A survey on smartphone user's security choices, awareness and education

Frank Breitinger[a,b,*], Ryan Tully-Doyle[a], Courtney Hassenfeldt[a]

[a] *Cyber Forensics Research and Education Group (UNHcFREG), Tagliatela College of Engineering, ECECS, University of New Haven, 300 Boston Post Rd., West Haven CT, 06516 United States*

[b] *Hilti Chair for Data and Application Security, Institute of Information Systems, University of Liechtenstein, Fuerst-Franz-Josef-Strasse, Vaduz 9490, Liechtenstein*

1. Introduction

Smartphone features and usage have changed significantly over the past few years. The increasing amount of personal / private data on smartphones make them a popular target for theft (Bitdefender.com, 2017; Urban et al., 2012). For instance, a survey conducted by the NYU Langone Medical Center found that 58% of smartphone users downloaded a fitness or health application (Krebs and Duncan, 2015; Pai, 2015) while Hom (2011) states that there are 70 million smartphones lost / stolen each year in the US, only 7 percent of which are recovered. In return, vendors provide better security features and users become more educated / aware.

In this paper, we examine smartphone users' choices, awareness, and education with respect to cybersecurity. While there have been several similar studies, there are some issues in the existing data: First, technology, education and user behaviors change quickly, thus requiring consistent up-to-date studies to understand users and to develop adequate strategies for addressing weaknesses in security behaviors. As discussed in Section 2 on prior work, most studies are either several years old, are from less reputable sources (i.e., not peer-reviewed) or do not focus on generations Y (ca. 1981–1996) and Z (ca. 1997–2012). Secondly, existing surveys often do not consider participants' cybersecurity familiarity / background and conclude that weak security practices could be solved with more vigorous user education, which is only partially true. Lastly, prior work does not analyze user precautions with respect to hard vs. soft security, which in our case means protecting the phone from unauthorized physical access (hard) or protecting the data and privacy (soft). Consequently, we conducted a survey with the aim of answering the following four research questions:

- R1 Do smartphone users choose appropriate lock (screen) settings on their phone?
- R2 Do smartphone users follow good security practices to protect the data on their smartphone (besides lock settings)?
- R3 Do smartphone users have differences in behavior and security choices for their desktops (compared to their smartphones)?

* Corresponding author at: Fuerst-Franz-Josef-Strasse, 9400 Vaduz, Liechtenstein.
E-mail addresses: Frank.Breitinger@uni.li (F. Breitinger), rtullydoyle@newhaven.edu (R. Tully-Doyle), chass1@unh.newhaven.edu (C. Hassenfeldt).
URL: http://www.FBreitinger.de (F. Breitinger), http://www.unhcfreg.com/ (C. Hassenfeldt)

R4 Are smartphone users more cautious about hard security than soft security (i.e., protection from getting physical access to the phone vs. protecting data and privacy)?

The scope includes only users who completed the majority of the questions. The survey, including results (in csv and SPSS) can be downloaded here: https://www.fbreitinger.de/wp-content/uploads/2019/04/smartphone_survey_data_2019.zip. Additionally, the paper makes the following contributions:

- The results show that the majority of users have appropriate lock screen settings, but that there is a deficiency when it comes to other security settings / choices, e.g., utilization of additional security software such as virus scanners.
- We find that education alone does not necessarily fix the problem of lax security practices, as many of our participants had moderate or higher security knowledge but still made poor decisions.
- We include several recommendations for software developers with respect to usability that increase better security practices: (1) a WiFi option connect only this time; (2) Emojis as an alternative to PINs; and (3) improving laws and regulations with respect to default settings.

The structure of this paper is as follows: first, we summarize the related work and previous similar studies in Section 2. Next, we outline the survey methodology including sample considerations in Section 3. The descriptive statistics results and the inferential statistics results are presented in Section 4 and Section 5, respectively. Section 6 discusses the limitations of the study. The last sections provide a discussion and analysis of the results as well as the conclusion.

2. Prior work

Smartphones and their security have been well studied. The main areas of research are threats and malware; there are several studies discussing security threats (i.e., vulnerabilities or attacks). For instance, La Polla et al. (2013) categorizes attacks including possible solutions from 2004 to 2011 to improve smartphone security. A similar, newer study was conducted by Zaidi et al. (2016), analyzing data from 2010 to 2015. On security awareness and behavior of smartphone users, the literature is limited:

Security awareness A first survey, now almost a decade old, by Breitinger and Nickel (2010) "revealed a very low security level of the devices. This is partly due to a low security awareness of their owners and partly due to the low acceptance of the offered authentication method." Specifically, 86% did not use any authentication like a PIN to access the phone. Similarly, a survey conducted by Imgraben et al. (2014) in 2014 found that "participants were generally unaware of the risks they subjected themselves to by leaving their WiFi and Bluetooth turned on at all times". The authors conclude that education and awareness programs are essential to correct misconceptions and usage behavior. Vecchiato and Martins (2015) is concerned with the awareness that users have towards the security dangers behind user-defined configurations. Their survey interviewed 554 participants with respect to 38 user-defined security settings where the results show that in average only 18 settings are correctly set. Consequently, Das and Khan (2016) points out that "one way to ensure adoption of security practices [...] is to enable them by default." In contrast, Furnell (2005) argues that it can be useful but sometimes a "single default level of security cannot reasonably be expected to suffice for all users". On the other hand, Murray (2014), who surveyed 143 more tech-savvy participants, "indicated that the majority of the respondents did, in fact, have a high degree of awareness regarding security risks to their smartphone devices. [...] The findings also suggested that the majority of users were not concerned about the privacy and protection of their personal data, with some believing that they did not have anything worth taking."

Apps and permissions Besides this broad research, there have been studies particularly targeting apps, including their permissions. Research by Mylonas et al. (2013) showed that 76% believed that applications downloaded from the application repository are secure; users tended to have disabled smartphone security software; and users preferred pirated apps. They conclude that "only technically and security savvy users tend to inspect [... security] messages." An article published in 2012 by Boyles et al. (2012) found that "57% of all app users have either uninstalled an app over concerns about having to share their personal information or declined to install an app in the first place for similar reasons." Alani (2017) designed a survey five years later to measure the user awareness with respect to permissions applications require when being installed. The paper concludes that only 35% look at required permissions.

Security concerns Felt et al. (2012) "asked 3115 smartphone users to rate their level of concern about 99 risks corresponding to 54 smartphone permissions" where the top three risks were: (1) permanently disabled (broke) your phone, (2) made phone calls to 1–900 numbers (cost money), and (3) sent premium text messages from your phone (cost money) (a full list is given in their Appendix). In the same year Chin et al. (2012) tried to understand user attitudes towards security and privacy for smartphones. They found that "participants are apprehensive about running privacy- and financially-sensitive tasks on their phones as a consequence of four main factors: fear of theft and data loss, misconceptions about the security of their network communications, worries about accidentally touching / clicking, and mistrust of smartphone applications."

In sum: there have been several studies showing that smartphone users are concerned about apps, permissions, settings and privacy. The literature claims that users are not adequately educated and therefore make poor security choices. This establishes one of the goals of this paper: understanding if there is a significant association between security familiarity and security choices / settings.

3. Methodology

To assess the smartphone user's security choices, awareness behavior, and education, an online survey was conducted from March to April 2018. In the following we briefly explain the survey design, the workflow, and some details about the statistical significance of the results.

3.1. Survey creation and design

The following high-level methodology was used to complete the survey:

1. A literature review was conducted (see Section 2) to ensure the relevance of this project / survey.
2. A survey was designed to gather general demographic information, personal phone basics, stolen device questions, cybersecurity questions, stored information, smartphone versus laptop information, device lock settings, and comments.
3. A category two exemption from the Institutional Review Board (IRB) at the University of New Haven was obtained, which restricts the survey from recording participant identification information or behavior, and disclaiming that it posed risk or harm to subjects not encountered in everyday life.
4. The survey was distributed on social media sites such as Facebook, Twitter, Tumblr, and LinkedIn as well as forums

such as Quora, Reddit, AskMe, and theGradCafe along with different mailing lists.
5. The data was obtained via the Baseline survey system and analyzed using statistical probability and cross-comparing different questions in the statistical software package SPSS.

The survey went through several drafts to ensure the questions were precise and supported the research questions. For the questions themselves, we followed guidelines to avoid leading questions and "to get correct and truthful responses" (Bhat, 2019), SurveyMonkey.

To make the survey possible to validate, the questions were designed to elicit similar responses from similar respondents. That is, high levels of subject knowledge should be reflected in similar responses across many questions. The questions were written to be platform independent in order to avoid biasing the responses towards iOS or Android users. The authors also designed the survey in parallel to similar surveys given over the past decade, both as models for comparison and to reveal information related to changing technology and behaviors.

IRB regulations require that all questions are optional to the participants, which means it is possible to leave questions unanswered. The target audience was any smartphone user over the age of 18 (underaged individuals are not allowed due to IRB). The goal was to receive responses from a diverse group of participants with varying age, gender, level of education, and geographic location. The survey itself consisted of 39 questions:

- 29 multiple choice.
- 8 multiple selection (check box).
- 2 free response.

Questions were made generic enough to be applied to any mobile phone, e.g., if a device connects automatically to open WiFi networks which is a setting for all operating systems; or another question asked if messages are shown on the screen when unlocked. When we found differences, we tried to be as comprehensive as possible, e.g., for lock options (some of these were specific to Android devices such as trusted places).

3.2. Result placement

Sample considerations Before summarizing our findings, this section discusses the quality of our results. The average duration to complete the survey was 9 minutes. The online survey was distributed using different channels (e.g., LinkedIn, mailing lists and private contacts) where the channel was not captured. The survey population is representative of the population that participates in informational, entertainment, or professionally oriented online communities. We also asked participants to share the survey with their contacts. In combination, this means that the survey responses involve self-selection. Standard inferential techniques will be applied to the sample data, with the caveat that the inferences drawn in the sequel sections reflect conclusions about a self-selected sample. In particular, the sample is skewed young: the majority of users are between 18 and 40.

Survey data Our survey has answer options that are either nominal or ordinal. When possible, survey responses have been organized into an ordinal arrangement with respect to increased quality of security practices. Questions with binary responses generally have 'no' as the less secure response, and 'yes' as the more secure, such as "Do you use a VPN on your device?" The arrangement of responses into ordinal data allows the application of tests designed to find trends in the responses.

In some cases, data from several possible responses has been combined into one larger label to facilitate valid statistical analysis. For example, with $n = 223$, a contingency table of security expertise (Q32) vs GPS service usage (Q11) has 35 possible response categories, too many for standard techniques to have the power to detect associations. In these cases, the inferential techniques have been applied to recoded data. In the above example, the 7 possible responses to Q11 (see Table 2) have been combined into 4: 'Never', 'Less than 2 hours', '2-12 hours', and 'Always'.

Survey question correlation and reliability Many of the survey questions address topics that are correlated - that is, for example, security knowledge is going to affect the responses to questions concerning settings, VPN practices, browsing behavior, etc. This inter-item correlation can be used to verify that users' responses are valid. Users with high security knowledge should, in general, also give answers that reflect that knowledge to other questions. One measure that takes advantage of these expected correlations is Cronbach's α test. The α test measures the degree to which high ranking answers on one question are correlated with high ranking questions on other questions. Values of α range from 0, indicating essentially random responses, to 1, indicating perfectly correlated answers by individual users. An α value of 0.7 or higher is typically considered to reflect an acceptable instrument in survey-based research.

Questions on the survey include inventory type questions and scale type questions. The scale-type questions are said to be *reliable* if administering the same questions to a different sample would result in similar outcomes. We evaluated reliability using Cronbach's α test on scale questions 8, 9, 13–15, 18–21, 32, 36, and 37, after correcting reverse scored variables. The result, $\alpha = 0.728$, indicates that the scale questions are reliable.

4. Results from descriptive statistics

The findings obtained by descriptive statistics are presented in following section. Percentages are with reference to the sample responses to each individual question. Answering questions was optional and therefore number of respondents varies with $\text{responses}_{\min} \geq 210$ for all but 4 questions: Q30, Q31, Q38 and Q39. Remark: all values are round to one decimal place and thus some answers / columns may not add up to exactly 100%. As the results in this section are descriptive, they should be viewed strictly with reference to the sample. Inferential conclusions are discussed in the sequel section.

4.1. Demographics (Q1 - 7, Q32)

The demographics of our participants are shown in Table 1. The majority of our participants were between 18 and 30 and lived in the United States or in South Korea. We had slightly more females than males participating.

Participants were asked to rank their familiarity with cybersecurity on a scale from 1 (least) to 5 (most). The majority of 35.8% rated themselves with a 2 (I follow the news of related topics) followed by 23.4% who reported 1 (I have no knowledge). Twenty percent stated that they have read / taught themselves about related topics (3). The remaining participants either had taken one or more courses in a related topic (14.2%) or even have a degree in this or a related field (6.4%).

Our population included 65% iOS and 30.9% Android users; the remaining answers included Blackberry, Windows or 'unsure'. While this does not match the actual market shares (e.g., according to IDC[1] the share between iOS and Android is roughly 15% to 85% (in favor of Android)), it follows a study from Leswing (2018) which states that "82% of American teenagers currently own an iPhone, the highest percentage ever in the history of a Piper Jaffray study about teens".

[1] https://www.idc.com/promo/smartphone-market-share/os (last accessed 2019-03-11).

Table 1
Demographics overview.

Gender	
Female	56.3%
Male	41.0%
Other	1.4%
I prefer not to answer	1.4%
Age	
18 to 23	55.8%
24 to 30	21.9%
31 to 40	7.6%
41 to 50	3.6%
51 to 60	8.0%
Over 60	1.3%
I prefer not to answer	1.8%
Highest completed level of education	
Some High School	2.2%
High School Graduate	27.0%
Technical Training	2.2%
Some College	35.0%
College Graduate	21.5%
Some Post Graduate	3.6%
Post Graduate Degree	8.5%
Country of residency	
Afghanistan	0.5%
Antigua and Barbuda	0.5%
El Salvador	0.5%
France	0.5%
Germany	0.9%
India	0.9%
Kyrgyzstan	0.5%
Saudi Arabia	0.5%
South Africa	0.5%
South Korea	37.8%
United Kingdom	0.9%
United States	56.3%

Table 2
Summary of the results for questions 10 and 11: how many hours per day are the Bluetooth / GPS services enabled?.

Responses	Bluetooth	GPS
Less than 2 hours	24.3%	26.2%
Between 2 and 4 hours	5.9%	5.4%
Between 4 and 8 hours	3.2%	3.6%
Between 8 and 12 hours	3.6%	3.2%
24 hours	17.1%	31.7%
I'm not sure	13.1%	18.1%
Never	32.8%	11.8%

74.0% of respondents stated that the phone is always in their possession, followed by 21.1% who indicated that it is sometimes left unattended (e.g., occasionally I forget it on my desk, or I leave it on the bar when going to the bathroom). The remaining 4.9% stated that their smartphone is often left unattended (e.g., left on the desk during lunch break or forgotten at home). This behavior coincides with other studies. For instance, Deloitte (2016) states that "Americans are viewing their smartphones more often than ever before, on average 52 times per day" while Parasuraman et al. (2017) "reported the increase of mobile phone dependence, and this could increase internet addiction".

4.2. Usage habits (Q8 - 12)

The next set of questions focused on usage habits for WiFi, Bluetooth and GPS, where we found that many smartphone users follow weak security practices. As shown in Table 2, there is a large group of users who have their GPS and Bluetooth services enabled 24/7, which may have two reasons: (1) convenience from a user's perspective or (2) these settings are required by other devices / services such as wearables. Regardless, there are several security issues coming with this choice: Besides existing attacks[2] like BlueSnarfing, BlueBugging or Blueover (details see Minar and Tarique, 2012), it can be used for surveillance (Dunning, 2010; Fuller, 2008). Similar privacy concerns exist for GPS, which is utilized by various apps to attach your locations to messages or social media posts (Ionescu, 2010).

Groeneveld et al. (2010) points out that "the consensus about privacy on the Internet seems to have changed a lot. A few years ago, people were still hesitant about using their real names online, but nowadays people are comfortable sharing their exact location with the whole world." While we expected to see a trend like: 'The less expertise a user had, the longer Bluetooth / GPS services were enabled and vice versa', the data did not show any correlation between the utilization of the services and the familiarity with cybersecurity (Q32).

We asked about user behavior concerning public WiFi, given the steady increase of publicly available WiFi networks (expected to almost double from 2018 to 2022 to almost 550 million available networks according to Cisco (2018)). Over three-quarters of the sample said they use public WiFi networks while the remaining 22.2% avoid them. The public WiFi users can be divided into three groups: (1) yes, always with 34.8%, (2) yes, but only for browsing with 35.8% (no sensitive information is transferred, e.g., no Banking Apps), and (3) yes, but I use additional encryption (e.g., a VPN software) with 7.2%. Naturally, the more cybersecurity background a user had, the more likely s/he is to use a VPN or not use public WiFi at all. However, there needs to be additional analysis why VPNs are used (e.g. for privacy reasons or overcoming Geoblocking / content filtering). For instance, Norton by Symantec (2017) states that "60% feel their personal information is safe when using public WiFi" and Patterson (2017) points out that VPN usage is higher in restrictive countries such as China or Saudi Arabia.

In addition to utilizing public unsecured WiFi networks, a majority of 78.7% also automatically connect to them. Specifically, 61.1% automatically connect to known networks (networks they have previously accessed) where 17.7% configured their devices to automatically connect to *any* open WiFi even if it has not been seen before. Both settings put the user at risk, as an active adversary can set a rogue access point or an evil twin.

Lastly, participants were asked if they enabled message preview, i.e., if a preview of the message such as Whatsapp or SMS / text is shown on the lock screen (or in the status bar). With this setting, anyone who has physical access to the phone can read messages without authentication. In our sample, this feature was enabled by 55.2% and disabled by 41.6%. The rest were not sure.

4.3. Content on devices (Q13, Q16 - 21)

Smartphones continue to become more and more powerful and are intensely used. Statistics show that smartphones have overtaken personal computers in some usage categories, e.g., the internet traffic that comes from mobile devices (Enge, 2018). Unsurprisingly, smartphones store a tremendous amount of information, and "your smartphone probably knows more about you than you do" (Ng, 2018). Before having participants list their phone contents, we asked if they have ever thought about all the information that is stored on their mobile phone. 36.8% of users answered that it is somewhat worrisome, followed by 28.6% who were not worried and 26.4% who stated that they are worried and try to secure their device as good as possible. This is similar to results in Murray (2014), which found that when "asked how concerned

[2] These attacks are older and usually do not impact modern devices anymore.

Table 3
Questions 16 and 17 analyzed which information is stored on devices; question 30 focused on information stored on stolen devices.

Responses	Smart-phone	Mac/PC	Stolen/ lost*
Contacts	87.3%	43.2%	38.9%
Email	85.0%	70.0%	46.0%
Personal Photographs	83.6%	72.7%	52.4%
Social Media Applications	77.3%	52.7%	38.1%
Calendar Events	73.2%	40.5%	33.3%
Maps (Saved Home)	61.4%	28.6%	17.5%
Autofill Banking Information	61.4%	20.0%	19.0%
Auto Saved Passwords	57.3%	56.8%	31.7%
Voice Assistant	50.5%	16.4%	12.7%
Cash Exchange Saved Info	45.5%	13.6%	7.9%
Autofill Debit / Credit Card Information	39.1%	28.6%	17.5%
Wallet	30.0%	6.8%	7.9%
Health Information	24.1%	17.7%	14.3%
IoT Autofill Information	10.0%	3.2%	6.3%

* We only considered the 63 respondents who answered *yes* or *lost* their phone for Q29.

Table 4
Question 18 and 19: How often do you preform backups on your device?.

Responses	Smart-phone	Mac/PC
Once a week	11.8%	8.6%
Once a month	13.1%	10.0%
Once every 3 months	10.0%	5.7%
Twice a year	6.8%	6.7%
Once a year	9.1%	10.5%
Never	22.6%	31.0%
When prompted by my device	26.7%	27.6%

Table 5
Summary for question 29: where devices were stolen.

Responses	total: 13.9%
Yes, on public transportation	2.8%
Yes, in the store / bar* / casino*	1.8%
Yes, at work / school*	4.6%
Yes, in a crowed	4.2%
Yes, in the bathroom	0.5%

* These options did not exist in the original survey but were entered by the participants.

they were about the privacy and protection of their personal data on their smartphone, only 30% of the respondents suggested they were either very / extremely concerned."

We then focused on what kind of information users store on their smartphone and compare it with their desktops. A result overview is given in Table 3 (the last column is discussed in Section 4.4) and shows that users reported storing significantly more information on their smartphones than on desktops. In addition to the items listed in the table, we asked if users would enter their Social Security Number (SSN) on the devices. 11.3% admitted to storing their SSN on their mobile device compared to 6.2% on their desktop. In contrast, 30.0% of the smartphone users and 39.4% of desktop users have never entered it. The last group indicated they enter the SSN when needed (smartphone: 49.3%, desktop: 63.8%).

Although having large amounts of data on devices, users often do not have appropriate recovery strategies. In our sample only 11.8% of smartphone and 8.6% of desktop users backup their devices once a week. All details are provided in Table 4 which let us conclude that often users depend on software (reminders) to perform a backup. According to Klein (2018), these numbers have been very similar throughout the last decade (for desktop users). In terms of mobile devices, more research is required as we could not find current statistics.

4.4. Stolen and lost devices (Q29 - 31)

According to Lookout (2014)'s "Phone Theft in America report, a survey of smartphone theft victims conducted by IDG Research [...], 1 in 10 U.S. smartphone owners are victims of phone theft and 68 percent of victims were unable to recover their device after the theft occurred." The report further states that most devices were stolen because the owner left the phone behind in a public setting. While both result in the same loss, we differentiated: in our sample, 13.9% had their phone stolen (more details are shown Table 5) and 15.2% lost their phone. A rundown of the data stored on the phones is given in Table 3.

Subsequently, in question 31, we analyzed the victim's reaction which included reporting a theft (39.7%[3]), remotely locking the phone (36.5%), changing passwords (28.6%), remotely resetting the phone (23.8%) or doing nothing (12.7%). In the free-response part of the question, the most common answer was that users tried to locate the phone using a map application (4.8%).

4.5. Lock screen settings (Q22 - 28)

In 2010, Breitinger and Nickel (2010) noticed that only 13% secured their phone by either a PIN or a visual code (Android pattern), however two-thirds of the participants were open to use biometrics authentication methods instead of the currently chosen setting. Four years later, Harbach et al. (2014) found that "42.7% of participants indicated that they use some form of lock screen, including PINs, passwords or unlock patterns". More recent studies even indicate higher numbers, e.g., Anderson (2017) said that 72% use a lock screen (PIN, thumbprint scanner, password, pattern of dots or other).

For our sample population, only 7.7% indicated that they can use their phone immediately; all others required some form of authentication as listed in Table 6:Q22 with fingerprint being the most popular choice. In general, our sample is favoring biometric lock options over knowledge based options with 68.8% to 31.2% (Q28). While fingerprints are not perfectly secure, as shown in the 'masterprint' study (Roy et al., 2017), user awareness has definitely increased over the past years. 59.1% stated that they were happy

[3] We only considered the 63 respondents who answered *yes* or *lost* their phone for Q29.

Table 6
Questions 22 and 23 analyzed which lock screen setting is in place and if users would prefer a different mechanism. Multiple answers were allowed.

Lock screen setting	Q22	Q23
Fingerprint	65.9%	13.0%
PIN (4 digits or less)	25.9%	3.3%
PIN (5 digits or more)	29.6%	5.1%
Password (at least one char)	15.0%	6.1%
Pattern	13.6%	6.5%
Face	6.8%	14.9%
Voice	4.1%	6.9%
Remainder (combined)*	7.8%	10.7%

* Other answers (e.g., unlock with trusted devices, trusted places) had $\leq$2.3% and thus were combined into one 'remainder' category.

Table 7
Question 24 asked how long after inactivity the devices locks itself; question 25 asked about the complexity / diversity of the PIN.

Q24. Inactivity to lock		Q25. PIN diversity	
30 sec	35.3%	One (e.g., 1111)	4.2%
1 min	24.8%	Two (e.g., 1122)	7.4%
2 min	9.6%	Three (e.g., 4432)	8.8%
3 min	4.1%	Four (e.g., 8471)	37.8%
4 min	0.9%	$\geq$ Four	30.9%
5 min	6.9%	N/A	11.1%
$\geq$ 5 min	6.9%		
Never	11.5%		

with their current lock screen setting while the remaining participants would favor changing the mechanism if it was available on their phone (see Table 6:Q23).

To look at security quality, participants were asked how long it takes until their device locks itself (Q24) and about the diversity / complexity of their PIN (Q25). For simplicity, complexity equaled the number of different digits in a PIN, e.g., one means the PIN has four identical digits; two means the PIN consists of two different digits like 1122 or 2525. Results for both questions are summarized in Table 7. Note, we purposely decided to have a straightforward complexity measurement for Q25 to avoid confusion and accept errors that come with it, e.g., 1234 is an easy PIN but would fall under 'Four'.

We also asked users to indicate how often they changed their lock settings. A group of 36.1% stated that they never update their lock settings (i.e., change PIN) where 41.7% change it when there is a reason, e.g., someone knows the PIN (Q26). The remaining users change it every year (6.5%), six months (5.1%), three months (8.8%) or one month (1.9%). To understand user choices, Q27 focused on the reasoning that best explains the chosen lock setting. Roughly over one-third responded with *security* and a little less than one-thirds said *convenience*. *Forgetfulness* and *no opinion* had 11.9% each; the remaining 8.3% stuck to the default phone settings.

4.6. Securing devices (Q14 - 15, Q34 - 38)

Willis (2013) found that many users "stick with the default settings on their computer-software programs, despite the ability to customize these, in part because they do not know that users can change these settings". 39.6% of our sample reported that they have checked all the settings on their phone and secured it the best they can, compared to 28.6% who use default options. The rest (31.8%) changed default settings as issues come to their attention. Interestingly, when looking into default browser settings on smartphones, 37.7% of users reported changing settings. Compared to an older study from Spool (2011), which found that "less than 5% of the users we surveyed had changed any settings at all", this is a significant change.

Table 8
Questions 34 and 35 asked which applications, if any, do you use to protect your device and the data on it?.

Responses	Smart-phone	Mac/PC
Virus Scanner	16.7%	43.1%
Password Handling Applications	15.4%	11.6%
Virtual Private Network (VPN)	12.1%	16.2%
Applications to Securely Delete Files	8.8%	17.1%
Secure Messaging Applications	7.0%	6.9%
None	39.1%	20.4%
I'm not sure	26.5%	21.8%

Table 9
Questions 36 and 37 asked for encryption of devices.

Responses	Smart-phone	Mac/PC
Yes, I changed it	15.7%	16.7%
Yes, by default	20.8%	18.1%
No	15.7%	19.1%
I don't know, I use the default settings	47.7%	46.2%

In a comparison of desktop and smartphone security, 34.6% rated their desktop device as more secure than their smartphone; 18.4% rated their smartphone higher. A group of 13.8% consider both devices equally secure while 11.1% admitted that neither are very secure. 22.1% is not sure which device has better protection. On the other hand, Chin et al. (2012) found that "study participants were more concerned with privacy on their phones than on their laptops. They were also less likely to make purchases and perform sensitive tasks (e.g., accessing health data) on their phones"

Following the previous subjective questions, Table 8 highlights specifics of the security choices survey participants made. Numbers are similar to Bitdefender.com (2017) and Vecchiato and Martins (2015) who found that roughly 40% of users have a security application installed. Table 9 shows responses whether or not devices are encrypted: this number almost tripled compared to a previous study (Centre for the Advancement of Social Sciences Research (CASR), 2012). Note: question 38 allowed to respondents to mention additional security choices. Although we received 96 responses, the majority said no / nope / none. The other responses included: common sense, ability to lock / locate / wipe remotely and proxy servers.

4.7. Comments and suggestions (Q39)

Finally, participants were given the opportunity to provide any additional feedback, comments or suggestions. Submissions were provided by 43 individuals. 55.8% were made up of answers such as Not applicable, N/A, none or thank you. Others asked to change the survey to be more specific about computers, provide more answer options for particular questions (18.6%). Two comments focused on topics / items we forgot in the survey and could have been beneficial such as more on two-factor authentication and including tablets. Three participants gave additional information on their security practices, e.g., 'do not give permissions to all the applications that you're using on your phone'.

The remaining comments (14.0%) addressed the respondents lack of security knowledge and included comments such as:

- I can really use a basic course in mobile device and PC security protection. How about lunch and learn sessions 3x a year.
- Now I feel like someone should help me keep my devices and information more secure!

Table 10
Users self-reported security knowledge by operating system.

Security knowledge	Android	iOS
1 - None	27.1%	9.1%
2 -	39.4%	35.4%
3 - Some	22.7%	20.1%
4 -	16.7%	13.9%
5 - High	12.1%	6.2%

Table 11
Phone security features by operating system.

Mobile security settings	Android	iOS
Use defaults	10.8%	34.0%
Change as needed	33.8%	32.6%
Checked all settings	55.4%	33.3%

- Wish they would make it easier to protect your personal information.
- I want to protect my information in PC / Phone, but actually I don't know any security applications.

5. Results based on inferential statistics

As our data is divided between nominal and ordinal variables, our primary analysis will depend on contingency tables. When one or both of the variables is nominal, we use χ^2-tests for independence to check for independence of the response categories. Whenever the expected count for any combination of responses is less than 5, we either combine categories to raise expected counts, or we use descriptive techniques to explore the data. When both categories are ordinal, arranged by increasing quality of security, we can instead use a more powerful Mantel-Haenszel linear-by-linear test for association to look for trends as we move through the category ranks. When such a test has been employed, we mark the resulting p-value with †.

The underlying hypothesis to the χ^2 test is that the category distribution of the crosstabulation is independent of category. Significance indicates that there is an underlying association between category counts and variable values. The underlying hypothesis in the linear-by-linear test for association is that the odds of moving up in rank in one variable do not change as ranks increase in the other. Significance indicates that the odds of moving up in rank in one variable vary as the rank of the other variable increases.

5.1. Ios is correlated with weaker security knowledge

Previous work, e.g. (Mylonas et al., 2013), concludes that a user's choice of smartphone operating system is correlated with the user's security/technology knowledge. In particular, iOS users report lower security knowledge and weaker security practices. We find that a similar trend is present in our data set. (Note: we have removed the responses corresponding to Mobile Windows and Blackberry, as there were too few responses for inference.)

Even at the descriptive level, one can see the concentration of iOS users in the low information categories. A χ^2 test for independence on the data in Table 10 is significant, $p = 0.012$, which indicates that the distribution here is not likely to be the result of random selection. The same test on Table 11 gives $p = 0.001$, which indicates the same relationship between operating system and security practices.

5.2. Less expertise means weaker lock screen settings

Section 4.5 discussed the utilization of lock screen settings and concluded that compared to previous studies, they became more popular. One might expect that an increase in familiarity with cybersecurity (Q32) would be strongly linked to improved lock screen settings. However, as depicted in Table 12, this expectation is not entirely supported by the survey data. A significant relationship exists between security knowledge and the use of passwords. A strong trend is visible in increasing password use with increased security knowledge. Knowledge was also associated with improved security practice in the strength of PIN selections, where a strong relationship exists between the use of long PINs and increased cybersecurity familiarity.

Table 12
Associations between security knowledge (Q32) and screen lock behaviors (Q22-26).

Variable	χ^2	df	p
Password use	12.013	4	.017
Biometric use	2.726	1	.099†
Pattern use	3.769	4	0.438
PIN use	3.642	4	0.457
PIN complexity	25.057	8	.002
Lock updates	4.617	8	0.594

Table 13
Associations between security knowledge (Q32) and security choices (Q13-15, Q18, Q36).

Variable	χ^2	df	p
Concern about information storage	15.568	1	.000†
Phone encrypted	32.223	6	.000
Phone security features	19.767	6	.003
Browser defaults	10.561	3	.014
Backup frequency	1.762	1	.184†

Biometric methods surveyed include the use of fingerprints, voice, and facial recognition, categories that were combined in analysis to support statistically meaningful interpretation. While a Pearson's χ^2 test failed to detect significance, a more powerful linear-by-linear test for association indicates that there is a weak relationship between increasing knowledge and increasing use of biometric methods. However, use of biometric lock methods are much more strongly associated with age than education (i.e., younger people are more likely to use biometrics).

These trends are even more striking in the percentages. 48.3% of respondents over the age of 40 reported using biometric locks, as compared to 80.8% of smartphone users between 18 and 23, and an identical trend is visible in the attitudes towards biometric security, with 77.3% of users in that age range reporting preferring biometric methods.

Some insight into why even high knowledge users have uneven security practices can be gained by considering the responses to Q27 about why users make their particular lock screen settings. Even in high expertise categories (self-reported 4 and 5), 33.3% of users reported *convenience* as the primary reason for their physical security choices and 37.8% reported *security*. This split is present in users of all levels of security familiarity (31.8% convenience vs.35.9% security).

5.3. Less expertise means poorer security choices

Table 13 depicts the associations between the familiarity with cybersecurity and security related choices throughout the questionnaire. The findings indicate user who are less familiar with cybersecurity are more likely to: (a) follow weak security practices (Q8-15), (b) not have a sophisticated backup strategy (Q18) and (c) not utilize security applications (Q35). Users familiar with cybersecurity are much more likely to know and use security features on their phones, change default settings, and use encryption. A linear-by-linear test shows a moderate trend in backup frequency

Table 14
Associations between security knowledge (Q32) and security application usage (Q35).

Variable	χ^2	*df*	*p*
VPN	17.335	1	.000†
Secure messaging	14.920	1	.000†
Virus scanner	12.216	1	.000†
Secure delete	4.903	1	.027†
Password handling	1.319	1	.251†

Table 15
Percent users Mac/PC (Q34) vs. smartphone (Q35).

	Mac/PC		Phone	
	Low	High	Low	High
Secure delete	11.6%	28.8%	5.4%	15.6%
Password handling	9.3%	17.8%	12.4%	22.2%
Secure messaging	2.3%	15.5%	3.1%	20.0%
VPN	6.9%	42.2%	6.2%	33.3%
Virus Scanner	34.1%	64.4%	10.8%	33.3%

associated with expertise, but visually the table clearly illustrates that users with at least moderate security knowledge are far more likely to backup regularly (37.8%) than users with no cybersecurity knowledge (27.4%).

In Table 14, we see strong links between increased familiarity and the use of security apps on mobile devices. We should note, however, that the effect sizes in these cases vary considerably. While very few low information users reported using security apps on their phones (almost 0% on each question), even among expert users, virus scanners (33.3%), VPNs (33.3%), secure messaging (20.0%), and secure deleting (15.6%) are not in widespread use.

5.4. Desktops versus phones

We now examine trends in security products on both phones and Mac/PCs. Our categories for comparison will be users who evaluated themselves as 1 or 2 in response to Q32 (that is, low expertise) and those that rated themselves 4 or 5 (that is, high expertise).

The differential distribution of security products for low expertise users, shown in Table 15, is somewhat ambiguous. Most products are hardly used by respondents in this group, though it is likely that because of their low expertise, there is an underreporting effect present in the data. For example, Mac/PC devices running modern operating systems have built-in virus scanners, though it is unclear that users in this category would know that. Use of VPNs and secure messaging applications is essentially indistinguishable. Interestingly, password handling software for both low and high expertise users seems to be more common on phones.

Examining the distribution of security products for high knowledge users, shows a sharp contrast with the low information respondents. However, even here we see the same practices affiliated with phones as with the low expertise group. Password handling and secure messaging is more common on phones, while secure deletion, VPN usage, and virus scanners are significantly more common on PCs. While expert users are more likely to use security products, even in this group the distribution is far from universal.

5.5. Soft security practices

In Section 5.2, we see a clear connection between increased domain knowledge in security and improved practices with physical protection of smartphones (e.g. passwords, complex PINs). A striking result of the survey data suggests that this relationship does not exist with respect to practices around user privacy and data. 33.3% of all respondents, including 28.5% of users with expertise, reported always using public WiFi. A test for linear-by-linear association found evidence of a weak association between increasing expertise and use of VPNs, though this is probably related to the fact that the bulk of VPN users report high levels of knowledge (though the converse is not true).

Table 16
χ^2 tests on security knowledge (Q32) vs. soft practices (Q8-11, 13).

Variable	χ^2	*df*	*p*
Public WiFi use	2.144	1	.143†
Automatic WiFi	6.620	6	0.357
GPS usage	13.321	12	0.353
Bluetooth usage	17.897	12	.119
Concern about information storage	15.568	1	.000†

Table 16 illustrates this theme in the responses. A linear-by-linear test shows little if any evidence for expertise being associated with best practices in the use of public WiFi networks, and there is even less of a relationship with respect to automatic connection to public networks.

There is also no relationship visible in the data suggesting an association between expertise and use of a smartphones GPS services. In fact, a higher percentage of expert users report GPS on 24 hours a day (14/45) than users who report no knowledge of security topics (16/50). This is particularly interesting given that there is a strong trend between increased user expertise (Q32) and increased user concern about information on the phone (Q13).

6. Limitations

While the authors followed common practices as discussed in Section 3.1, bias may have been introduced in the questionnaire. We anticipate that any technology survey is going to attract a response pool that is more technologically literate than the general population, especially given the large number of questions. Another limitation in the results, addressed briefly in Section 3, is the method of collection of survey responses. As the survey was advertised on internet channels and through contact networks, the sample collected is not independent. Additionally, the randomness of the survey is somewhat limited by the fact that internet surveys like ours are answered by a self-selected pool of respondents.

With regard to the construction of the sample, the majority of respondents to the survey are under the age of 30, originate mostly from the US or South Korea and are unevenly spread across the highest level of education options. The sample and results would be improved by a more representative cross-section by these demographics, given the ubiquity of smart phones across demographic groups.

Certain parts of the statistical analysis, including the χ^2 tests for independence, would gain more power with a larger sample size. The main question that we used to sort respondents was question 32, and some of the groups were small enough that when cross-tabulated with the survey questions of interest resulted in contingency tables with cell counts too small to make χ^2 tests reliable. In these cases, with ordinal data we could employ linear-by-linear tests for trends. With nominal data, we had to fall back to descriptive methods.

7. Discussion and analysis

The findings of our survey show some interesting behavior which will be discussed throughout this section in response to the four research questions leading this survey.

[R1] Do smartphone users choose appropriate lock (screen) settings on their phone? Urban et al. (2012) "asked Americans whether they thought the information on their phones was more private, less private, or about as private as information on their home computers. [...] A large majority - 78% - of Americans consider information on their mobile phones at least as private as that on their home computers. Fifty-nine percent consider it about as private and 19% consider it 'more private'.' Consequently, many individuals are worried about their phones and information stored on them and therefore protect their phone from physically being accessed. In our sample, only 7.7% do *not* use any form of lock screen setting which means anyone with physical access to the phone does have access to all stored content. Compared to previous studies, there is a trend that more and more users require authentication (e.g., in 2010 only 13% secured their phone (Breitinger and Nickel, 2010), followed by 42.7% (Harbach et al., 2014) in 2014 and 72% (Anderson, 2017) in 2017). Moreover, many users (especially with the age of 40 or younger) rely on biometrics and set up their phone to automatically lock after inactivity. Overall, we conclude that the majority of users use appropriate settings but there is space for improvements. As an example, biometrics often requires a fallback authentication method (often PIN) which may only have 4 digits (complexity 10^4). A more secure option (and in keeping with the theme of the importance of usability) would be changing the alphabet to emojis where the complexity[4] increases to $\approx 2823^4$.

[R2] Do smartphone users follow good security practices to protect the data on their smartphone (besides lock settings)? In comparison to the lock screen settings, smartphone users employ inadequate additional security settings and often do not follow good security practices. According to our results, most smartphone owners do not use (third party) software to protect their phone (e.g., using a VPN when being connected to a public WiFi) which is a major concern. As shown by Alsaleh et al. (2017) in 2017 "many participants expressed their interest in taking protective actions but mentioned that a lack of knowledge about strategies that could help them protect themselves against potential IT threats prevented them from adopting secure behaviors. Some users indicated that they had no idea about the availability of smartphone security protection programs. Furthermore, most of our participants stated that they have no idea how to stay safe while they are connecting to public WiFi networks." Here, our conclusions are in line with Androulidakis and Kandus (2011), who argues that because "users fail to secure their phones they should either be educated or preferably presented with transparent security features, built in their phones, in order to mitigate the dangers". Additionally, Parker et al. (2015) proposed that "user education using a simple, non-technical design is key to encourage security awareness and adoption of security controls, especially in emerging markets." As a consequence of the unawareness, users tend not to change default settings Arthur (2013) and rely on them, which can be dangerous. Liu et al. (2011) found that for Facebook "36% of content remains shared with the default privacy settings [... and] match users' expectations only 37% of the time". To address this issue, it will require stricter laws and regulations similar to the recent law prohibiting default passwords for IoT devices in California.

[R3] Do smartphone users have differences in behavior and security choices for their desktops (compared to their smartphones)? Our sample showed that individuals are more likely to use security applications on desktops compared to smartphones (Section 4.6) while having more personal data on their smartphones (Table 3). This coincides with Murray (2014) who found that when "asked on which devices they used security software, 100% of survey respondents used some form of security software on their PC / Laptop / Desktop while only 31% found it necessary to install it on their smartphone." Interestingly, Chin et al. (2012) found that "most participants (over 80%) have or are willing to perform each type of task on their laptop. However, they may be less likely to do some types of tasks on their smartphone. We find that there is a significant difference in the users' willingness to provide their SSN, make purchases, access health / medical records, and access their bank account on their smartphone as compared to their laptop." To conclude: "compared to PC users where nowadays everybody is using (at least) an antivirus, [the low usage rate of mobile antivirus] shows a clear lack of security education and different mind-set" (Androulidakis and Kandus, 2011). Worryingly, even the choices for desktops are weak and many apparently do not know what they are using. One possible response is that "educating users about the security properties of the different media and particularly emphasizing the benefits of end-to-end encryption can go a long way in helping clear such misconceptions" (Chin et al., 2012). Users should also be educated on the amount of information that synchronized accounts are sharing across desktops and mobile devices.

[R4] Are smartphone users more cautious about hard security than soft security (i.e., protection from getting physical access to the phone vs. protecting data and privacy)? As outlined in Section 5.5, the majority of users is less cautious when it comes to soft security practices, i.e., using public WiFi or turning off GPS / Bluetooth, which could have multiple explanations. First, these issues are less omnipresent, and even individuals with higher cybersecurity familiarity may not be aware of them, e.g., one may not be familiar with the privacy concerns around being tracked through WiFi or Bluetooth. Due to the fast change of technology and security threats, users have to stay up to date, e.g., by reading an easy-to-understand news portal or participating in yearly knowledge-refresher seminars. Secondly, soft security practices are often harder to accomplish / less convenient due to the underlying unfriendly nature of the technology (Furnell, 2005). As an example, most devices will automatically add a WiFi network to 'preferred networks' and automatically connect to it in the future. A more security friendly option would be: *connect only this time*. Hence, we have to improve the design of applications / settings to ease security features usability (but should not forget that additional options / settings may be desirable by some users while others prefer convenience over security). Thirdly, "teens today grow up in a state of constant surveillance where there is no privacy, so they can't really have an idea of it being lost. The risk of the government or a corporation coming in and looking at their MySpace site is beyond their consideration" (Berton, 2006).

8. Concluding remarks and future work

The majority of users secure their phones from physical access (lock screen setting), but other security practices are mostly poor. Existing literature stresses cybersecurity and safety education, which have largely been left out from the educational system (Androulidakis and Kandus, 2011). Only now are universities starting to offer courses in cybersecurity specifically designed for non-majors because of the way that cybersecurity issues impact the everyday individual. Some make it mandatory for *all* students to acquire some form of cybersecurity training. For instance, Loyola University has Maryland[5] a 'Cyber Security and Digital Forensics' course that focuses on the basics of cybersecurity measures; University of Washington, Bothell, offered a cybersecurity course for non-majors that included a lab section, teaching students technical

[4] According to the FAQ, https://emojipedia.org/faq/#how-many (last accessed 2019-03-11).

[5] https://www.loyola.edu/academics/computer-science/degrees/non-majors (last accessed 2019-03-11).

skills, such as installing protective software, and teaching students how to regularly backup information to the cloud (Dupuis, 2017). However, there is currently no (mandatory) training or education for individuals already out of university.

While education is important, our results show that even advanced users (higher security familiarity) follow weak practices. This means that: *Education alone will not fix the issue*. Moreover, it will require: (1) rules and regulations for secure default settings (e.g., default encryption, turn off Bluetooth automatically after a period of time.), (2) easier-to-use security options (usable security (Furnell, 2016)) and (3) a change in mindset of the general public that security is important (e.g., although many are worried about cyber threats, individuals are less willing to spend money nor time on possible seminars (Ricci et al., 2018)).

On the other hand, as a community, users should be more curious about, e.g., explore all possible phone settings, inform themselves about the reasons for those settings, and adjust them according to their needs. Additionally, users will have to become more open regarding new technologies and receptive to trying them. Too many individuals still follow the saying: Never kill a running system.

The survey results indicate several areas of interesting future exploration, particularly in regard to the implicit trust that users have with default settings to keep their devices safe. For example, the responses to questions about security products on phones and PCs (see Table 15) indicate that many users just do not know what is installed on their devices. Modern PCs and Macs have built-in antivirus packages. Modern browsers have built-in password handlers, as do smartphones. A survey designed to probe this lack of knowledge would give insight into user practices and perceptions around these default programs.

Another interesting question is user beliefs about the priorities of the manufacturers phones and their operating systems. We saw that users seem to regard their data with less concern than their physical devices. It would be interesting to examine their perception of the data industry and the role that phone providers like Google and Apple play in collecting and using data, or the access to information that companies like Facebook gain once apps are installed on a phone.

Complete questionnaire

In the following is the complete questionnaire for the article *A survey on smartphone user's choices, awareness and education concerning security* currently under review.

Question 1: Where do you currently live?

- Drop down list provided

Question 2: Which age range do you fall under?

- 18–23
- 24–30
- 31–40
- 41–50
- 51–60
- over 60
- I prefer not to answer

Question 3: I identify as:

- Male
- Female
- Other (specify)
- I prefer not to answer

Question 4: What is the highest level of education that you have accomplished?

- Some high school
- High school graduate
- Technical training
- Some college
- College graduate
- Some postgraduate
- Post graduate degree

Question 5: Do you have a smart phone?

- Yes
- No
- I have a phone that is not a smartphone.
- I'm not sure

Question 6: If you answered yes to question 4, which operating system (OS) is your phone running? Otherwise select N/A

- iOS
- Android
- Blackberry
- Windows
- I'm not sure
- Other(Specify)
- N/A

Question 7: My mobile phone:

- Is always in my possession
- Is often left unattended (e.g. is on my desk during lunch break; left at home when I am out)
- Is sometimes left unattended (e.g. occasionally I forget it on my desk; leave it on the bar when going to the restroom)

Question 8: Do you use public available Wi-Fi's / Hotspots (e.g., at Starbucks, McDonalds, Hotels or Airports).

- Yes, always
- Yes, but only for browsing; no sensitive information is transferred (e.g., I am not using Banking Apps)
- Yes, but I use an additional encryption (e.g., a VPN software)
- No, I don't use Public WiFi's

Question 9: Does your device automatically connect to Wi-Fi networks?

- Yes, any open Wi-Fi (e.g., your phone automatically connects to the open Wi-Fi at Atlanta airport although you have never been there).
- Yes, to known ones (the ones I accessed in the past)
- No
- I'm not sure

Question 10: On average how many hours a day is your bluetooth enabled?

- Less than 2 hours
- between 2 and 4 hours
- between 4 and 8 hours
- between 8 and 12 hours
- 24 hours
- I'm not sure
- Never

Question 11: On average how many hours a day is your location/GPS enabled?

- Less than 2 hours
- between 2 and 4 hours
- between 4 and 8 hours
- between 8 and 12 hours
- 24 hours

- I'm not sure
- Never

Question 12: If you receive a text when your phone is locked does it show a preview of the message on the screen?

- Yes
- No
- I'm not sure

Question 13: Have you ever thought about all the information that is stored on your mobile phone?

- Yes, this worries me so I secure my device as well as I can
- Yes, this is somewhat worrisome to me
- Yes, but it does not worry me
- No

Question 14: How familiar are you with the security features on your phone?

- I have checked all the settings on my phone to secure it the best I can
- I change the default settings as issues come to my attention
- I use the default options

Question 15: Did you change your default browser settings?

- Yes
- No
- I use the default options

Question 16: Which of the following information do you have stored on your Mac/PC? (check all that apply)

- Autofill Saved Credit/Debit Card Information
- Autofill Saved Passwords
- Autofill Banking Information
- Calendar (i.e. Saved Events)
- Personal Photographs
- Cash Exchange Applications (i.e. Cash App, Paypal, Venmo)
- Contacts
- Email
- Health Information (i.e. Documents, Stored Health Data)
- IOT Applications/Autofill IOT Website Data (i.e. Thermostat Controls, Light Controls, House Alarm Controls)
- Maps (i.e. Saved Home Address)
- Social Media Applications (i.e. Facebook, Twitter, Snapchat)
- Voice Assistant (i.e. Siri, Google Now, Cortina)
- Wallet (i.e. Apple pay, Samsung pay, Android Pay)
- None

Question 17: Which of the following information do you have stored on your phone? (check all that apply)

- Autofill Saved Credit/Debit Card Information
- Autofill Saved Passwords
- Autofill Banking Information
- Calendar (i.e. Saved Events)
- Personal Photographs
- Cash Exchange Applications (i.e. Cash App, Paypal, Venmo)
- Contacts
- Email
- Health Information (i.e. Documents, Stored Health Data)
- IOT Applications/Autofill IOT Website Data (i.e. Thermostat Controls, Light Controls, House Alarm Controls)
- Maps (i.e. Saved Home Address)
- Social Media Applications (i.e. Facebook, Twitter, Snapchat)
- Voice Assistant (i.e. Siri, Google Now, Cortina)
- Wallet (i.e. Apple pay, Samsung pay, Android Pay)
- None

Question 18: How often do you preform backups on your Mobile phone?

- Once a week
- Once a month
- Once every 3 months Twice a year
- Once a year Never
- When prompted by my device

Question 19: How often do you preform backups on your Mac/PC?

- Once a week
- Once a month
- Once every 3 months Twice a year
- Once a year Never
- When prompted by my device

Question 20: Do you enter your Social Security Number on your device? - Mobile Phone

- Yes, it is stored on my device
- Yes, I enter it when needed
- No, I've never entered it

Question 21: Do you enter your Social Security Number on your device? - Mac/PC

- Yes, it is stored on my device
- Yes, I enter it when needed
- No, I've never entered it

Question 22: Which lock settings do you have in place on your phone? (check all that apply)

- None, I can use it immediately
- Pin (4 digits or less)
- Pin (5 digits or more)
- Password (has at least one character)
- Pattern (most commonly on Androids)
- Voice
- Fingerprint
- Face
- Lock your Android Phone from Device Manager
- Trusted Places (unlock when certain locations are reached)
- Keep your device unlocked when it is in your hand
- Unlock with trusted devices
- Other (please specify)

Question 23: Would you use a different lock setting if it was available on your phone? (check all that apply)

- None, I can use it immediately
- Pin (4 digits or less)
- Pin (5 digits or more)
- Password (has at least one character)
- Pattern (most commonly on Androids)
- Voice
- Fingerprint
- Face
- Lock your Android Phone from Device Manager
- Trusted Places (unlock when certain locations are reached)
- Keep your device unlocked when it is in your hand
- Unlock with trusted devices
- Other (please specify)

Question 24: How long after inactivity on your device does your device become locked?

- 30 Seconds
- 1 Minute
- 2 Minutes

- 3 Minutes
- 4 Minutes
- 5 Minutes
- More than 5 minutes
- Never

Question 25: If you use a pin (numbers only) to lock/unlock your device, how many different digits does your pin consist of?

- One (e.g 1111 or 2222)
- Two (e.g. 1122 or 5656)
- Three (e.g. 4432 or 4899)
- Four (e.g. 4567 or 8403)
- More than four
- N/A

Question 26: How often do you update your lock settings? (eg. Change your pin from 0000 to 1111)

- About every 30 days
- About every 90 days
- About every 6 months
- About every year
- Never
- When given reason to (i.e. someone knows your passcode)

Question 27: Which reasoning best explains why you chose the lock settings that you have?

- Convenience
- Forgetfulness
- Security
- Default Phone Settings
- No opinion

Question 28: Do you favor biometric lock options (eg. fingerprint) over knowledge base options (eg. password)?

- Yes
- No

Question 29: Have you ever had a mobile phone stolen? (If answer is no, you can skip the next 2 questions)

- Yes, on public transportation
- Yes, in the store
- Yes, at work
- Yes, in a crowd
- Yes, other (specify)
- No, but I lost it
- No

Question 30: What information/features were on your stolen phone? (Check all that apply)

- Saved Credit/Debit Card Information
- Saved Passwords
- Banking Application Information
- Calendar Events
- Personal Photographs
- Cash Exchange Application Stored Login Information (ie. Cash App, Paypal, Venmo)
- Stored Contacts
- Email
- Health/Fitness Stored Information (Height, Weight, Blood Type)
- IOT Application Controls (eg. Thermostat Controls, Light Controls, House Alarm Controls)
- Mapping Application (with stored addresses such as home)
- Social Media Login Information Stored (eg. Facebook, Twitter, Snapchat)
- Voice Assistant (i.e. Siri, Google Now, Cortina)
- Wallet (i.e. Apple pay, Samsung pay, Android Pay)
- None

Question 31: If your phone was stolen what actions did you take? (Check all that apply)

- Change your passwords
- Remotely lock your phone
- Remotely reset your phone
- Report the theft
- Nothing
- Other (Specify)

Question 32: How familiar are you with cybersecurity (on a scale of 1–5)?

- 1- I have no knowledge of related topics
- 2- I follow the news of related topics
- 3- I have read/taught myself about related topics
- 4- I have taken one or more courses in a related topic
- 5- I have a degree in this or a related field

Question 33: Which device is better secured; your mobile device or Mac/PC? (For instance, if your PC is encrypted, behind a firewall and using a Virus scanner while your phone is not, your PC has a better protection)

- Mobile Device
- Mac/PC
- Equally as secure
- Neither are very secure
- I'm not sure

Question 34: Which applications, if any, do you use to protect your Mac/PC or the data on it? (check all that apply)

- Applications to Securely Delete Files (i.e. CCleaner)
- Password Handling Applications (i.e. LastPass)
- Secure Messaging Applications (i.e. Signal)
- Virtual Private Network (VPN)
- Virus Scanner
- I'm not sure
- None

Question 35: Which applications, if any, do you use to protect your phone and the data on it? (check all that apply)

- Applications to Securely Delete Files (i.e. CCleaner)
- Password Handling Applications (i.e. LastPass)
- Secure Messaging Applications (i.e. Signal)
- Virtual Private Network (VPN)
- Virus Scanner
- I'm not sure
- None

Question 36: Is your device encrypted? - Mobile Phone

- Yes, I changed it
- Yes, by default
- No
- I don't know, I use the default settings

Question 37: Is your device encrypted? - Mac/PC

- Yes, I changed it
- Yes, by default
- No
- I don't know, I use the default settings

Question 38: Do you use anything else to protect your phone? Please explain

- Text submission accepted

Question 39: Please write any comments and/or suggestions that you may have:

- Text submission accepted

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank Dr. Joshua I. James for helping create and review the survey as well as for distributing it. Additionally, we would like to thank graduate researcher Laura Sanchez for her support and feedback.

References

Alani, M.M., 2017. Android users privacy awareness survey. Int. J. Interact. Mobile Technol. (iJIM) 11 (3), 130–144.
Alsaleh, M., Alomar, N., Alarifi, A., 2017. Smartphone users: understanding how security mechanisms are perceived and new persuasive methods. PLoS ONE 12 (3), e0173284.
Anderson, M., 2017. Many smartphone owners don't take steps to secure their devices. http://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/.
Androulidakis, I., Kandus, G., 2011. Mobile phone security awareness and practices of students in budapest. In: Proceedings of the 6th International Conference on Digital Telecommunications, pp. 17–22.
Arthur, C., 2013. Why the default settings on your device should be right first time. https://www.theguardian.com/technology/2013/dec/01/default-settings-change-phones-computers.
Berton, J., 2006. The age of privacy; gen y not shy sharing online-but worries about spying. San Francisco Chronicle 20.
Bhat, A., 2019. Leading questions: definition and characteristics with examples. https://www.questionpro.com/blog/leading-questions/.
Bitdefender.com, 2017. US: Personal data stored on smartphones by 50 percent of users. https://www.bitdefender.com/news/us:-personal-data-stored-on-smartphones-by-50-percent-of-users-3368.html.
Boyles, J. L., Smith, A., Madden, M., 2012. Privacy and data management on mobile devices. http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.
Breitinger, F., Nickel, C., 2010. User survey on phone security and usage.. In: BIOSIG, pp. 139–144.
Centre for the Advancement of Social Sciences Research (CASR), 2012. Report on privacy awareness survey on smartphones and smartphone apps. Technical Report. Hong Kong Baptist University. https://www.pcpd.org.hk/english/publications/files/smartphone_survey_e.pdf
Chin, E., Felt, A.P., Sekar, V., Wagner, D., 2012. Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, p. 1.
Cisco, V., 2018. Cisco visual networking index: forecast and trends, 2017–2022. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. White Paper.
Das, A., Khan, H.U., 2016. Security behaviors of smartphone users. Inf. Comput. Secur. 24 (1), 116–134.
Deloitte, U., 2016. Global mobile consumer survey: us edition. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html#form.
Dunning, J.P., 2010. Taming the blue beast: a survey of bluetooth based threats. IEEE Secur. Privacy 8, 20–27. doi:10.1109/MSP.2010.3.
Dupuis, M.J., 2017. Cyber security for everyone: an introductory course for non-Technical majors. J. Cybersecur. Ed. Res.Practice 2017 (1), 3.
Enge, E., 2018. Mobile vs desktop usage in 2018: mobile takes the lead. https://www.stonetemple.com/mobile-vs-desktop-usage-study/.
Felt, A.P., Egelman, S., Wagner, D., 2012. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices. ACM, pp. 33–44.
Fuller, J., 2008. How bluetooth surveillance works. https://electronics.howstuffworks.com/bluetooth-surveillance.htm.
Furnell, S., 2005. Why users cannot use security. Comput. Secur. 24 (4), 274–279.
Furnell, S., 2016. The usability of security–revisited. Comput. Fraud Secur. 2016 (9), 5–11.
Groeneveld, F., Borsboom, B., van Amstel, B., 2010. Over-sharing and location awareness. https://cdt.org/blog/over-sharing-and-location-awareness/.
Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M., 2014. It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: 10th Symposium On Usable Privacy and Security (SOUPS), pp. 213–230.
Hom, E. J., 2011. Mobile device security: startling statistics on data loss and data breaches. https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches.
Imgraben, J., Engelbrecht, A., Choo, K.-K.R., 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav. Inf. Technol. 33 (12), 1347–1360.
Ionescu, D., 2010. Geolocation 101: how it works, the Apps, and your privacy. https://www.pcworld.com/article/192803/geolo.html.
Klein, A., 2018. Computer backup awareness in 2018: getting better and getting worse. https://www.backblaze.com/blog/computer-backup-awareness-in-2018/.
Krebs, P., Duncan, D.T., 2015. Health app use among us mobile phone owners: a national survey. JMIR mHealth uHealth 3 (4), e101. doi:10.2196/mhealth.4924.
La Polla, M., Martinelli, F., Sgandurra, D., 2013. A survey on security for mobile devices. IEEE Commun. Surv. Tutor. 15 (1), 446–471.
Leswing, K., 2018. Over 80% of teenagers prefer iphone to android and that's great news for apple. https://www.businessinsider.com/apple-iphone-popularity-teens-piper-jaffray-2018-4.
Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A., 2011. Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, pp. 61–70.
Lookout, 2014. Phone theft in America: breaking down the phone theft epidemic. https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf.
Minar, N.B.-N.I., Tarique, M., 2012. Bluetooth security threats and solutions: a survey. Int. J. Distrib. Parallel Syst. 3 (1), 127.
Murray, C., 2014. Smartphone Security Risks: The Extent of User Security Awareness. Trinity College Dublin Master's thesis.
Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? security awareness in smartphone platforms. Comput. Secur. 34, 47–66.
Ng, A., 2018. Your smartphones are getting more valuable for hackers. https://www.cnet.com/news/your-smartphones-are-getting-more-valuable-for-hackers/.
Norton by Symantec, 2017. Norton WiFi risk report. https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf.
Pai, A., 2015. Survey: 58 percent of smartphone users have downloaded a fitness or health app. https://www.mobihealthnews.com/48273/survey-58-percent-of-smartphone-users-have-downloaded-a-fitness-or-health-app/.
Parasuraman, S., Sam, A.T., Yee, S.W.K., Chuon, B.L.C., Ren, L.Y., 2017. Smartphone usage and increased risk of mobile phone addiction: a concurrent study. Int. J. Pharm. Invest. 7 (3), 125.
Parker, F., Ophoff, J., Van Belle, J.-P., Karia, R., 2015. Security awareness and adoption of security controls by smartphone users. In: 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). IEEE, pp. 99–104.
Patterson, R., 2017. VPN statistics: What the numbers tell us about VPNs. https://www.comparitech.com/vpn/vpn-statistics/.
Ricci, J., Breitinger, F., Baggili, I., 2018. Survey results on adults and cybersecurity education. Educ. Inf. Technol. 1–19. doi:10.1007/s10639-018-9765-8.
Roy, A., Memon, N., Ross, A., 2017. Masterprint: exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Trans. Inf. Forensics Secur. 12 (9), 2013–2025.
Spool, J., 2011. Do users change their settings. https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/.
SurveyMonkey,. Avoid bad survey questions: Loaded question, leading question. https://www.surveymonkey.com/mp/5-common-survey-mistakes-ruin-your-data/.
Urban, J.M., Hoofnagle, C.J., Li, S., 2012. Mobile phones and privacy. BCLT Res. Paper Ser. https://www.ftc.gov/es/system/files/documents/public_comments/2013/12/00007-89101.pdf.
Vecchiato, D., Martins, E., 2015. Experience report: a field analysis of user-defined security configurations of android devices. In: Software Reliability Engineering (ISSRE), 2015 IEEE 26th International Symposium on. IEEE, pp. 314–323.
Willis, L.E., 2013. When nudges fail: slippery defaults. Univ. Chicago Law Rev. 80 (3), 1155.
Zaidi, S., Shah, M., Kamran, M., Javaid, Q., Zhang, S., 2016. A survey on security for smartphone device. Int. J. Adv. Comput. Sci. Appl. 7 (4), 206–219.

Dr. Frank Breitinger received the B.S. degree in computer science from the University of Applied Sciences in Mannheim (2009, Germany), his M.S. degree in computer science from the University of Applied Sciences Darmstadt (2011, Germany) and his Ph.D. degree in computer science from the Technical University Darmstadt (2014). He was self-employed for 5 years and a visiting researcher at the National Institute of Standards and Technology to lead NIST SP 800-168 on Approximate Matching. From 2014 - 2019 he was an Assistant Professor at the University of New Haven, CT before changing to the University of Liechtenstein. His research focuses on cybersecurity and digital forensics. Additional information about him and his work is on his website: https://www.FBreitinger.de.

Dr. Ryan Tully-Doyle received a B.S. degree in mathematics from California Polytechnic University (2001, San Luis Obispo), and a Ph.D. degree in mathematics from University of California (2015, San Diego). He is currently an Assistant Professor in

the Department of Mathematics and Physics at the University of New Haven. His research interests are in the areas of operator theory, complex analysis, and functional analysis, as well as in mathematical modeling and numerical approaches in undergraduate mathematics. Tully-Doyle is a member of the American Mathematical Society and the Mathematical Association of America.

Courtney Hassenfeldt received a B.S. bachelor's degree in Cyber Systems from the University of New Haven (2018, West Haven). She is currently a pursuing a M.S. degree in Cyber Security and Networks the University of New Haven. Her research interests are digital forensics, cybersecurity and education.