Virginia Journal of Science / Volume 71, Issue 3 & 4 / Fall & Winter 2020 / doi: 10.25778/c4f6-bm81

A Survey on Securing Personally Identifiable Information on Smartphones

Dar'rell Pope, Yen-Hung (Frank) Hu, Mary Ann Hoppa

Department of Computer Science

Norfolk State University, Norfolk, Virginia, USA

ABSTRACT

With an ever-increasing footprint, already topping three billion devices, smartphones have become a huge cybersecurity concern. The portability of smartphones makes them convenient for users to access and store personally identifiable information (PII); this also makes them a popular target for hackers. This survey paper shares practical insights derived from analyzing 16 real-life case studies that exemplify: the vulnerabilities that leave smartphones open to cybersecurity attacks; the mechanisms and attack vectors typically used to steal PII from smartphones; the potential impact of PII breaches upon all parties involved; and recommended defenses to help prevent future PII losses. The contribution of this research is recommending proactive measures to dramatically decrease the frequency of PII loss involving smartphones.

Keywords: Cybersecurity, Smartphone, Personally identifiable information

INTRODUCTION

PII is defined as "any information about an individual which includes (1) information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" (McCallister, Grance, & Scarfone, 2010). In 2010, analysts predicted a spike of smartphone exploits was rapidly approaching as cybercriminals figured out how to hack smartphones for financial gain (Gross, 2010). In a survey conducted by Dimensional Research, an amazing 94 percent of the respondents expected the frequency of mobile attacks to increase, and 79 percent confirmed it is becoming more difficult to secure mobile devices (Collett, 2017).

In 2009, 170 million smartphones were sold worldwide. By 2016 sales increased to 1.5 billion and surpassed 2.7 billion for the first time in 2019. According to information calculated in 2016, Android controlled 82 percent of the market share while Apple held 17 percent (Statista).

This increase in smartphone sales was paralleled by a dramatic increase in PII leak cases. In 2010, over 13 percent of apps were deemed susceptible to PII leaks. By 2014, that number climbed to over 49 percent (Ren, Rao, Lindorfer, Legout, & Choffnes, 2016). The smartphone footprint has become huge, and their mobility makes them more accessible and useable than traditional computers. Because of their popularity and constant connectivity, smartphones have become a primary target for PII attacks.

According to the 2019 Internet Crime Report published by the FBI's Internet Crime Complaint Center (IC3), there were 467,361complaints – over 1,200 every day – with reported individual and business losses exceeding $3.5 billion. Additionally, there were 16,053 reported cases of identity theft, as well as 38,218 reported personal data breaches. Losses due to credit card fraud were reported 14,378 times. Financial losses due to identity theft and personal data breaches were $160 and $120 million respectively, and credit card fraud accounted for $112 million in losses. Since this report was first created in 2000, more than 4.8 million complaints have been registered. The top three states reporting money lost to Internet fraud in 2019 were California ($574 million), Florida ($293 Million), and Ohio ($265 million) (FBI IC3, 2020).

As documented in the case studies that appear later in this report, PII leaks have become a serious problem today. Users need guidance on maintaining the confidentiality, integrity, and availability of PII on their smartphones. Remediating these knowledge gaps is the motivation for performing research on how to improve PII security on smartphones.

This study shares practical insights derived from analyzing 16 real-life case studies that exemplify: the vulnerabilities that leave smartphones open to cybersecurity attacks; the mechanisms and attack vectors typically used to steal PII from smartphones; the potential impact of PII breaches upon all parties involved; and recommended defenses to help prevent future PII losses. The contribution of this research is recommending proactive measures to dramatically decrease the frequency of PII loss involving smartphones.

The remainder of this paper is organized as follows: Section 2 summarizes research motivation and objectives. Section 3 describes the types of PII stored on smartphones. Section 4 covers 16 case studies. Section 5 discusses how PII is stolen. Section 6 proposes 11 approaches to protecting PII on smartphones. Section 7 concludes the paper with some reflections on findings and suggestions for future work to build upon them.

MOTIVATION AND OBJECTIVES

Smartphone popularity and capabilities are growing at a tremendous rate. Users' increasing demands for more apps to meet their every need creates new opportunities for PII leaks. In addition to the standard cell phone capabilities such as voice calls and text messaging, smartphones offer a wide range of value-added functionalities such as global positioning system (GPS), email, voice and video recording, web-browsing, third-party apps for banking, loyalty programs, and games to name just a few.

Smartphones generate and store a wealth of personal data including location, usage logs, contacts, photos, documents, call lists and messages. Even when a smartphone is at rest, it is gathering PII about the user such as location traces and date-time logs of activations and shutdowns. This potentially sensitive information is collected from the operating system or apps on the device and serves to motivate research on securing PII on smartphones. There are not enough government and industry solutions in place to prevent the issues.

The objectives of this work are to identify the types of PII stored on smartphones, provide case studies depicting attacks on PII, explain how PII is stolen, provide approaches to protecting PII, and finally offer solutions to mitigate risks to PII.

PII STORED ON SMARTPHONES

Research has identified the following types of PII that can be stored on smartphones. While specifics are provided for Android, analogous content, capabilities, and concerns exist on other major smartphone brands too.

GPS

GPS tracks current location and subsequent movements. For example, by using the Android service 'android.location.LocationManager,' GPS coordinates can be obtained from where they are stored in the cache and/or consolidated.db file. The consequence of unwittingly beaconing this data is unapproved traceability (Lee, Ahn, Choi, & Choi, 2014).

Phone Call Log

The phone call log stores information about outgoing and incoming calls as integers in a calllog.db file. Leaking this data provides a means for mobile malware to propagate itself by sending text messages to phone numbers from the user's call log (Bilić, 2015).

Information Searches

Information searches comprise anything that is googled. Google tracks users' search and browsing history and creates a private map of where they go with their signed-in devices. This information can be tracked through a portal called "My Activity." It is stored in the cloud and is later used to send targeted advertisements (Murphy, 2017).

Social Networking Activities

Social networking platforms provide their users many means to connect to others including web, email, and mobile applications. Venues like Facebook, Instagram, SnapChat, WeChat, and Twitter offer mobile versions that can be downloaded from app stores for quick and easy access via smartphones (Salehan & Negahban, 2013). One of the consequences of this mobilization of social media is misuse of PII as reported in current news media. For example, Facebook improperly accessed user information to build profiles on American voters that allegedly were used to help elect a specific presidential candidate in 2016 (Ingram, 2018).

Photos

Photos taken with the smartphone's pre-installed camera are stored in Digital Camera Images (DCIM) by default. Photos also can be stored on the external Secure Digital (SD) card in the My Files>SD card folder. Images taken with a third-party camera app are automatically saved in a folder named after that app as jpeg files (Bruce, 2017). If compromised, strangers could have access to personal photos with potential criminal uses such as blackmail and stalking.

Contacts

Contacts are stored on the Subscriber Identity Module (SIM) in .vcf format. If the contacts list is compromised, that data leak becomes a means for mobile malware to send text messages to phone numbers from the user's contact list to propagate itself (Bilić, 2015).

Calendars

Calendars can contain important information about birthdays, meetings, special occasions, and reminders. They are stored in .ics format in an SQLite database. The read_calendar permission allows an application to read the user's calendar data. Compromise of the calendar can expose others' PII: names and birthdays recorded in the calendar can be mapped to the contact list to garner even more granular information (Nauman, Khan, & Zhang, 2010).

Microphone and Audio

Audio recordings are stored as .m4a files in the Audio folder. Lost audio recordings can be mined for personal details files, besides resulting in a tedious restoration task if the user has no backup. Eavesdropping on voice or data communications by surreptitiously activating the phone's microphone also can disclose PII (Department of Homeland Security, 2017).

Camera

The camera stores data as jpeg files in internal memory or on the SD card in the DCIM\Camera folder. If compromised, personal photos can provide the raw material for crimes such as blackmail and stalking. The camera can be used to uniquely identify a user via analysis of patterns captured by the device's sensors (Department of Homeland Security, 2017).

Service Set Identifier

The phone's Service Set Identifier (SSID) is used to connect to Wi-Fi. If stolen, this information can be used to determine the social structure of a set of people. In other words, the Wi-Fi connections stored on their smartphones provide another means of tracking the location of users and their associates (Barbera, Epasto, Mei, Perta, & Stefa, 2013).

Data Storage

Data storage includes internal memory and/or a memory card. The format of this data can be vcf, jpg, aac, docx, mp4, ics, pdf, 3gp, m4a, and log files to name a few. Photos, emails, text messages, and contact names are stored in memory, so compromised storage exposes PII to the attacker. When a file is deleted, the operating system merely removes corresponding pointers in a file table and marks the space formerly occupied by the file as free. In other words, content

is not wiped from the device and thus the data remains in the storage and subject to discovery and exfiltration (Storm, 2014).

Passwords

Passwords are known to be one of the easiest targets for hackers. If stolen the attacker has the "keys to the kingdom." For this reason, single factor authentication is no longer considered secure. Passwords for websites are stored in /data/data/com.android.browser (Acharya, Polawar, & Pawar, 2013).

Bank and Credit Card Information

Smartphone users use their contacts list to store names, addresses and phone numbers. In addition, the contact list may be used to store bank and credit card information, account numbers, and login credentials. When apps that provide access to such accounts are hacked by means of phishing or Man-in-the-Middle (MitM) attacks, PII is put at risk (Bodkin, 2017).

CASE STUDIES

The growing number of smartphones and apps has produced a dramatic, remarkable surge in cases of stolen PII. An attacker can initially target a smartphone that contains little or no PII, then use it as a steppingstone to build a more complex attack to gain access to sensitive applications or confidential data (Blagojevic, 2016). The following 16 case studies are examples of exploits that resulted in stolen PII.

Case Study 1

The first case study occurred on December 6, 2017. An analyst discovered vulnerabilities in banking apps that are used by millions of people. The weakness was "certificate pinning" (IBM) (Bodkin, 2017), which normally strengthens the security of an app. However, in this case it masked vulnerabilities from being detected. One of the flaws left users susceptible to Wi-Fi exploitation. This exploit is known as the Janus attack (Ehrenhofer, 2019), which is very similar to a MitM attack (Chivers, 2020) (Man-in-the-Middle Attack (MITM), 2017). In a Janus attack, the attacker connects to the same network as an app user, via Wi-Fi or a corporate network. The cybercriminal covertly intercepts, relays, and changes the communication between the two parties, unbeknownst to the end users.

Case Study 2

The second case study reveals how Janus attacked Android smartphones in a different way. The vulnerability allowed attackers to modify the code of Android apps without affecting their signature verification certificates (Kumar, 2017). This allowed them to distribute malicious updates for the legitimate apps that look and work the same as the original apps. Once the malicious versions were created, attacks were released in several ways, such as fake apps, spam, bogus updates, social engineering, and MitM attacks. The vulnerability has since been mitigated, but it took months to deploy the fix, leaving an extremely large number of smartphone users vulnerable in the interim.

Case Study 3

The third case study was reported on November 9, 2017 (Pyments, 2017) (Amir, 2017). The vulnerability was identified as Eavesdropper. Eavesdropper allowed hackers to intercept texts, voice messages and other data from about 1.8 million smartphones through mobile apps. In addition, Eavesdropper impacted 700 mobile apps that were downloaded 180 million times. Careless hard coding of credentials – a common developer error – was the cause of this weakness. The reason Eavesdropper is such a serious threat is that it can allow attackers to access confidential company information such as negotiations, pricing, recruiting calls, company disclosures, health diagnoses, and market data. Recorded audio files also could be converted to text enabling massive search of corporate data.

Case Study 4

The fourth case study was reported on March 15, 2017 (VOA News, 2017). Check Point Software Technologies revealed that Telegram and WhatsApp were both susceptible to an attack that worked by infecting digital images with malicious code, activated once the picture was clicked upon. Having gained access, attackers were able to control the account, access message history, all photos that were ever shared, and send messages on behalf of the user. WhatsApp claims to have billions of users and Telegram touts more than 100 million users. The selling point of these apps is their end-to-end encryption to ensure privacy. However, it was the end-to-end encryption that made it difficult to detect the malicious code involved in this attack that potentially affected hundreds of millions of users.

Case Study 5

The fifth case study reported that dating apps Tinder, Bumble, and OK Cupid were vulnerable to being hacked. The research was performed by Kaspersky Lab in Moscow (Hackett, 2017). Kaspersky Lab was able to retrieve PII from 60 percent of the accounts targeted. Because most of the apps have minimal HTTPS encryption, hackers were allowed easy access to sensitive data. Once the account was compromised hackers were able to access location information, real names, login, password, message history, and profiles visited. Additional vulnerable dating apps are Badoo, Flirt, Zoosk, Happn, WeChat, and Paktor. A hack of this nature left victims susceptible to blackmail because users could be cheating in a relationship or involved in sexting conversations (Fussell, 2017).

Case Study 6

The sixth case study reported on January 23, 2018 that Tinder does not use encryption (Fowler, 2018) (Barasch, 2018). However, this finding was reported as early as November 2017 by a security company named Checkmarx (Zahger, 2018). The problem is Tinder chooses to use HTTP instead of HTTPS, possibly as a cost-saving measure. This means users' photos are transmitted via an unencrypted connection, so anyone on the wireless network can intercept them, exposing users' sexual and dating preferences. Another anomaly detected with Tinder is the relationship between swipes and byte size. Researchers discovered swiping left, right, matching, and super-liking each comprised a different byte size. With this knowledge they were able to

determine whom users were interested in, whom they were very interested in, and who had reciprocated.

Case Study 7

The seventh case study was reported on June 14, 2017, and it involves Samsung, the most popular smartphone maker in the world (Franceschi-Bicchierai, 2017). Samsung let the domain ssuggest.com expire. This was used to control a stock app that was installed on older devices. The stock app, S Suggest, recommends other popular apps for use. By letting the domain expire, Samsung effectively gave whoever acquired the domain carte blanche access to millions of smartphones. With this newfound power they could push malicious apps to the smartphones. Fortunately for users of older model Samsung smartphones, the domain did not fall into the hands of someone with malicious intent. Instead, Joao Gouveia, the chief technology officer at Anubis Labs took over the domain. Anubis Labs confirmed that in just a 24-hour period they observed 620 million check ins/connections from 2.1 million unique devices.

Case Study 8

The eighth case study was documented on September 12, 2017 by the security company Armis (Biggs, 2017). They discovered a group of eight exploits, collectively known as BlueBorne. BlueBorne, as the name implies, exploits a Bluetooth vulnerability that impacts most devices in use today. This vulnerability allows attackers to access smartphones without ever touching them. In addition, it can perform remote code execution as well as MitM attacks. This attack is similar to Heartbleed which exploited web servers, forcing them to display passwords and other keys remotely. A BlueBorne patch has been created and distributed. Devices running older versions of Android and Linux could still be vulnerable, which should motivate users to retire any outdated devices.

Case Study 9

The ninth case study was reported on January 5, 2018 by Apple (Griffin, 2018). They confirmed that almost all their products were affected by a major bug related to Intel chip, leaving their customers' PII exposed. At the time of this writing the resolution to the problem remains undetermined. In addition to a fix not being identified, it is impossible to ascertain the magnitude or the imminent danger that may exist. Fortunately, yet no one has taken advantage of this exploit, in part because there is so little known about it other than it does exist. Apple is being diligent about finding a fix for the problem. Until then it is important to keep operating system and virus definitions up to date as well as to avoid questionable websites.

Case Study 10

The tenth case study is about an attack known as Cloak and Dagger (Fratantonio, Qian, Chung, & Lee, 2017). Researchers at Georgia Institute of Technology discovered this attack and reported it in The Hacker News on May 25, 2017. Cloak and Dagger impacts all versions of Android up to 7.1.2. This attack allows hackers to take control of the device and steal PII, including keystrokes, chats, device PIN, online account passwords, One Time Password (OTP) passcode, and contacts. While the attack takes place, the user is unable to notice any malicious

activity. The flaw resides in the design of the Android OS. Unfortunately, until this is resolved most smartphone users will continue to be victimized by ransomware, adware and banking Trojans at least for another year (Khandelwai, 2017).

Case Study 11

The eleventh case study is about a weakness that was found in the Android operating system that allows Gmail accounts to be hacked with a 92 percent success rate (Hackett, 2014). The vulnerability was reported on August 23, 2014 by a team of researchers, two from the University of Michigan and one from the University of California Riverside. The vulnerability encompasses several other apps such as H&R Block, Newegg, WebMD, Chase Bank, Hotels.com, and Amazon. Amazon was the most difficult to hack at a success rate of 48 percent, while the others had an 80 to 90 percent success rate. Researchers believe the vulnerability also applies to Apple iOS and Microsoft Windows, although those systems had not been tested by the release of the article.

Case Study 12

The twelfth case study was documented in Mashable on April 28, 2017 by a group of researchers from the University of Michigan (Morse, 2017). They determined hundreds of apps had a security flaw that potentially would allow hackers to install malware and exfiltrate PII from millions of Android smartphones. The research team tested 24,000 apps and found 410 that were potentially vulnerable. One of these vulnerable apps has over one million downloads. The root of the vulnerability is contained in apps that create open ports on cell phones. Apps use Wi-Fi File Transfer that allows users to connect to a port on their phone via Wi-Fi and access its contents. The apps facilitate easy file transfers from a smartphone to a computer. Due to a lack of security, others may intercept this data. In the past, this problem has been seen on computers, but it has now migrated into the mobile world.

Case Study 13

The thirteenth case study was reported in Fortune Magazine on May 13, 2017 (Morris, 2017). The vulnerability resided in the Starbucks mobile app and left user accounts open to hacking. Of course, once the attackers have access to the account erroneous charges start to occur. Approximately 30 percent of purchases, valued at billions of dollars, are made with a mobile app or online. So far only one percent of Starbucks accounts have fallen prey to the attack. Another consideration is patrons who use the same username and password for multiple sites. Hackers may be able to use credentials stolen via one mobile app to hack another, thus poising them to gather more PII from other compromised websites. Corey Williams the Senior Director of Products and Marketing at Centrify stated, “Passwords are the number one security problem in the world. The only reliable defense against attackers is to enable two-factor authentication” (Williams, 2017).

Case Study 14

The fourteenth case study was discovered by Appvigil and reported on September 29, 2017 (Kanekal, 2017). Appvigil reported that 70 percent of the top 100 mobile banking apps for

Android OS are weak and susceptible to attacks such as data leakage, password stealing, and internet spoofing. As more research is being performed, more app deficiencies are being highlighted. One conclusion is that the easier and more convenient the app, the more security issues it presents. Worryingly, banks have placed a higher priority on convenience and not security.

Case Study 15

The fifteenth case study, documented in a Naked Security publication, reminded users that their movements are easily tracked when Wi-Fi and Bluetooth are enabled (Stockley, 2013). On October 25, 2013, research uncovered all Wi-Fi capable devices broadcast a unique ID, a Media Access Control (MAC) address that enables them to connect to networks. The MAC address is also known as the Mobile Location Analytic (MLA). The reason companies want to track users' movement is for marketing purposes i.e., financial gain.

Case Study 16

The sixteenth and most recent case study included in this study was reported on March 17, 2018 (Cadwalladr & Graham-Harrison, 2018). A whistleblower revealed that Facebook harvested information on 50 million users to help influence the outcome of the 2016 Presidential election. Cambridge Analytica used personal information taken without authorization in early 2014 to build a system that could profile individual U.S. voters, to target them with personalized political advertisements. PII collected included emails, invoices, contracts, and bank transfer. The data were collected through an app called thisisyourdigitallife. Hundreds of thousands of users were paid to take a personality test and agreed to have their data collected for academic use. The app also collected information about the test-takers' Facebook friends. The data were used to build an algorithm that could analyze individual Facebook profiles and determine personality traits linked to voting behavior. The algorithm and database together made a powerful political tool. It allowed a campaign to identify possible swing voters and craft messages more likely to resonate with those individuals.

These 16 case studies collectively highlighted weaknesses with various mobile apps, manufacturing design flaws, and Bluetooth vulnerabilities. They provided information on different occurrences of stolen PII and the impacts of breaches on users or organizations. As shown in Table 1, common outcomes resulting from a breach are financial loss, a damaged reputation, and legal impacts such as lawsuits.

Table 1: Summary of the 16 Case Studies

Case study	PII Stolen	Impact
1. certificate pinning	usernames, passwords, PIN	damaged reputation, unspecified financial loss
2. Janus	usernames, passwords, PIN	damaged reputation, unspecified financial loss

3. Eavesdropper	texts, voice mails, company confidential information, negotiations, pricing, recruiting data, disclosures, health diagnoses, market data	1.8 million smartphones infected, 700 mobile apps, downloaded 180 million times, damaged reputation
4. WhatsApp	message history, photos, send messages on user behalf	100 million plus users, damaged reputation
5. dating apps	location, actual names, passwords, message history, profiles visited	possible blackmail, damaged reputation
6. http	photos, sexual and dating preferences	damaged reputation
7. Samsung	potential access to all PII, usernames, passwords, photos, contact list, email, messages, location, PIN, contacts	millions of phones, damaged reputation
8. Blueborne	access to all PII, usernames, passwords, photos, contact list, email, messages, location, pin, contacts	unspecified financial loss, damaged reputation
9. Apple	access to all PII, usernames, passwords, photos, contact list, email, messages, location, pin, contacts	unspecified financial loss, damaged reputation
10. Cloak and Dagger	keystrokes, chats, pin, account password, one-time passwords, contacts	unspecified financial loss, damaged reputation
11. Android OS	email	damaged reputation
12. Wi-Fi	access to all PII, usernames, passwords, photos, contact list, email, messages, location, pin, contacts	unspecified financial loss, damaged reputation
13. Starbucks	user accounts	1% of accounts, damaged reputation
14. banking apps	passwords	70% of banking apps, damaged reputation
15. movement	location	financial gain, high traffic areas, busiest timeframes
16. Facebook	location, age, gender, photos, languages spoken, relationship, education, career, finances, home ownership, ethnicity, generation, family, life events, politics, interest, behavior, other social media connections	damaged reputation, changed election outcome, $40k penalty per user

HOW IS PII STOLEN?

Smartphones are more at risk in certain venues such as hotels, coffee shops, airports, cars, trains, etc. Also, home Wi-Fi connections can be potential risk areas if users do not configure them properly. An attacker easily could access PII in the form of emails, documents, contacts, calendar, call history, Short Message Service (SMS), Multimedia Messaging Service (MMS), user identification, passwords, mobile applications that store PII, and geolocation data (Blagojevic, 2016). Research has shown that PII can be stolen in many ways as detailed below.

Weak Passwords or No Passwords

A password is a protected string of characters used to authenticate an individual. Passwords are one of the most often used authentication mechanisms today. A strong password is a major countermeasure to password cracking attempts. Policy should dictate strong passwords contain a minimum of eight upper and lowercase characters, two special characters and two digits. A brute-force attack can unscramble weak passwords in seconds (Rouse, 2019). Once acquired the attacker has access to username and credentials. If that same password is used for other accounts, the attacker has access to them as well.

Unsecure Wi-Fi

Smartphones transport data wirelessly over airwaves and then to a wired network. The wireless space the data travels is not necessarily encrypted. So, encrypting data for transmission on a smartphone does not necessarily guarantee end-to-end encryption. A common attack is Wi-Fi traffic monitoring, whereby a hacker uses a simple free application that can be downloaded from the internet to watch all traffic on a public Wi-Fi network. As soon as the username and password are entered, the software notifies the hacker that information is captured. There are numerous hacking tools readily available, such as, AirSnort, Aircrack, and WepAttack (Shankdhar, 2019) to aid in hacking processes aimed at stealing PII like usernames and passwords.

Nonencrypted Transmission

HTTP is the foundational data communication protocol of the web, and many dating apps use HTTP instead of its secure counterpart HTTPS (Barasch, 2018) (Fowler, 2018). HTTPS is HTTP running over Secure Socket Layer (SSL); it uses public key encryption and provides data encryption, server authentication, and message integrity. In addition to HTTP not using encryption, an additional weakness is the lack of a mechanism to verify the identity of a website. This means it is theoretically possible for an attacker to impersonate the site being visited. The attacker then has a means to deliver malicious content or attempt to steal PII (Trevellyan, 2015). Stolen PII can include location information, real name, login ID, password, message history, and other profiles visited.

Fake Apps

Fake apps are downloaded from Google Play, App Store or Play Store. Fake apps can collect sensitive data from the user (e.g., usernames and passwords), access personal data stored on the device (e.g., calendar and contacts list), and use sensitive device capabilities (e.g., the

GPS, camera, or microphone). Once these malicious apps make their way onto a device, they can monitor and transfer certain categories of data, depending on the app's permissions and controls; this includes the security sensitive data, phone information, contacts list, GPS location, SMS messages, and files stored on external storage. These apps are designed with malicious intentions (Wei, Gomez, Faloutsos, & Neamtiu,, 2012).

Social Media and Dating Apps

Social media is a catch-all term for a variety of internet applications that allow users to create content and interact with each other. Some examples are Tinder, Facebook, Instagram, and LinkedIn (Fussell, 2017) (Hackett, 2017) (Cadwalladr & Graham-Harrison, 2018). As suggested earlier, dating apps such as Tinder are very vulnerable to having PII stolen because they use HTTP instead of HTTPS. The PII stolen from social media and data apps can include location information, real name, age, gender, relationship status, login ID, password, message history, and other profiles visited.

Man-in-the-Middle Attacks

MitM attacks occur when an intruder injects himself into an ongoing dialog between two users to intercept and read messages being passed back and forth (Chivers, 2020) (Man-in-the-Middle Attack (MITM), 2017). In layman's terms, a MitM attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the intended receiver has been replaced by an unknown attacker who intercepts and modifies the message before retransmitting it to the intended receiver. Thus, the attacker controls the entire communication. User credentials are stolen during a MitM attack.

Phishing

Phishing is a form of social engineering with the goal of obtaining personal information, authentication credentials, credit card numbers, and/or financial data. PII stolen during successful phishing exploits also can include social security numbers and account PINs. Attackers lure, or "fish," for sensitive data through various methods including emails and phone calls (Phishing, 2013).

Outdated Anti-Virus Software

Most existing anti-virus software tools rely on an up-to-date virus signature database to detect malwares. If its virus signatures are outdated, the ani-virus software's effectiveness diminishes. This can happen when a new malware emerges, and anti-virus researchers have not yet identified its signature; or because the system on which the anti-virus software is installed has not kept its signature files up to date. For example, a smartphone may not have 24 X 7 Internet connectivity. As a result, even when new virus signatures are available, the smartphone may not obtain it in a timely fashion (Cheng, Wong, Yang, & Lu, 2007).

Bluejacking

Bluejacking (Fuller) is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain physical radius. First, the hacker scans his surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices. Typical PII lost via a Bluejacking attack are the contacts list and calendar.

Cell Phone Cloning

Cell phone cloning is a technique whereby secured data from one cell phone is transferred into another phone. The other cell phone becomes an exact replica of the original cell phone. During cell phone cloning, a stolen cell phone is essentially reprogrammed with someone else's credentials. The PII leaked when a phone is cloned can include text messages, contacts list, photos, and information gleaned by eavesdropping calls without the user's knowledge. (Hayes, 2020).

APPROACHES TO PROTECT PII ON SMARTPHONES

This section provides guidance on how to protect PII on smartphones. These approaches will apply to the previously researched means whereby PII is stolen. Each approach is described along with the mechanism of the approach, and finally an explanation of how the approach remedies the PII leak issue.

Implementing Two-Factor Authentication for Passwords

Two-factor authentication dramatically improves the security of a smartphone security and all the personal information stored there (Two Factor Authentication for Apple ID). Weak passwords that have low complexity can be hacked in a matter of hours. Implementing two-factor authentication for mobile transactions resolves the loss of PII due to weak passwords or no password being used. This is one way to assure that using an app will not expose users to fraud. With two-factor authentication, accounts will be accessed only on devices trusted by the user. When signing into a new device for the first time, the user provides two pieces of information — a password and a [six-digit] verification code. Entering the code verifies the new device is trusted.

Encryption

Unencrypted data makes an easy target for hackers because the information is in readable form, also known as plaintext. If an unauthorized person gains possession of an unencrypted smartphone they can easily access all the plaintext PII it contains. Encryption is a reversible process that scrambles plaintext information into an unreadable format called ciphertext, that looks like gibberish to unauthorized individuals trying to read it. This is a simple fix because most smartphones come with an encryption feature built in, but users tend to turn it off to avoid extra steps like entering credentials and codes. User data always should be encrypted. (Phifer, 2013).

Virtual Private Network

A Virtual Private Network (VPN) is a secure private connection through a public network or an otherwise unsecure environment. It is a private connection because encryption and tunneling protocols are used to ensure the confidentiality and integrity of transmitted data. As one example, many dating apps use HTTP which is not secure, making them an easy target for hackers. Using unsecured dating apps, especially on public, unprotected Wi-Fi networks, should be avoided. Public networks, like those configured in coffee shops, airports, or hotel lobbies, often do not require passwords, and allow anyone to monitor the activity on them. If users choose to access accounts via their smartphone while in public, they should use Bluetooth instead of public networks and install a VPN. Also, disabling GPS and tracking for dating apps is recommendable so that cybercriminals cannot monitor users' location and movements (Tripwire Guest Authors, 2018).

Multi-Factor Authentication for Banking

Multi-factor authentication should be used for online banking to help prevent loss of PII due to unencrypted transmissions between apps and banks. Much like dating apps, communication between the smartphone app and bank is unencrypted when data is transferred using HTTP. Data transferred using HTTP can be compromised by a MitM attacks. This protects users' logins from the loss of a password. Besides providing their user id and password, users must vouch for all logins, as well as those from unrecognized computers or locations, by typing in an additional one-time passcode sent to their smartphone via text message. Even if a cybercriminal steals the username and password, they are out of luck unless they also steal the user's smartphone, since without it they cannot receive the additional authentication code needed to login each time (Ducklin, 2014).

Review Smartphone Settings

Users should review their smartphone settings and make sure third-party app downloads are not permitted from untrusted sites. Fake apps downloaded from Google Play, App Store or Play Store are designed with malicious intent. Fake apps come in the form of anti-virus software, games, and browsers. Cybercriminals use emails and SMS messages that appear to be from legitimate banks, credit card companies or other well-known brands to lure people into downloading applications that will compromise their data. Sometimes fake apps pose as security updates, and clicking on links also may lead to PII being stolen. To help prevent PII leaks due to fake apps, users should resist a sense of urgency, and instead remember to always think before clicking (Norton).

Wi-Fi Protected Access II

Wi-Fi Protected Access II (WPA2) is the strongest type of encryption available and – if offered – is the preferred option. The biggest threat to Wi-Fi security is the ability for the hacker to position himself between the user and the connection point, so users are sending their information to the hacker instead of the hotspot (Kaspersky). Using unsecured Wi-Fi networks and Bluetooth connections thus creates vulnerable points of access for data and identity theft. There are numerous ways to decrease opportunities for being victimized. Encryption is the best

way to keep PII safe since it makes intercepted data unintelligible to the hacker. Bluetooth connections can be used to connect to wireless headsets, transfer files, and enable hands-free calling while driving, to name a few. Usually this so-called "pairing" must occur first to allow a Bluetooth connection before data is shared. Pairing provides a measure of data security; but just like Wi-Fi connections, Bluetooth can put PII at risk if users are not careful. For one thing, if a user connects their smartphone to a rental car, the phone's data may get shared with that vehicle. Users must remember to unpair their smartphone from the car and clear any personal data from the car before returning it to the provider. Bluetooth also should be turned off when not in use, since keeping it active enables hackers to discover another connected device they can use to spoof the user into gaining access to their phone. Bluetooth should be used in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding that smartphone's Bluetooth connection (Federal Communications Commission, 2019).

Private Mode

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing, and collaboration (Rouse, 2020). Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media. On social media, PII often is handed over voluntarily. For example, users reveal their birthdate, place of birth, phone number, address, and photos – valuable PII that can be used to steal identities or to speed hacking weak passwords. To prevent PII leaks on social media accounts such as Facebook, Twitter, Instagram, and others, users should put them into a locked-down, private mode to evade detection (Johnson, 2020). When social media accounts are locked down, site visitors cannot see what is inside another user's account without explicit permission. This works well for staying up to date with close friends and family while preventing random internet users from perusing and mining PII from social media venues.

Certificate Pinning

Certificate pinning is an approach to preventing PII from being stolen (IBM) (Fronczak, 2019). Within mobile apps, it helps ensure the app is communicating with the intended device, thus defending against MitM attacks, a popular method for hackers to steal PII. Certificate pinning links the certificate to the destination's hostname to create trust. It is important to have pinning between the certificate and the server's hostname and to confirm that the certificate is from a valid root authority. All these controls are built directly into the mobile app.

Do Not Click on Hyperlinks

Users should never mindlessly click on links inside emails from unknown or untrusted users. This helps prevent losing PII to phishing attempts that often involve malicious links inside emails. Phishing scams are a leading technique used by cybercriminals to steal PII (SEORG, 2018). The sender may pose as a bank or someone with authority and send victims an email that has a sense of urgency associated with it (e.g., Subject: Get back to me ASAP!!). Inside the email is a link that the sender urges the recipient to click. Such links typically take the user to a fake website that lures them into revealing PII. Even after being taught about phishing, users still can

be fooled into these actions due to the proficiency and skill of professional scammers. User must be disciplined to never give out account information or provide information through a source that is not irrefutably known to be genuine (Zamora, 2018).

Keep Software Updated

Like all other devices, smartphone software must be kept up to date. Outdated software raises the risk of losing PII because vulnerabilities with known fixes are not being mitigated. Updates provide security patches and sometimes additional functionality to your software. Operating systems are an important part of the smartphone and should be updated regularly. Anti-virus software also is important to keep up to date. Anti-virus software uses "definitions" to protect from threats. Most vendors will update their definition files daily, and it is important to keep these files up to date. If the definitions are not up to date, the anti-virus software will not be able to provide protection from the latest threats (Verizon Blog, 2016) (Zamora, 2018).

Awareness

Awareness is perhaps the most important means of protecting smartphones and their users against cybersecurity risks. As one example, consider bluejacking, an attack conducted on Bluetooth compatible devices, such as smartphones. Bluejacking is initiated by an attacker (aka bluejacker) who forwards unsolicited messages to a user of a Bluetooth-enabled device (Bali, 2013). The actual message sent to the user's device does not cause detriment but is used to entice the user to react in some way that will facilitate unauthorized PII access, such as adding a new contact to the device's address book. This message-transmitting attack resembles spam and phishing attacks conducted against email users. Users also should disable the Bluetooth device when not in use, use an unidentifiable device name, employ security mode 3 or 4, disable unused services and profiles, set device to non-discoverable mode when not in use, use hard-to-guess PIN codes of at least 12 or more alphanumeric characters, and perform pairing only when absolutely required.

Table 2 rolls up the three key areas – causes, effects, and prevention mechanisms relevant to protecting PII on smartphones – as discussed in this section.

Table 2: Summary of Stolen PII Causes, Effects and Mitigations

Cause of Stolen PII	Problems Caused by Stolen PII	Approach to Fix Problem
weak or no password	compromised credentials, damaged reputation, financial loss	use strong password, two-factor authentication
unencrypted information	compromised credentials, damaged reputation, financial loss,	use encryption
unsecured dating app	location, actual names, message history, profiles visited, damaged reputation, financial loss	use HTTPS, VPN

unencrypted transmissions	compromised credentials, damaged reputation, financial loss	use HTTPS, VPN
fake apps	compromised credentials, damaged reputation, financial loss	do not allow 3-party app downloads from untrusted sites
unsecured Wi-Fi	access to all PII, usernames, passwords, photos, contact list, email, messages, location, pin, contacts	use WPA2 encryption, turn Bluetooth off when not in use, use Bluetooth in "hidden" mode not "discoverable" mode
social media	location, age, gender, photos, languages spoken, relationship, education, career, finances, home ownership, ethnicity, generation, family, life events, politics, interest, behavior, other social media connections	use in private mode
MitM attack	damaged reputation, financial loss, username, password, PIN	use certificate pinning
phishing	damaged reputation, financial loss, username, password, PIN	do not click on any links inside emails
outdated virus definitions	user credentials	keep anti-virus software up to date
Bluejacking	contact list, user credentials	user awareness, disable device when not in use, use an unidentifiable device name, employ security mode 3 or 4, disable unused services and profiles, set device to non-discoverable mode when not in use, use non-guessable pin codes of at least 12 or more alphanumeric characters, perform pairing only when absolutely required

RECOMMENDATIONS

This section summarizes recommendations for end-users to better secure PII on their smartphones.

- Do not jailbreak or root the smartphone. Although this enables personalization, running otherwise prohibited apps and functions exposes the smartphone to a higher risk of malware and data leakage.
- Use passphrases instead of passwords. Passphrases are easier to remember and nearly impossible to crack. Passphrases can contain spaces as well as numbers and special characters which meet the complexity requirement.

- Install and use anti-virus for virus protection, antivirus scans and mobile security against malware and adware; keep signature files up to date.
- Install and use VPN.
- Install anti-theft apps. This protects smartphone apps by requiring a secret code to gain access, and safeguards PII by hiding such data in a secure encrypted folder.
- Be prepared for a breach. Maintain an up-to-date inventory and secure backup of the PII contained on the smartphone.
- Perform frequent backups of all data.
- Review and appropriately adjust permissions on all smartphone apps.
- Lock smartphone when not in use. Enable fingerprint or facial recognition to unlock.
- Set smartphone to erase all data after a set number of failed login attempts.
- Enable "remote-wipe" in case the smartphone is lost or stolen.
- Do not use auto log-in feature.
- Lock individual apps in case the smartphone is stolen while it is unlocked. Folder Lock is a good app for this functionality. It has been downloaded over 5 million times and is free.
- Install monitoring apps to monitor identity on sites such as Gmail, Dropbox, and Facebook. The app alerts on suspicious activity, such as logins from unfamiliar places, giving the user a chance to step in and change credentials before serious harm can be done.
- Limit sharing on social media.

CONCLUSION

Through research this paper presented various scenarios in which PII can be stolen from smartphones. These instances were shown to occur for a wide variety of reasons, including poor manufacturer design, cybercriminals, unencrypted communications, user error, and outdated software. Unfortunately, there is no single-point solution that can address all causes of PII loss. Fortunately, in nearly every case of PII loss there is a potential solution that can mitigate associated vulnerabilities and therefore help prevent the exploit from occurring.

Overall, the best protection mechanism against losing PII is a defense-in-depth approach. Defense-in-depth is the act of using multiple security measures in a layered approach to protect the integrity of information. These security measures include using multi-factor authentication, VPN, HTTPS, keeping anti-virus software up to date, operating in private mode, and not clicking on unverified hyperlinks in emails.

ACKNOWLEDGEMENTS

"This work was supported [in part] by the Commonwealth Cyber Initiative (CCI), an investment in the advancement of cyber R&D, innovation and workforce development. For more information about CCI, visit cyberinitiative.org."

LITERATURE CITED

Acharya, S., Polawar, A., & Pawar, P. Y. (2013). Two factor authentication using smartphone generated one time password. *IOSR Journal of Computer Engineering (IOSR-JCE), 11*(2), 85-90.

Amir, U. (2017, 11 10). "Eavesdropper" flaw exposes millions of call, texts and recordings. https://www.hackread.com/eavesdropper-flaw-exposes-millions-of-call-texts-and-recordings/

Bali, R. (2013). Bluejacking technology: Overview, key challenges and initial research. *International Journal of Engineering Trends and Technology (IJETT), 4*(7), 5.

Barasch, A. (2018, 1 24). Tinder isn't the only dating app that leaves your information and swipes vulnerable to hackers. https://slate.com/technology/2018/01/tinder-isnt-the-only-dating-app-that-leaves-your-information-and-swipes-vulnerable-to-hackers.html

Barbera, M. V., Epasto, A., Mei, A., Perta, V. C., & Stefa, J. (2013). Signals from the crowd: Uncovering social relationships through smartphone probes. IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference, (pp. 265-276). Barcelona, Spain.

Biggs, J. (2017, 9 12). New Bluetooth vulnerability can hack a phone in 10 seconds. https://techcrunch.com/2017/09/12/new-bluetooth-vulnerability-can-hack-a-phone-in-ten-seconds/

Bilić, D. G. (2015, 12 16). How do you know if your smartphone has been compromised? https://www.welivesecurity.com/2015/12/16/know-smartphone-compromised/

Blagojevic, N. (2016, 4 2). Smartphone security. https://www.fraud-magazine.com/article.aspx?id=4294992799

Bodkin, H. (2017, 12 6). Flaw discovered in banking apps leaving millions vulnerable to hack. https://www.telegraph.co.uk/science/2017/12/06/flaw-discovered-banking-apps-leaving-millions-vulnerable-hack/

Bruce, I. (2017, 6 25). Where are pictures stored on android phone? https://www.recovery-android.com/pictures-tored-on-android.html

Cadwalladr, C., & Graham-Harrison, E. (2018, 03 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cheng, J., Wong, S. H., Yang, H., & Lu, S. (2007). SmartSiren: Virus detection and alert for smartphones. Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys,07), (pp. 258-271). San Juan, Puerto Rico.

Chivers, K. (2020, 3 26). What is a man-in-the-middle attack? https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Collett, S. (2017, 8 1). Five new threats to your mobile security. https://www.csoonline.com/article/2157785/five-new-threats-to-your-mobile-security.html

Department of Homeland Security. (2017, 4). Study on mobile device security. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

Ducklin, P. (2014, 01 10). Just how secure is that mobile banking app? https://nakedsecurity.sophos.com/2014/01/10/just-how-secure-is-that-mobile-banking-app/

Ehrenhofer, J. (2019, 10 18). Advisory note for users making use of subaddresses. https://web.getmonero.org/2019/10/18/subaddress-janus.html

FBI IC3. (2020, 2 22). 2019 Internet crime report. https://pdf.ic3.gov/2019_IC3Report.pdf

Federal Communications Commission. (2019, 10 8). Wireless connections and Bluetooth security tips. https://www.fcc.gov/consumers/guides/how-protect-yourself-online

Fowler, B. (2018, 1 23). Flaws in Tinder app put users' privacy at risk, researchers say. https://www.consumerreports.org/privacy/tinder-app-security-flaws-put-users-privacy-at-risk/

Franceschi-Bicchierai, L. (2017, 6 14). Samsung left millions vulnerable to hackers because it forgot to renew a domain, researchers say. https://www.vice.com/en_us/article/7xp79x/samsung-left-millions-vulnerable-to-hackers-because-it-forgot-to-renew-a-domain

Fratantonio, Y., Qian, C., Chung, S. P., & Lee, W. (2017). Cloak and dagger: From two permissions to complete control of the UI Feedback Loop. 2017 IEEE Symposium on Security and Privacy (SP) (pp. 1041-1057). San Jose, CA, USA.

Fronczak, Y. (2019, 3 5). What does certificate pinning mean? https://carvesystems.com/news/cert_pin/

Fuller, J. What is bluejacking? https://electronics.howstuffworks.com/bluejacking.htm

Fussell, S. (2017, 10 24). Researchers hack Tinder, Ok Cupid, other dating apps to reveal your location and messages. https://gizmodo.com/researchers-hack-tinder-ok-cupid-other-dating-apps-to-1819803674

Griffin, A. (2018, 1 5). Every iPhone, iPad and other Apple devices vulnerable to hacking: Here's what you need to do. https://www.independent.co.uk/life-style/gadgets-and-tech/news/iphone-apple-intel-bug-flaw-security-issue-how-to-safe-protect-update-latest-download-a8143126.html

Gross, G. (2010, 10 5). Mobile malware exploits on the way, experts say. https://www.computerworld.com/article/2516167/mobile-malware-exploits-on-the-way--experts-say.html

Hackett, R. (2014, 08 22). Gmail smartphone app vulnerable to hackers, researchers say. http://fortune.com/2014/08/22/gmail-smartphone-app-vulnerable-to-hackers-researchers-say/

Hackett, R. (2017, 12 25). Kaspersky researchers uncover flaws in popular dating apps like Tinder, OkCupid, and Bumble. https://fortune.com/2017/10/25/tinder-kaspersky-okcupid-bumble-dating-app-security-hack/

Hayes, R. (2020, 4 9). How cell phones are cloned and how to stop it from happening to you. https://www.techjunkie.com/how-to-clone-cell-phone/

IBM. Certificate pining. https://www.ibm.com/support/knowledgecenter/en/SSHSCD_7.1.0/com.ibm.worklight.dev.doc/monitor/c_cert_pinning_intro.html

Ingram, D. (2018, 3 21). Zuckerberg apologizes for Facebook mistakes with user data, vows curbs. https://www.reuters.com/article/us-facebook-cambridge-analytica/zuckerberg-says-facebook-made-mistakes-on-user-data-vows-curbs-idUSKBN1GX0OG

Johnson, J. (2020, 6 3). Guard your social privacy - How to make your Instagram, Twitter, TikTok and other social media accounts private. https://www.androidcentral.com/how-make-your-instagram-twitter-tiktok-and-other-social-media-accounts-private

Kanekal, V. (2017, 09 29). 70% Of the mobile banking android apps are vulnerable: Appvigil. http://trak.in/tags/business/2015/04/02/mobile-banking-android-apps-vulnerable/

Kaspersky. How to avoid public wifi security risks. https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Khandelwai, S. (2017, 05 25). All android phones vulnerable to extremely dangerous full device takeover attack. https://thehackernews.com/2017/05/android-hacking-technique.html

Kumar, M. (2017, 12 9). Android flaw lets hackers inject malware into apps without altering signatures. https://thehackernews.com/2017/12/android-malware-signature.html

Lee, H., Ahn, H., Choi, S.-W., & Choi, W. (2014, 1). The SAMS: Smartphone Addiction Management System and Verification. *Journal of Medical Systems, 38*(1).

Man-in-the-Middle Attack (MITM). (2017, 3 30). https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm

McCallister, E., Grance, T., & Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). Gaithersburg, Maryland, USA: National Institute of Standards and Technology.

Morris, D. Z. (2017, 5 13). Hackers are targetting the Starbucks app. https://fortune.com/2017/05/13/starbucks-app-hacked-security/

Morse, J. (2017, 04 28). Whoops. Millions of Android phones are wide open to hackers. https://mashable.com/2017/04/28/smartphones-hack-android-open-ports-google-play/#IHbDE7cPkPqi

Murphy, M. (2017, 8 21). Destroy all evidence: How to see what Google knows about you – and how to delete it forever. https://www.thesun.co.uk/tech/4288350/how-to-see-what-google-knows-about-you-including-places-youve-visited-and-a-guide-to-switching-it-off/

Nauman, M., Khan, S., & Zhang, X. (2010). Apex: Extending Android permission model and enforcement with user-defined runtime constraints. ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, (pp. 328-332). Beijing, China.

Norton. How to spot a fake Android app. https://us.norton.com/internetsecurity-how-to-how-to-spot-a-fake-android-app.html

Phifer, L. (2013, 03 27). How mobile device encryption works to protect sensitive data. https://searchmobilecomputing.techtarget.com/tip/How-mobile-device-encryption-works-to-protect-sensitive-data

Phishing. (2013, 9 23). https://www.techopedia.com/definition/4049/phishing

Pyments. (2017, 11 10). 180M Smartphones vulnerable to hacker eavesdropping. https://www.pymnts.com/news/security-and-risk/2017/appthority-mobile-apps-vulnerable-to-hacking/

Ren, J., Rao, A., Lindorfer, M., Legout, A., & Choffnes, D. (2016, 8 19). ReCon: Revealing and controlling PII leaks in mobile network traffic. https://arxiv.org/abs/1507.00255

Rouse, M. (2019, 1). Brute Force Attack. https://searchsecurity.techtarget.com/definition/brute-force-cracking

Rouse, M. (2020). Social Media. http://whatis.techtarget.com/definition/social-media

Salehan, M., & Negahban, A. (2013, 11). Social networking on smartphones: When mobile phones become addictive. *Computers in Human Behavior, 29*(6), 2632-2639.

SEORG. (2018, 4 16). Identity thieves – Phishing and pilfering your PII. https://www.social-engineer.org/general-blog/identity-thieves-phishing-and-pilfering-your-pii/

Shankdhar, P. (2019, 2 22). 20 Popular wireless hacking tools. http://resources.infosecinstitute.com/20-popular-wireless-hacking-tools-updated-for-2016/#gref

Statista. (n.d.). Global smartphone sales to end users from 1st quarter 2009 to 2nd quarter 2018, by operating system. https://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/

Stockley, M. (2013, 10 25). Is your smartphone broadcasting your movements when you shop? https://nakedsecurity.sophos.com/2013/10/25/is-your-smartphone-broadcasting-your-movements-when-you-shop/

Storm, D. (2014, 7 9). Think you deleted your dirty little secrets? before you sell your Android smartphone. https://www.computerworld.com/article/2476496/think-you-deleted-your-dirty-little-secrets-before-you-sell-your-android-smartphone.html

Trevellyan, R. (2015, 10 7). HTTPS. Why your website should use it instead of HTTP. https://trevellyan.biz/why-your-website-should-use-https-instead-of-http/

Tripwire Guest Authors. (2018, 2 Retrieved 03 29, 2018, from Tripwire: https://www.tripwire.com/state-of-security/security-awareness/tips-staying-secure-using-dating-apps/

Two factor authentication for Apple ID. https://support.apple.com/en-us/HT204915

Verizon Blog: Cell phone security: 30 tech experts share important steps to securing your smartphone. (2016, 6 8). https://drivesaversdatarecovery.com/blog/verizon-blog-cell-phone-security-30-tech-experts-share-important-steps-to-securing-your-smartphone/

VOA News. (2017, 3 15). 2 Popular messaging apps vulnerable to hackers. https://www.voanews.com/silicon-valley-technology/2-popular-messaging-apps-vulnerable-hackers

Wei, X., Gomez, L., Faloutsos, M., & Neamtiu, I. (2012). Malicious Android applications in the enterprise: What do they do and how do we fix it? Riverside: Department of Computer Science and Engineering, University of California.

Williams, R. (2017, 05 15). Starbucks app vulnerable to hacking, fraudulent charges. https://www.mobilemarketer.com/news/starbucks-app-vulnerable-to-hacking-fraudulent-charges/442710/

Zahger, D. (2018, 1 23). Are you on Tinder? Someone may be watching you swipe. https://www.checkmarx.com/2018/01/23/tinder-someone-may-watching-swipe-2/

Zamora, W. (2018, 8 16). Top 10 ways to secure your mobile phone. https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/