked because of what information a hacker could access. Some information hackers could access are the date of birth, personal information, and access to messages, photos, and videos. Instagram is a photo-sharing platform owned sold to Facebook in 2012. Many people and companies use Instagram (and other social media platforms) to advertise and build a brand. Nowadays, social media use is growing exponentially, and these companies are constantly updating their privacy and security terms. However, no matter how secure they may think they are, the users are always at risk through other means of hacking.

Phishing has been around since 1996, and it is when someone tries to access an account by sending a link or message that asks for personal information. Usually, the phisher or attacker will include legitimate links or create a link that looks exactly like the legitimate page to trick the user into thinking they are accessing the real website. On Instagram, phishers send messages that send malicious links claiming that the account may be deleted or banned if the user doesn’t follow their directions. They could also trick users by sending a message that says they won something or found them in a photo online and to click a link. That link allows the attacker to access the user's account and send spam to whoever the user is following (and possibly random people too). Since the message comes from someone you know (the attacker gained access to someone else’s account), it creates a chain of messages for people they know, which would include you. If you happen to fall for this message and believe “your friend”, your account will end up getting hacked, and the same messages will be sent to people you follow.

Another kind of attack that hackers can use for Instagram is a brute-force attack. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hopes of eventually guessing the password correctly. The most basic brute force attack is a dictionary attack where the attacker uses a program with a list of all the words in the dictionary and tries them all. Brute force attacks also typically rely on weak passwords. In 2019, Laxman Muthiyah, a security researcher, did something similar to brute forcing. Muthiyah was studying how Instagram handled password reset requests for users who forgot their login credentials. Instagram sends an email or text message to the email or phone number the account is registered with. The content of those messages contains a six-digit code, which can be used to regain access to the Instagram account. Muthiyah created a program that generated the six-digit code but realized Instagram slows down the attempts made. To bypass this, he rotated IP addresses to brute force the code, which allowed him to send a large number of requests without being slowed or limited. Muthiyah sent this bug to Instagram and was rewarded $30,000.

Although Instagram doesn’t have much control over bad passwords, it is still a security risk for the user. A strong password means it’s less likely for a brute force attack to occur and will keep you secure. Strong passwords usually consist of a mix of uppercase and lowercase letters, numbers, symbols, no dictionary words, and no ties to personal information. Having personal information in a password can lead to other attacks on other websites and possibly risk getting your identity stolen. While these are attacks to gain access to an account, there is another type of attack where someone tries to impersonate you or a business. This could pose as a threat to you or a business, and they can attack in two different ways. The attacker could trick your friends or customers and attempt a phishing attack or send malicious data, or they could contact support and claim to be the real you. Claiming to be the real person requires additional documents that can be faked and potentially get your account deleted or banned from the platform.

On September 10, 2019, Ray Parisi, a writer for CNBC, found out they were getting impersonated. The person impersonating Parisi had almost three times the followers as Parisi did and was trying to convince people to mine bitcoin. Parisi reported the account and was told to upload a selfie while holding their drivers’ license. The name on the account was Ray, and Parisi’s license is spelled “Raimondo”. Instagram rejected the report because of the spelling issue. Parisi changed the name on the Instagram account to Raimondo and successfully reported the account, which led to removing the impersonator account. Something as small as a nickname on the account not being the same on an ID can cause issues with identifying the real you. Although this may seem annoying, it is just another security measure Instagram takes.

Earlier this year, Instagram suffered an attack that they downplayed a lot. A team at Check Point found a vulnerability where it allowed an attacker to perform any action inside Instagram (like any user could do) and spy on the victim by accessing GPS location, phone contacts, and camera. Check Point said that the attack could be done by only saving a photo, and the next time the victim opens Instagram, the attack is executed. Facebook did say the vulnerability was patched, but due to the vulnerability, Check Point didn’t publicly announce it until a patch was released. As mentioned earlier, once the attack is executed, the attacker can spy on the victim, and that’s because Instagram has many permissions such as camera, GPS, contacts, photos, etc., and an attack can have access to these and spy on anyone using Instagram. Facebook downplayed the vulnerability by claiming the user would need to upload the image and how many people it could affect. Although many other vulnerabilities can be prevented, this exploit is much more severe.

Instagram, like other social media platforms, has taken security measures to prevent attacks. Something I learned is that Instagram enabled two-factor authentications (through third part authenticators like Google Authenticator, SMS messages, and Duo Mobile). A lot of these attacks can also be prevented if the user knew what to look out for and what is an attack attempt. Revoking access to third-party apps like ones that track the user’s followers is also a simple way to prevent unauthorized access to your account.

Jaewoo Cho: Database Security

Databases can be found and stored in various locations, like online in the cloud or at a physical warehouse with tons of servers to store information. Database security refers to the multiple measures companies take to protect their databases from internal and external threats. As mentioned in class, these measures are done using the CIA triangle: confidentiality, integrity, and availability. Confidentiality is ensuring that the database can only be accessed by the members that are authorized. Integrity refers to not allowing data manipulation and making sure the data stored cannot be changed. Availability is making sure the data is reliable and can continuously be accessed by the authorized people.

Databases store tons of information and are at high risk if they are attacked. Compared to the past, where data would be physically stored on paper, data can now be stored in the cloud, which means it’s vulnerable to other attacks. Database security is very important because some of the data can include medical, financial, personal, academic, social, and many other fields that are at risk of compromises. Risks to these databases lead to financial loss, reputation damage, consumer confidence decreasing, privilege abuse, and database injection attacks. In December 2019, Facebook had a breach where 267 million Facebook users/accounts were exposed on the dark web. Some of the exposed database information includes names, phone numbers, email, date of birth, and Facebook IDs. This information was posted on a hacker forum on the dark web for two weeks until access was removed. Three months after access to the database was removed, a second server containing identical records with 42 million users was released but removed two days later by anonymous hackers.

The methods used to access the compromised data are still unknown, but one possibility is that the data was stolen from Facebook’s developer API database. Between 2013 and 2015, Cambridge Analytica collected profile data from 87 million users by using a loophole in Facebook’s API that allowed third-party developers to collect data from users of their apps and everyone in the friends’ network on Facebook. Facebook didn’t care about the data being collected until 2015 when they updated the third-party API to block access to the kind of data that Cambridge Analytica was collecting. Previous (and after) to this incident, other apps collected similar data on Facebook users. In April 2020, hackers sold 267 million Facebook profiles for 500 Euros. Researchers bought this user list and verified the information. Facebook believes some of the data in the breach was from previous incidents. Something I learned is that Facebook had a breach, and the accounts were released on the dark web. I’m surprised no one sold the accounts, but somehow had a similar database incident with a similar number of accounts breached. It’s also surprising how little the accounts were sold for, considering how many accounts were breached.

There are typically five types of cybercriminals: the social engineer, the spear phisher, the hacker, the rogue employee, and the ransom artist. As mentioned earlier, there are many risks to having a database exposed. These criminals manipulate the database for phishing and spam through text messages, emails, and messages. Some of these threats are financial, academic, social, work, and personal. If a criminal gains access to any database, they could use your money, pose as you, and hurt your social, work, or personal life. One of the most significant database breaches was in October 2013, where 153 million user records were stolen from Adobe. Besides having the username and passwords hacked, the hack also exposed names, IDs, and credit/debit card information. Adobe was fined 1.1 million dollars for legal fees and an undisclosed amount to users for settle claims, but the reported number is at 1 million dollars. Criminals could’ve used the username and passwords to check other websites and see if it was a match, which means the user reuses the same password, and it is the users’ fault. The criminal also could’ve used the credit/debit card information to buy things for themselves or others.

Database breaches present themselves as any other hack. If a hacker wanted to gain access to something like another account, the hacker sends messages to everyone you are friends with. The message usually contains a malicious link that allows access to the account that clicked the link. Some organizations and companies specialize in protecting databases. An example of a database security company is DBAPPSecurity. DBAPPSecurity was founded in 2007 and is one of the most well-known database security companies. Like any other database securities, they look for vulnerabilities, exploit them, and then patch them. Another way to keep databases safe is by the principle of least permissions. The principle of least permissions limits the number of people that can access specific data or information, which means that only certain trustworthy people can access the database. Although this may be costly, encrypting the information in the database is another way to secure a database. Encrypting the database transforms readable data into a cyphertext of unreadable characters. Monitoring databases frequently is another way to keep a database secure. Being on an active lookout for database breaches allows you to patch and secure the database faster.

Recently, the United States had a presidential election, and there were many claims of election fraud, both from the president and the president’s followers. People claimed that multiple votes were made or a dead person voted. In 2015, 191 million US voter records were leaked and available for anyone to view. Some of the available data are names, addresses, phone numbers, date of births, party affiliations, and whether they voted. This information dated back to 2000. Chris Vickery, a researcher who found the database, said he found records of multiple people, including himself, within a matter of minutes. Jim Gilliam, CEO of NationBuilder (a service that sets up digital campaigns for political parties), said that the information leaked might have come from the data that is available for free to campaigns. Gilliam also stated that these voter records are publicly available from each state government, and no new information was released. The database was later taken down, but it is still unknown what happened.

Brian Chau – WeChat

WeChat is China’s popular messaging app similar to QQ (another popular messaging platform), Twitter, Facebook, and WhatsApp. WeChat is also a popular app in the US because Chinese people (and other people) use WeChat to communicate with family back in China. It is a free talking alternative to sites like Facebook and WhatsApp, which may be banned in certain areas. I have family in China (I don’t talk to them often), but my mom usually calls them or messages them on WeChat. In the US, WeChat can be used to send messages, make audio and video calls, share photos with friends, and look at other posts created by a friend of your friend. Since WeChat is primarily popular in China, WeChat offers different uses, including payment and mini-programs. If you have a bank from China, you can link the bank account to your WeChat account and send payments to friends, family, and merchants. WeChat has become a popular payment method, and some places strictly take WeChat, removing cash altogether. WeChat also has mini-programs or apps that can be used by users. For example, a developer can upload their game for users to play.

Messaging users is like any other messaging platform. You can add/find someone by their QR code, phone number, or username/ID. You can also find someone and add them if they are nearby and turn the nearby feature on. There are two options for communicating. You can use either text the message or send a voice recording to the other person. Although I’m not sure what other languages WeChat translates, WeChat does translate Chinese text messages. As mentioned earlier, people use WeChat for both personal and business purposes. It is easier for some businesses to conduct business and message through WeChat because it is familiar to them. Sending payments is also easy. All you need to do is scan a QR code or barcode and type the payment amount and click send. WeChat’s payment service is like Venmo or PayPal but is limited to Chinese bank accounts.

Although WeChat may seem like a great app, it suffers from the Chinese government. Chinese cyberspace is one of the most surveilled and censored in the world. The Chinese government doesn’t want citizens to access pages like Facebook and Google because it contains information that the Chinese government censored. An example of something they censor and never talk about is the Tiananmen Square Massacre in 1989. Many citizens know what happened that day but aren’t allowed to talk about or they risk getting executed or imprisoned. One of China’s biggest tech giants, Tencent, owns or has partial ownership in many companies like WeChat, Reddit, Riot Games, Epic Games, and Discord. Since Tencent is a Chinese company, and they have at least partial ownership of a company, they can ask to censor specific posts or messages. WeChat actively censors political posts and messages on accounts registered with a mainland China phone number.

In March 2019, over 300 million Chinese private messages were exposed online. The data breached contained Chinese citizen ID numbers, photos, addresses, GPS location, and device information. This information was sent to seventeen other servers that researchers think are police stations. It is unclear what or why the information was sent to police stations, but the police station servers have that information. China is known to censor and block tons of websites, messages, and specific phrases. China’s laws and regulations are usually open and well known because people typically accept to the government collecting data on users. Due to these laws and regulations, WeChat tells its users that the information must be available to share with the government, and that is precisely what they do. China keeps track of everyone and what they do, what they say, and basically their everyday life. The Chinese Communist Party (CCP) is still active and has recently also released facial recognition in public cameras. Life in China is heavily regulated, and these messages may be considered a breach to the US but may also be something normal for China.

WeChat trains their algorithm for what to censor through users outside china. Communication among users with WeChat accounts registered outside China is under surveillance, and those messages are used to train algorithms to censor and monitor china registered users. For example, if I sent a message to my mom (we both have US registered accounts), WeChat takes the message and gives it to China's algorithm. The China algorithm looks at the message and sees something it doesn’t like, so it blocks it and will prevent messages containing the same message in China from sending. Earlier this year, President Donald Trump tried to ban WeChat and TikTok for infringing on privacy and security rights. Trump put in an executive order to stop the use of WeChat in the US, but a judge blocked the order because there wasn’t enough evidence that WeChat was violating privacy rights. The judge that made the ruling said WeChat’s terms and conditions comply with Chinese governments (as it is supposed to) but shouldn’t have much of an issue in the US. A group called the WeChat Alliance argued that the ban would violate the first amendment rights and that there were no alternative apps that can do everything WeChat does. As of right now, WeChat is still usable and downloadable.

WeChat also has another security issue where they don’t offer end-to-end encryption. This allows third parties to read messages you send and receive without needing to decrypt anything. Most messaging apps, like WhatsApp and Facebook Messenger, have end-to-end encryption. There is encryption between the user and the WeChat server, but this is also likely because of the Chinese government. WeChat claims that they securely encrypt messages sent and received between their services and that they don’t permanently retain the content of messages. This has been proven wrong, not only recently but soon after they said that. WeChat will continue to remain the most popular messaging platform in China, but privacy and security problems will still exist. Tencent has done a great job at making WeChat an all-in-one app that allows people to pay, send messages, play games, and hail rides.

Renhai Zhou – Video Game Hacking

Video game hacking or cheating has been a prevalent issue since video games were released. People were trying to find ways to enhance their gaming experience so they can continuously win. There are two different kinds of cheating: Indie game cheating (PVE: player versus environment) and online game cheating (PVP: player versus player). PVE games refer to playing against computers or bots. Multiple kinds of cheats can be used for each game, such as using bots and software assistance, boosting/win trading, and game code modification. There are some public, private, free, and paid hacks that modify game code and includes software assistance. I used to play a game called Combat Arms, which was owned by Nexon at the time and now owned by Valofe. It was heavily filled with hackers and still is (even though the game died down a lot since Nexon sold it to Valofe). These hackers could see enemy players' location (and teammates if they chose it), aimbot (aiming assistance that made all shots a certain area such as always shooting at the head), unlimited ammo, unlimited health, etc. Most of these hacks were free and made available to the public, but I recently looked into it, and most of them are either private or are a paid subscription.

Boosting/win trading is a more common hack nowadays for games because it’s less likely to be detected by the game's anti-cheat software. Boosting is where you queue with players with higher ranks than you and let them carry you until you reach your desired high rank. Win trading usually involves the enemy team where you win or lose on purpose to boost an account. You can either have a friend do this or hire someone to do it for free or for money. I see boosting sold for many games on platforms like eBay. A popular game many people do boost/win trade is League of Legends by Riot Games. As much of a problem this may be, it is very hard to find a booster in-game. It is easy to determine who was the person that was boosted because if they’re in a game with all high ranks, but they constantly do horrible, it’s clear that they don’t belong at that rank. Riot Games hasn’t done much to counter boosting for multiple reasons. One of them is that it generates Riot more money because the players are likely to buy more merchandise and in-game products. There can also be false player reports where someone reports another player for thinking they are boosting when in fact, they are not.

Cheating has been around for a long time and is available among many platforms. There is something called the Konami Code in video game consoles like the Nintendo NES, Xbox, or PlayStation. Konami Code is the earliest and well-known video cheating code known. It is a form of game code modification and was the most popular Indie game hacking technique, right ahead of exploits. The Konami Code is a special combination of buttons that allows the player to get certain benefits such as extra lives or weapons. The code was first used in 1986 with Gradius' release for the Nintendo NES but became popular with the game Contra. The developer (Kazuhisa Hashimoto) of Gradius was going through the game to test it and found it too difficult to complete without a boost. He created a cheat code to give the player power-ups (normally attained throughout the game). When they released the game, they forgot to remove the code and was still present. Players discovered the code and shared it, which led to the code being included in other games.

Game code modification, also known as mods, is an older cheat and used less now. Like the Konami Code, mods can be used to give a player power-ups or alter the look of something. For example, the Nintendo DS' had something called an Action Replay device. This mod allowed you to play whatever game you wanted and give player boosts. I remember having an Action Replay, and I used it for my Pokémon game. I caught a legendary Pokémon, and the Action Replay allowed me to duplicate whatever Pokémon I wanted, so I duplicated the legendary Pokémon I had. Nowadays, mods are mainly used for GTA V (Grand Theft Auto 5) and Minecraft. You can add or make maps look different in both games and give other boosts. There is no way to prevent a game code modification because it injects the mod directly into the game files. It is all user-dependent, and only the users can remove mods whenever they feel like it.

There are some ways for game companies to prevent hacking/cheating. Many companies have third-party programs running in the background to detect if a player uses any kind of cheats. These programs work like an antivirus software. The programs' reliability also depends on how much the company cares about the game and what the program looks for. The hack I mentioned previously about Combat Arms can bypass the anti-cheat software that the companies put in place. However, due to the low player count, Valofe doesn’t care much about hackers and hasn’t altered the code of the program. Riot Games does a decent job of detecting hackers. They have a dedicated anti-cheat software that comes with the game, Valorant. Valorant is a first-person shooter (FPS) game like Counter-Strike: Global Offensive (CSGO). Valorant was released earlier this year, and you’re more likely to find boosters/boosted players than a hacker in real time.

If a player manages to bypass the anti-cheat software while loading the game, the anti-cheat software still runs, and if it sees the player doing extremely good, it will ban the player on the spot, and the game ends there. There is also a law in South Korea that says if someone is caught cheating in an online game, they will go to jail. Reporting players is arguably the most effective way to prevent cheaters. Some games allow developers or employees to enter a game in real time (with or without the other players knowing) and observe suspicious players. Reporting players could trigger an employee to watch the game or trigger the anti-cheat software (like Valorant does). Some companies like Riot also ban the hardware ID, which prevents the player from playing the game ever again on that device. There are workarounds such as spoofing the hardware ID, but cheating will never get you anywhere.

References

4, Hrithik Unnikrishnan June, et al. “Cheaters To Remain Banned From Valorant.” *EssentiallySports*, 4 June 2020, www.essentiallysports.com/esports-news-cheaters-to-remain-banned-from-valorant-riot-games/.

“5 Reasons Why Riot Doesn't Care about ‘MMR Boosting’ A.k.a. Eloboosting.” *Lol*, lol-eloboosting.com/blog/lol/misc/5-reasons-why-riot-doesn-t-care-about-mmr-boosting-a-k-a-eloboosting-.

Basset, Romain. “5 Common Phishing Techniques.” *Vade Secure*, 29 May 2020, www.vadesecure.com/en/5-common-phishing-techniques/.

Brewster, Thomas. “191 Million US Voter Registration Records Leaked In Mystery Database.” *Forbes*, Forbes Magazine, 30 Dec. 2015, www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/?sh=19a77a845b98.

Budington, Bill. “Ring Doorbell App Packed with Third-Party Trackers.” *Electronic Frontier Foundation*, 31 Jan. 2020, www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers.

“California Consumer Privacy Act (CCPA).” *State of California - Department of Justice - Office of the Attorney General*, 20 July 2020, www.oag.ca.gov/privacy/ccpa.

“Cheating in Video Games.” *Wikipedia*, Wikimedia Foundation, 10 Nov. 2020, en.wikipedia.org/wiki/Cheating\_in\_video\_games.

Cluley, More from Graham, et al. “How Any Instagram Account Could Be Hacked in Less than 10 Minutes.” *Security Boulevard*, 16 June 2020, securityboulevard.com/2019/07/how-any-instagram-account-could-be-hacked-in-less-than-10-minutes/.

Dey, Dipanjan. “Valorant: Vanguard Detects and Bans Some of the Biggest Cheating and Spoofing Softwares.” *Sports News*, Sportskeeda, 8 Oct. 2020, www.sportskeeda.com/esports/valorant-vanguard-detects-bans-biggest-cheating-spoofing-softwares.

Dissent, et al. “191 Million Voters’ Personal Info Exposed by Misconfigured Database.” *DataBreaches.net*, 28 Dec. 2015, www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/.

Doffman, Zak. “Facebook Dark Web Deal: Hackers Just Sold 267 Million User Profiles For $540.” *Forbes*, Forbes Magazine, 21 Apr. 2020, www.forbes.com/sites/zakdoffman/2020/04/20/facebook-users-beware-hackers-just-sold-267-million-of-your-profiles-for-540/?sh=e3aa6a67c85a.

Doffman, Zak. “How This One 'Malicious' Photo Could Hack Your Instagram Account.” *Forbes*, Forbes Magazine, 24 Sept. 2020, www.forbes.com/sites/zakdoffman/2020/09/24/how-this-one-malicious-photo-could-hack-your-instagram-account/?sh=49ce8f043378.

Gandel, Stephen. “Ring to Tighten Privacy amid Concerns It Shares Customer Data with Facebook and Google.” *CBS News*, CBS Interactive, 14 Feb. 2020, www.cbsnews.com/news/ring-facebook-google-personal-information-privacy-settings-change/.

Gonzalez, Carlos. “The Government Is Stepping Up Security on IoT Devices.” *StackPath*, 9 Aug. 2017, www.machinedesign.com/automation-iiot/article/21835814/the-government-is-stepping-up-security-on-iot-devices.

HARBERT , TAM. “Practical Uses of the Internet of Things in Government Are Everywhere.” *Government Technology State & Local Articles - E.Republic*, 2017, www.govtech.com/network/Practical-Uses-of-the-Internet-of-Things-in-Government-Are-Everywhere.html.

Harwell, Drew. “Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns.” *The Washington Post*, WP Company, 13 Dec. 2019, www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.

Kay, Russell. “Sidebar: The Origins of Phishing.” *Computerworld*, Computerworld, 19 Jan. 2004, www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html.

Kelion, Leo. “Amazon's Ring Logs Every Doorbell Press and App Action.” *BBC News*, BBC, 4 Mar. 2020, www.bbc.com/news/technology-51709247.

“Konami Code.” *Contra Wiki*, contra.fandom.com/wiki/Konami\_Code.

Liao, Shannon. “Over 300 Million Chinese Private Messages Were Left Exposed Online.” *The Verge*, The Verge, 4 Mar. 2019, www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police.

Lyons, Kim. “Judge Again Blocks Trump Administration Push to Ban WeChat in the US.” *The Verge*, The Verge, 23 Oct. 2020, www.theverge.com/2020/10/23/21531154/judge-denies-trump-administration-ban-wechat-tencent-china.

Messner, Steven. “Every Game Company That Tencent Has Invested In.” *Pcgamer*, PC Gamer, 9 Aug. 2020, www.pcgamer.com/every-game-company-that-tencent-has-invested-in/.

Ng, Alfred. “China Tightens Control with Facial Recognition, Public Shaming.” *CNET*, CNET, 11 Aug. 2020, www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

Parisi, Ray. “Someone Impersonated Me on Instagram (and Had 3x More Followers than Me)-Here's How I Stopped Him.” *CNBC*, CNBC, 14 July 2020, www.cnbc.com/2019/09/24/how-i-stopped-someone-impersonating-me-on-instagram.html.

“r/HongKong - For Those Googling ‘What Does Tencent Own?" In Relation to the Blizzard HS Blunder.” *Reddit*, www.reddit.com/r/HongKong/comments/dfrmj5/for\_those\_googling\_what\_does\_tencent\_own\_in/.

“r/VALORANT - Hardware Id Bans for Cheaters Confirmed.” *Reddit*, www.reddit.com/r/VALORANT/comments/fyveo8/hardware\_id\_bans\_for\_cheaters\_confirmed/.

“Ring Doorbell 'Gives Facebook and Google User Data'.” *BBC News*, BBC, 28 Jan. 2020, www.bbc.com/news/technology-51281476.

Romano, Aja. “The Facebook Data Breach Wasn't a Hack. It Was a Wake-up Call.” *Vox*, Vox, 20 Mar. 2018, www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained.

Sacco, Dom. “Elo Boosting: How Much Money Do Boosters Make and What Effect Is It Having?” *StackPath*, 12 July 2017, esports-news.co.uk/2017/07/12/elo-boosting-how-much-boosters-make/.

Swinhoe, Dan. “The 15 Biggest Data Breaches of the 21st Century.” *CSO Online*, CSO, 17 Apr. 2020, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

“You Should Never Use WeChat. Here's Why.” *NordVPN*, 21 Oct. 2020, nordvpn.com/blog/is-wechat-safe/.

Zaagman, Elliott. “Outside of China, WeChat Is a Fish out of Water.” *Tech in Asia - Connecting Asia's Startup Ecosystem*, 13 Oct. 2017, www.techinasia.com/outside-china-wechat-is-a-fish-out-of-water.