Why Do People Adopt, or Reject, Smartphone Password Managers?

Nora Alkaldi & Karen Renaud
School of Computing Science
University of Glasgow
Email: n.alkaldi.1@research.gla.ac.uk; karen.renaud@glasgow.ac.uk

***Abstract*—People use weak passwords for a variety of reasons, the most prescient of these being memory load and inconvenience. The motivation to choose weak passwords is even more compelling on Smartphones because entering complex passwords is particularly time consuming and arduous on small devices. Many of the memory- and inconvenience-related issues can be ameliorated by using a password manager app. Such an app can generate, remember and automatically supply passwords to websites and other apps on the phone. Given this potential, it is unfortunate that these applications have not enjoyed widespread adoption. We carried out a study to find out why this was so, to investigate factors that impeded or encouraged password manager adoption. We found that a number of factors mediated during all three phases of adoption: searching, deciding and trialling. The study's findings will help us to market these tools more effectively in order to encourage future adoption of password managers.**

***Index Terms*—Password managers, Adoption factors, Smartphone applications, Password security**

I. Introduction

Passwords constitute a crucial barrier to repel attackers. The barrier is weaker than it could be because users choose weak passwords, and those who do choose strong passwords are likely to write them down, which defeats the purpose of a secret authenticator [1, 2]. Many of these coping behaviours occur because users have difficulty remembering all their passwords. Smartphone password management adds another dimension to this, with limited screen size and keyboard multi-layer interaction making password entry arduous [3].

Password managers remove the effort from password management. These applications act as a vault for all of a person's passwords, with access controlled via one master password. The person only has to remember one password rather than tens of passwords, so memory load is drastically reduced. Password managers also auto-fill credentials, rendering shoulder surfing futile [4]. The resulting strength makes brute force and dictionary attacks less likely to succeed [5]. Despite these obvious benefits very few people use password managers. One study on 836 employees in a large organisation reported that only 1% used password managers [2].

This poor adoption applies to many security tools [6][7], [8], not only password managers. Poor usability has often been blamed for non-adoption of security measures [9, 1]. However, even usable techniques, such as biometric authentication, have not enjoyed widespread adoption [10]. A survey of iPhone users in Saudi Arabia [11] found that even though the majority of respondents agreed that TouchID was usable and secure, only 33% actually used it for securing their devices.

Much of the research literature focuses on the technical and design aspects of these tools, either attempting to improve usability, security, or both. To the best of our knowledge, only one study by Chiasson *et al.* in 2006 [12] considered the user's perspective. They detected usability issues, but did not really examine adoption factors. Further investigation is needed to understand why people do, or do not, use password managers.

In this paper we report on an investigation into the following:

- Current usage of password managers (in 2016).
- An investigation into factors impacting on the adoption, or rejection, of Smartphone password managers.

II. Related Work

Prata *et al.* [13] suggest that people go through three phases with respect to mobile phone apps: *Search, Purchase* and *Evaluate*. Häubl and Trifts [14] also refer to these three activities but do not incorporate them into a life cycle model. We depict the adoption phases in Figure 1, renaming "purchase" to "decide", since many of these apps are free. The figure shows how different factors feed into the phases.

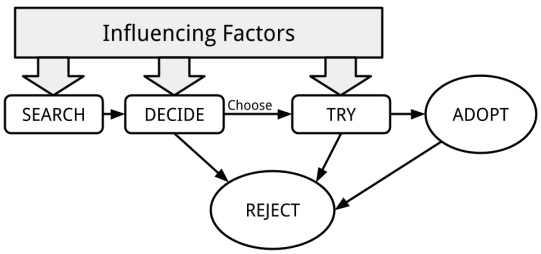

Fig. 1. Smartphone application adoption life cycle

EuroUSEC '16, 18 July 2016, Darmstadt, Germany

http://dx.doi.org/10.14722/eurousec.2016.23011

The **search** phase occurs when someone becomes aware of the existence of these applications. After the user initiates a search, a number of applications will be presented. The **decide** phase incorporates the decision to install one of the applications or to reject the idea. In the case of choosing to install one of these applications, the user moves to the third phase of the application life cycle where he or she **trials** the application and decides either to continue using it or to discard it. The arrow from Adopt to Reject was added based on arguments by Böhmer *et al.* [15], who talks about mobile app usage, describing the "try" phase, where an initial period of adoption can be followed by rejection, or adoption and continued use.

Tool Adoption Factors

1) General Adoption Factors: Nikou [16] systematically reviews the adoption literature and highlights three meta-categories of factors: **contextual, psychological & social** and **age-specific** factors. The first group includes *cost, perceived usefulness* and *context of use*. The second includes *social aspects* and *barriers to use*, while the third includes aspects such as *technology anxiety* and *resistance to change*. He emphasises the importance of the sociological & psychological factors in predicting adoption.

Hassan *et al.* [17] investigated the determinants behind Smartphone users' intention to adopt applications with students in Pakistan. They report on mostly contextual factors such as *perceived usefulness* and *perceived ease of use* but also refer to *social need* as an influential factor. These factors are confirmed by [18].

Another contextual factor was reported by Chong [19], who found that *cost* was a significant factor influencing the adoption of m-commerce. This finding was confirmed by [20]. Kit [21] identifies a number of pertinent contextual adoption factors: *performance expectations* and *effort expectancy*. The latter is confirmed by [22].

Another meta-category that emerges from the literature is that of *hedonic* factors [15]. Hassan *et al.*'s [17] study do not report on perceived enjoyment but Yang [18] confirms enjoyment as an adoption factor, as does Kit [21].

2) Specific App Adoption Factors: Some researchers have studied specific app adoption, such as the 'Snapchat' messaging application [23, 24, 25]. Vaterlaus *et al.* [23] studied Snapchat application usage by young adult Smartphone owners and found that it impacts their interpersonal relationships with friends and family. This adoption factor is confirmed by [26].

Cho *et al.* [27] developed a theoretical model of the adoption of health-related mobile applications. They reported that *consciousness, health information orientation, eHealth literacy, Internet health information use efficacy* and *subjective norms* all play a significant role in influencing the intention to use health applications. Some of these are clearly specific to health-related apps, and might not apply to security app adoption but subjective norms and efficacy (perceived usefulness) can be expected to influence adoption of other apps as well.

Some researchers focused on the impact of adoption factors related to biometric authentication on mobile phones. The impacting factors for these mechanisms are related to *ethical & social* concerns, probably due to the inherently personal nature of biometrics [28].

Sandholzer *et al.* [29] investigated adoption of educational Smartphone apps. They found that gender, interest in new technologies and perceived benefit (perceived usefulness) impacted adoption. Moreover, they also report that previous experiences of educational app usage predicted adoption. Kit [21] also found that previous usage (habit) influenced future adoption.

3) Summary: To summarise, the adoption factors that have been identified by other researchers are:

Contextual: perceived usefulness [21, 17, 27], perceived ease of use [17, 27], security [30], cost [19, 20], required effort [21], gender and interest in new technologies [29].

Psychological & Sociological: core features supporting relatedness/social need [23, 17, 25], subjective norms [27], ethics [28], habit [21].

Age-Specific: Technology anxiety, resistance to change [16].

Hedonic: enjoyment [21].

Few of these have been tested in the context of security tools, the focus of this paper. We will return to this list once we have presented our findings in order to consider which of these were confirmed, or not confirmed, by our study.

Smartphone Password Manager Applications

A number of password managers are available for mobile platforms. These applications differ in terms of features and functions that are offered to meet users' needs (see Table II in the Appendix)[1]. If one examines the table, we see that some of the applications store passwords in local storage (1Password); others rely on cloud services for storage and synchronisation (LastPass). Others use a hybrid approach which stores passwords both locally and on the cloud. Many of these applications require a strong master key (Dashlane); others have no restrictions on the chosen key so as to minimise forgetting (1Password). To support the memorability of the master key, some offer a 'hint' feature either shown on the login screen or sent to the registered email address. Some of these applications have started to utilise the presence of the 'fingerprint' feature on recent Smartphone devices as an alternative authentication mechanism. Based on this review it is clear that the poor uptake of these tools is not due to a lack of choice.

III. Methodology

Two types of data were collected:

1) reviews from application stores representing the opinions of users who chose to trial password managers;

[1]These examples have been selected based on their popularity in the iPhone App and/or the Google Play store. The cost and storage requirements were considered to cover a variety of features. The information was gathered in Nov 2015 and kept current by incorporating later reviews.

2) an online survey gathering 352 responses about password manager use, and exploring factors that encourage or discourage password manager adoption.

A. Reviews

As a preliminary investigation to help us understand why users use Smartphone password managers we analysed users' reviews of the two most popular password manager applications, namely LastPass and 1Password, on Google's Play store [31], and the Apple store [32] in three countries: UK, US and Saudi Arabia. The choice of three different countries was to include different populations of users to uncover region-specific usage patterns, and these three countries were chosen to reflect countries at different stages of technological development. A similar approach was used by [33] and [34] to reveal users' perceptions of applications in Google play and Apple stores. The idea was to use the most recent 20 reviews for each of the two password managers in each of the two stores. Reviews in Google play can be sorted by date, helpfulness or rate. It is recommended to have a minimum sample size of 20 for each culture measure in [35]. Surprisingly, in the Saudi Arabian store, no reviews or ratings were found for either application [2]. Although this does not mean that these applications are not used in Saudi Arabia, it might suggest they do not as readily review applications. It also gives an initial indication of the popularity of password managers as compared to other types of applications such as messaging apps. The latter are highly rated in Saudi Arabian App store. In the end, 120 user reviews were analysed to identify adoption factors.Among them, there were 60% positive reviews.A review was considered positive if it contained more positive than negative sentences. The sentence is rated as positive if it contains positives terms to indicate satisfaction.

B. On-line survey

An open-ended questionnaire was designed and validated by testing it with 34 randomly selected testers. Ethical approval was granted by the College of Science and Engineering at the University of Glasgow. It was posted in April 2016 via Google Survey. Using an online survey allowed us to elicit responses from Smartphone users worldwide and the afforded anonymity to offset social desirability bias [36]. Participants were recruited using a snowball sampling methodology, via email and social media such as WhatsApp, Facebook, Twitter and Path. To avoid incomplete participation due to fatigue, a maximum of five questions were posed. To encourage disclosure we did not collect any identifying information or demographics. We received 370 responses; 3 were incomplete, 4 skipped 1 question and 11 were either invalid or the respondents clearly did not engage with the survey. After excluding these responses we were left with 352 usable responses.

[2]This is also true in almost all app stores in other Arabic countries: UAE, Qatar, Bahrain, Oman and Egypt

IV. Results

A thematic analysis was conducted by two analysts (the authors). High level themes were established based on the analysts' individual reading of the collected data. The data were then coded according to the themes. A second analysis was carried out on the resulting categories aiming to explore sub-themes. The second analysis was done by one analyst and reviewed in detail by the other; an approach deemed sufficient giving that this is an exploring study.

After analysing the results of the survey and the reviews, some adoption- and rejection-related factors emerged which fell naturally into the three Smartphone Application Life Cycle phases, as shown in Figure 2.

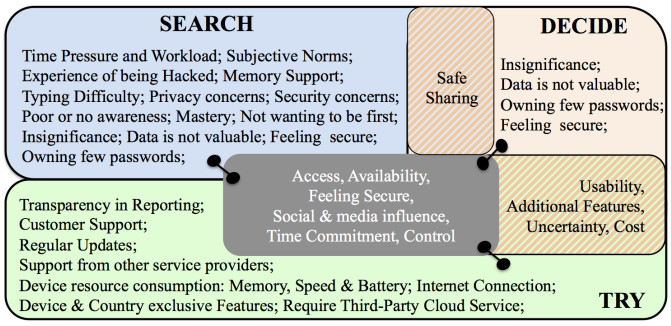

Fig. 2. Search, Decide and Try Factors

A. Password Manager Usage

Based on the online survey,we investigated the widespread of password manager usage. Although this was self-reported, 62 respondents (17.6%) said that they used a password manager application on their phone. However, only 24 of them (6.8%) provided the name of a secure password manager application; the rest either misunderstood the question or used other methods that they thought were password managers. Thirteen used PC-based password managers. About half of the Smartphone password manager users (32) misunderstood the term 'password manager application' (even though a brief description of these tools was provided at the beginning of the questionnaire). Some thought it was the screen lock mechanism. Two respondents considered their mailbox and notepad a tool for managing passwords. Four users stated that they used the Google Chrome password manager. While Google Chrome can overcome the password memorability issue, it constitutes a huge threat due to the fact that such passwords are easily accessed in the clear. The use of this memory aid might prevent adoption of a secure password manager. Usage was low: somewhat higher than that reported by Hoonakker [2] but, given the fact that almost a decade has passed, the increase is paltry.

B. Factors Leading to Adoption

Based on the analysis of the reviews and responses from the survey, some factors that influence users' decisions to start using password managers, or to continue using them in the

long term, have been identified. Where the theme confirms a theme suggested by the literature this is shown in brackets.

Subjective norms

One of the reviews emphasised the role of subjective norms i.e. the perceived social pressure to engage, or not to engage, in a certain behaviour. In terms of influencing people to use password manager applications:

"*In fact, it's not just about you, but about your family, friends, and colleagues. Have you considered that when your computer, mobile device, or online accounts are stolen or hacked that you may be exposing information about your family members, friends, and colleagues? Well, the truth is, you are (Review)*"

Time (Perceived Usefulness)

Password managers saved people time that had previously been spent on logging in manually:

"*go read a book or something with all the free time you now have.(Review)* "

Work Demands (Perceived Usefulness)

In some reviews, uses stated their need to accomplish their work on time that requires them to deal with many passwords, and they found it helpful to use such applications. For example:

"*Being an IT/Network Administrator, and having to remember over a 100 different logins and passwords, this thing is a life saver (Review)*"

"*this app has been essential for my day to day work with my 130 something logins (Review)*"

"*If you're like me, then you have 50+ login credentials throughout the Internet (Review)*"

"*It has truly kept me from losing my mind due to the amount of passwords stored in my head (Review)*"

Experience of Being Hacked (Experience)

A couple of reviewers stated that their experience of previous attack influenced them to start using password manager applications:

"*the headache that comes with it, as happened to me after my email address and password were kindly hacked into by someone in China and displayed online along with the other 300 000. I only found out by curiosity in searching for my email address.(Review)*"

"*It was literally just by sheer luck that I captured it before it happened. I used similar passwords for almost everything and let a colleague type in my password on my office PC while I was in the middle of something else. Big mistake. He "jokingly" logged onto my Twitter and Facebook accounts and put up comments without my knowledge. Although it was a joke to him and I wasn't upset, it made me think, so the following day I downloaded LastPass and changed all my passwords to 256 bit AES encryption.(Review)*"

Memory Support (Perceived Usefulness)

One of the strongest reasons for adopting these tools, according to both survey respondents and reviewers, is the memorability issue. The fact that many users possess increasing numbers of accounts makes it a challenge for most of them to construct unique and secure passwords that they can remember. This encourages the adoption of password manager applications. Here are some examples of 5-star rated reviews:

"*For me, it's a great tool not having to remember numerous login details...(Review)*"

"*I was struggling to remember all the different passwords I had at all the different websites I visited (Review)*"

"*I used to have a single password for all of my secure sites due to the hassle of trying to remember multiple ones. Then I discovered Lastpass. This makes logging in to all of your secure pages simple and hassle free. No longer do I have a single password, in fact, every password I have now is so complex, even I can't remember it. The only password I need to remember now is the Lastpass one itself.(Review)*"

Some survey respondent referred to memory-related reasons for adopting password manager applications:

"*Because I always forget my passwords (Survey)*"

"*I use a lot of different passwords that I forgot after a while or when i have to change the password to another, i keep remembering the old one not the new one (Survey)* "

"*My passwords are different for each account and difficult to remember them (Survey)*"

They said it helped to retrieve infrequently used passwords:

"*I'm no longer reluctant to create accounts for things I only rarely look at (because I don't have to worry about remembering login credentials and passwords); I never have to try to remember what I used for security questions and answers (because I record all of that into OnePass) (Review)*"

or being used years ago:

"*If you've ever found yourself staring blankly at the "security questions needed to verify identity" password reset prompt, because you have absolutely no clue what your favourite food was 8 years ago, then do yourself a favour and download Lastpass (Review)*"

Moreover, password managers help their owners to construct strong passwords instead of trading off between memorability and security of their passwords:

"*It's an incremental life-changer that actually lets you have stupid-complex passwords without having to remember them all (or use the same one over and over).(Review)*"

"*Now, instead of agonizing over a password I can remember vs. one that's secure, I am able to choose secure every time (Review)*"

In addition, some reviewers reported that these tools eliminate the need for fallback authentication when they forget their passwords:

"*Even those ridiculous fallback questions (what's your favourite movie... Like that's never going to change!).*

Even for my "mother's maiden name", I use secure random strings, unique per site, on most sites (Review)"

Typing difficulty (Effort Amelioration)

One of the reviews referred to the difficulty related to entering a secure password when using a phone which emphasises the importance of using supportive tools, according to the reviewer:

"*shudder to think what it would be like to type an actually secure password on one of your phones (Review)*"

Synchronisation (Perceived Usefulness)

This feature was a strong reason for adopting these applications. This might be because of the fact that many users own multiple devices that they need to access their accounts from. For example:

"*and keep everything in sync on multiple devices and computers (Review)*"

While users, in general, referred positively to this feature in their reviewse, some specifically gave evidence of their security awareness by being concerned about sending their passwords over the Internet. They prefer password mangers that provide safe synchronisation. For example:

"*1password can work and sync with other 1password installations without ever sending a single password over the internet (Review)*"

However, some users indicated their preference for a variety of different synchronisation methods:

"*One thing that has bothered me for a long time that I don't understand is the lack of options for syncing more than one vault. I don't have a Dropbox account and even if I did, shouldn't there be other ways to sync one of the vaults that may very well contain some sensitive information besides just Dropbox? I keep thinking one of these updates will address this issue but so far I am still unable to make use of a secondary vault because I don't have a Dropbox account. Just doesn't make sense.(Review)*"

Privacy

Those who posted positive ratings believe that their privacy is respected by the developers of the application:

"*you do not even have to tell them your email address (Review)* "

Some users believe that companies that provide these services have no interest in violating their users' privacy:

"*which is equal parts awesome and scary, right? All your passwords passing through the ether, supposedly protected, out there for the NSA or some other mad scientist to steal. With convenience comes risk. That risk is yours to take (or not). The purveyors of this software have a vested interest in not screwing with the trust of its customer base. For that reason you can (arguably) trust them to be hyper-vigilant in the maintenance and security of this software (Review)*"

This shows that user perceptions of an application's privacy preservation plays a role in their decision to adopt these kinds of tools.

User interface (Perceived Ease of Use)

The interface might contribute to influencing decisions to use a password manager:

"*The easy user interface, consistent quality and continual development keeps both desktop and phone/tablet software ahead of the competition (Review)*"

The participants who do not use password manager in their phone declared that the simplicity of the application might make it possible for them to start using these applications:

"*If I find a very simple app. With less text and more graphics (Survey)* "

However, some reviews referred to their bad impression of the user interface of some password manager applications. For example, this review is found in the 1password Android application:

"*why do I have to go very deep into the app before I can search for a login? That's a very frequent user journey! (Review)*"

Interestingly, other reviewers said they liked the user interface of this particular application:

"*Most user friendly interface I've come across in terms of password managers(Review)*"

Moreover, the reviews reveal that users prefer less interaction from the application such as using their phone's keyboard instead of using a bespoke keyboard:

"*I don't want to use a different keyboard, but I do want to autofill (Review)*"

Safe Sharing (Perceived Usefulness)

Some reviews pointed out that password manager applications allowed them safely to share their passwords and important documents with their partners:

"*Because it's securely synced to my Dropbox and shared with my wife, there's never a worry about getting locked out of a site. We use it on all our devices (Review)*"

"*makes it a breeze to share logins with my wife, as well as store and use personal info (Review)*"

Regular Updates to Meet User Needs (Perceived Usefulness)

Many users like regular updates and continued improvements to fix flaws, improve usability, and introduce new features:

"*The other great thing is that the company continually improves and optimizes the app, making it constantly better, faster and even more useful (Review)*"

"*This application has never failed me yet and more importantly the app is regularly updated (Review)*"

This may encourage reliance on these applications.

Customer support (Social Need)

Many reviews indicated that the customer support delivered made a good impression. This can be clearly seen from the responses to user reviews. This might positively impact the user's decision to continue using the system and meet the "relatedness" basic human need as can be seen in this review:

"*Their technical support truly listens to you. With most apps, you sometimes wonder if there is someone still on*

the other end. If there is any problem they will fix it (Review)"

"*they responded within minutes ! Their help was spot on correct, courteous, and quick (Review)*"

Moreover, some reviewers who were unhappy with the password manager referred to poor communication with the service provider:

"*contact support with a serious issue and they give you an unhelpful curt answer and when you try to follow up with a request for clarification they shut down the opportunity with a "status resolved" door slam in your face.(Review)*"

Transparency (Security)

The reviews reveal that when a password manager reported an attack, the transparency in explaining how that was happening could increase user confidence in the application:

"*Security now also explained on a previous episode how LastPass was hacked; which calmed my nerves after listening to the episode (Review)*"

Transparency in explaining how the system manages their data can influence decisions to adopt these applications:

"*I didn't trust these programs for a long time. Agile bits is very transparent about HOW your data is kept safe, so I started (Review)*"

One participant that open source code made the application more reliable:

"*Open source code and easy to understand description (survey)*"

Additional features (Perceived Usefulness)

Many reviewers were impressed with the different options and functions available. They reported that these apps have not only changed their password usage behaviour but also provide extra security features that make their lives easier:

"*I have scanned and added many important documents such as birth certificates, auto insurance cards, social security cards, passports, drivers licenses, medication lists, banking info and much more. ALL of these items are available to me and my wife anywhere, any time with the touch of a screen, and they are all encrypted using 256 bit AES encryption (Review)*"

"*but it acts as a complete storage for everything important such as wallet items, router & server info, and much much more (Review)*"

Usability (Perceived Ease of Use)

Due to security and/or usability requirements, the availability of the biometric fingerprint authentication mechanism seems to have had a big impact on usage of password managers. While iPhone users rated 1password because of the support of TouchID, Android users complained about the lack of support for biometric authentication, especially those who used 1password on their iPhone or had migrated from iOS. For example:

"*But there is no fingerprint support for Android. iOS version does have the fingerprint feature (Review)*"

Although some of the existing password manager applications already accept fingerprint authentication, some non-users said the incorporation of biometric authentication might make them start using these tools:

"*integration of the passwords with the fingerprint or any other biometric sensor (Survey)*"

"*If the password is my fingerprint or something like that.(Survey)*"

Some who used 1Password and password Saver applications claimed that they chose them because of the availability of the "finger print" feature:

"*No one can enter it unless with my finger print (Survey)* "

Feeling Secure (Security)

The majority of the reviewers and survey respondents who do use password managers on their phones stated that these applications increased the security level of their online accounts:

"*it is really really really encrypted (Review)*"

Some said their search for 'more safety' or 'security purposes' in general made them use these applications. Others indicated the importance of the password generator function provided by these applications, in terms of maximising the security of their passwords, and thus helping them stay secure on the web by generating 'long and complex' passwords. For example:

"*use 1Password generated password and feel safe that you have a password that cannot be hacked and it still easy to use (Review)*"

" *1Password looks great, comes with a strong password generator to help my pick good passwords every time I change one (Survey)*"

Furthermore, some are aware of the importance of having 'unique passwords' for each account:

"*My passwords are different for each account (Survey)*"

Also, some stated that password manager applications prevent poor password behaviour:

"*stop using the cat's name for every password on every site you access, and download this app (Review)* "

and make them aware of password weaknesses

"*Identify any password weakness or any password matching (Survey)*"

Some users pointed out the advantage of having a password manager when one of their accounts had been attacked, compared with the situation where they might have used the same password for more than one account. For example,

"*I use 1Password multiple times a day to recall and fill one of my 1600 or so unique and ridiculously complex passwords. If someone gives away one of my accounts, it is zero panic.(Review)* "

"*In summer 2014 when eBay passwords were compromised, I didn't worry. My eBay password was unique to eBay so I new my other accounts were safe. I simply changed my eBay password and went on with my day. OnePass makes this all possible (Review)*"

Moreover, the fear of certain kinds of attacks, such as shoulder surfing attacks, may influence Smartphone users to adopt password manager applications:

"*Will prevent others to see my password while I type it (Survey)*"

Social & Media Influence (Social Need)

The media, such as podcast shows, can influence users to attempt using a password manager. For example:

"*What convinced me to try it was the Mac Power Users' podcast #173 where they spent the whole hour on how useful 1Password is. Listen to that show and you will appreciate this app (Review)*"

Or it could persuade them to continue using the app

"*watched security now with the CEO of LastPass and after that interview I felt safe to still continue with LastPass (Review)*"

The reviews demonstrate the power of social influence in influencing user decisions about using password managers. The pronouncements of experts that users know from the media can play a role:

"*Steve Gibson will still be using LastPass and so will I (Review)*"

"*Just got done watching Joe on Security Now with Steve Gibson and Leo LaPorte. Joe is staying on with the team (Review)*"

Having those close to you interact with them directly also has an impact:

"*My husband encouraged me to download this app (Review)*"

"*I've recommended it in person to countless friends and they use and love it (Review)*"

"*Got multiple friends and family members to use their service (Review)*"

A number of participants who do not use password manager applications indicated that they might consider using them if they knew that other users were doing so:

"*If many people use it first without problems (Survey)*"

"*if it became popular and many people use it without any issues (Survey)*"

or if it was suggested by others:

"*suggested by closed friends (Survey)*"

"*friends recommendations (Survey)*"

Moreover one participant said "intervention of others" influenced her/him to use a password manager on her/his phone. This confirms the findings of [37] about the importance of our peers and significant others when it comes to Smartphone usage.

Access (Perceived Usefulness)

Users believe that using these applications ensure they are not locked out of a website, as they can access their accounts from any other device too. For example,

"*removes the aggravation that ensues from getting locked out of an account because of a lost password (Review)*"

Storing passwords in the cloud such as DropBox is seen as a positive feature since they can use their passwords from all their devices.

"*Now any computer or phone or tablet i use my passwords are stored and i can get to them (Review)*"

Availability (Perceived Usefulness)

password manager users reported in the reviews their satisfaction about having their password and important documents available at anytime:

"*I store passwords for sites, credit card details, passports and driving licence copies so I have them to hand 24/7 without the need to carry the originals, documents and secure notes.(Review)* "

C. Factors Leading to Rejection

Here are the factors that deter smartphone usesr from starting to search about password manager application or reasoning them for not starting to think about adopting these tool:

Poor or No Awareness

Many participants did not know about the existence of these applications. Some examples of their responses are:

"*I have no idea about their existence; (Survey)*"

"*I did not hear about it before (Survey)*"

I am already Secure (No Perceived Usefulness)

Some participants said that they did not need to use password manager applications because they believed that their current password behaviours were secure:

"*I use one strong password for everything (Survey)*"

or they used other security tools such as one-time passwords:

"*I don't feel I need it I use one-time password applications and I believe it is secure (Survey)* "

In addition, some participants were confident in their ability to remember their passwords:

"*I don't need it , can remember my passwords (Survey)*"

"*I can remember my passwords I use. And I would not feel safe with all passwords saved accessible through just one other password (Survey)*"

Some prefer to use the recovery function instead of a password manager:

"*Because I rarely forget my passwords, also I prefer if it happened and forgot the password to reset it (Survey)* "

Moreover, some participants believe that they do not need these supportive security tools because they are already taking online protective action by visiting only what they believe to be trusted websites :

"*Because I do not think I need it. I visit only popular websites so I do not need very very complex password for them (Survey)*"

However, some participants mistakenly considered themselves to be secure. Here are some examples demonstrating that people thought using the same password for many accounts was secure behaviour:

"*I didn't need it yet. I always choose the same password. I am good at memorising numbers and codes (Survey)* "

"*I have one password for all my accounts ..i don't need to write it (Survey)*"

"*Because I use similar passwords for different accounts so I do remember my passwords (I don't feel I need it) (Survey)*"

"*I dont feel like I need it.I use strong passwords by myself and they are very similar, so i dont get confused (Survey)*"

I have Few Passwords (No Perceived Usefulness)

Some participants did not see the need to use password manager applications because they do not have many online accounts:

"*I use to memorize my password since I don't have too many (Survey)*"

"*Also, I have a few passwords to remember so I don't need an external help (Survey)*"

Data is not Valuable (No Perceived Usefulness)

Some participants consider their data not to be valuable:

"*No reason I do not have anything to worry about I do not want to bother myself with complicated passwords (Survey)*"

"*I have not got important things on my mobile (Survey)*"

"*Maybe if have important accounts like a bank account (Survey)*"

Insignificance (No Perceived Usefulness)

Some participants did not see the need to have strong passwords as they believed that their online accounts would not be attractive to attackers.

"*If I get rich or became a politician then I would think about strong passwords(Survey)*"

"*I believe that it is too much for me to have such applications, as i am not a celebrity or politician and therefore have no stalkers (Survey)*"

"*I don't use my Smartphone for my critical information. I prefer to use it as a communication device to call and message and browse on google, not to login into any important websites because i believe i might forget it somewhere. so i prefer to check emails and important login information through my desktop computer (Survey)* "

Not wanting to be first

As this tool is not widely known by smarphone users, many thought it was a recent development and they believed and thus did not want to be the first to take the risk in using such an applications:

"*Not that popular so it must be not that good (Survey)*"

"*If i see many people use it and like it or famous people use it and like it (Survey)*"

Mastery

Some participants attribute their decision not to use a password manager to their desire to challenge themselves by retrieving the right password from their memory.This can be explained by Pink's motivation theory [38] as the human basic need for 'mastery'. It can also be illustrated by the need for 'competency' ,according to self determination theory [39].

"*I like to challenge myself by remember my passwords .. feel proud of myself it's not a joke! (Survey)*"

"*I do not like to depend on technology to remember all my passwords This will make my memory lazy (Survey)*"

Security Concerns

While many password manager application users believed that these applications maximised their online security, those who chose not to adopt these tools had concerns about their security:

"*I always feel that the security of these applications are not good (Survey)*"

"*I do not fully trust that the software will be able to provide enough security. After all, there is no such thing as an impenetrable security, especially in digital world. Should someone hack into my account, they will know all my passwords. Even though there is a risk that I will not be able to remember some of the passwords, then at worst, the data will just be lost (Survey)*"

Particularly, the fact that these type of systems have a single point of failure:

"*Risk of keeping all eggs in one basket (Survey)*"

"*May be because when the attacker can get inside the password manager, he/she can take all my passwords.But when attacker get one password and get inside my email that will be more secure because I only lose the access to my email account only not all accounts (Survey)*"

" *It is a risky application if master key is attacked then every thing gets lost (Survey)*"

"*... its going to be easier for other people to hack my account since they can get the password from the password manager (Survey)*"

They worry that these types of systems might attract attackers:

"*I don't like the idea of having all my passwords stored in one place (The password manager app) which will be most likely on the list of hackers to crack and if they already did crack it, it will obviously be the first thing they will look for after attacking my PC or Phone and that doesn't quite feel safe, nor assuring. To me using a word document that doesn't look like anything special feels safer and you can lock it with a password too (Survey)*"

"*I don't trust applications. Hackers may use these kinds of applications to achieve their personal and illegal goals (Survey).*"

or even if it lands up in the hands of another person:

"*My accounts are very important to me and cannot trust putting them in danger of getting lost if my phone get damaged or stolen (Survey)*"

"*Because my cell phone is sometimes used by my children and other family members there is a risk to use it (Survey)*"

Also some participants believed that their phone itself was not secure; that it might have viruses that could affect their passwords if they used a password manager:

"*It's a security matter. I use it in my computer because it has anti virus and firewall and sometimes when I google a website it tells me which website is risky. My phone has non of these things and I have some applications in my phone games that I believe they are not very safe (Survey)*"

"*Cuz my phone got viruses and not safe (Survey)*"

Also, they seem aware of the security risk of using public Internet services :

"*I use public wifi networks which make it much easier for attackers to attack my passwords if I used password manager application(Survey)*"

In addition, users seem unsure about their current security knowledge and information and thus do not want to put themselves at risk of having yet another critical application to look after:

"*advices how to stay secure when using it (Survey)*"

Privacy Concerns

While some reviewers show their confidence about preserving their privacy by the serive providers as explained earlier, some of those who chose not to adopt password manager cited privacy concerns a lack of trust in the vendors. For example,

"*personally I don't know anything about the developers or the app source (Survey)*"

"*I don't trust these application.They made in U.S. to know everything about us.Now they know everything but not passwords so they made this application to trick us. If you see imges of Google data centre you will not use these kinds of systems anymore (Survey)*"

"*Because I don't trust the software not to collect my passwords for itself (Survey)*"

"*I dont trust it, as I am not sure about the developers of this app and what they can do with my details (Survey)*"

Also, some stated that if they trusted the developers then that would make it possible for them to use these applications:

"*May be if it is:..from a trustful source (Survey)*"

For example if it is developed by a well known orgnization:

"*A password manager that is developed by popular companies like google, apple (Survey)*"

"*If distributed by trusted source or big industry name like apple keychain (Survey)*"

or developed by people who they trust

"*Nothing will make me use it unless I develop it myself or someone trusted like people in universities (Survey)*"

others said if the application was open source they might use it:

"*Open source code and easy to understand description (Survey)* "

However, one of the reviews referred to the importance of trading off between privacy concerns and their security password behaviour:

"*This is not an app for nerds, geeks or those who overdramatise the importance of internet security. Put simply, if you care in any way for your personal privacy and / or the stuff you store and access online, you need to wise up, stop using the cat's name for every password on every site you access, and download this app (Review)*"

Smartphone users may encounter some factors that affect their decision to adopt one of the available password manager applications:

Uncertainty

Some participants who not use these applications referred to a lack of understanding about how these applications build and work, which constitute a barrier in terms of trusting these tools:

"*...After I did a quick reading about it I have an idea but I do not know how it works? I don't mean how I use it but how this application takes my passwords and make them strong and where are they kept? Is it in America? All these things I need to know before trusting these applications (Survey)*"

"*.. not understand how they are implemented; the available information for these application is complicated and not clear (Survey)*"

"*More elaboration on how to really function with less complicated terms of agreement (Survey)*"

In some cases, smartphone users might be thought of using password manager applications and adopted one of these tools but then uninstalled it. These are some factor that influenced their decision:

Device Speed (Negative Features)

According to the reviews, some Smartphone users complained about the efficiency of their devices after installing and using password manager applications:

"*Also for some reason it makes my Mi 3 significantly slow when it is running on the background, so only three stars for now.(Review)*"

"*According to System Panel this app is using a lot of CPU cycles even though it's not being used that much (the icon does keep coming up in the status bar for no known reason). Considering uninstalling, at least temporarily as an experiment (Review)*"

Device Memory & Battery (Negative Features)

As the memory size on Smartphones is relatively small compared with other computer devices users are careful about apps they install. They only use applications that they believe they need. Some users indicated that they did not have enough space to install a password manager application. For example:

"*Takes up a lot of battery and RAM (Survey)*"

"*i am enough with using application,i use note or my mind (Survey)*"

"*I don't have enough space in my phone Even i delete the applications that I have in my phone when I need memory to capture a moment for my kids and then I re-install the apps later when I find space. In the case of password manager I can't do that! (Survey)*"

In the review, one of the users pointed out the preference of having lastPass over Dashlane application because of their size:

"*Lighter than Dashlane, which makes LastPass more preferable than Dashlane (Review)*"

Some participants expressed concern about apps consuming the battery:

"*latest version sucks more battery than the screen! Have it force stopped on phone, just turn it on when I need it (Review)*"

Battery consumption clearly negatively affects the users experience.

Connectivity (Negative Features)

Some users indicated that having a poor Internet connection was a usage barrier:

"*Poor Internet in my country I do not want to use online password account each time I want to access one of my accounts. This will double my online access +sometimes I want to access my email to know something but I don't have Internet in my place so I call one of my family member to see my email If my password is in this application then how can they access my email (Survey)*"

An Android user who had already adopted LastPass complained about the Internet connection. This clearly impacts their experience and the continued adoption of these tools:

"*Very nice and convenient app that let you save all of your passwords. But very difficult to access it when the Internet connexion is poor.(Review)*"

Differences Across Platforms (Negative Features)

Many reviews claimed that developers only focused on iOS but not Android and they considered the Android version to be inferior to the iOS one. Some reviewers complained about the lack of features such as fingerprint authentication in the Android version of 1Password, especially those who used the same application on the iOS platform:

"*I have this on all my iOS/OSX devices and it's so much nicer on those platforms.... Only reason I'm even using it on Android is all my stuff is already saved to it from Apple devices. I wouldn't have given this app a shot at all if it wasn't for the other version hooking me in (Review)*"

Another review on LastPass:

"*But there is no fingerprint support for Android. iOS version does have fingerprint feature (Review)*"

Another negative review is about paying for the same application on each different platform while the point is to synchronise passwords across devices:

"*Bit tired of having to pay for each different OS. Isn't the whole point of this app to be able to sync credentials across devices and operating systems? Bit cheeky then to charge extra for that (Review)*"

Linkage with Other 3rd Party Services (Negative Features)

In the reviews, some users complained about having to use an additional account with a specific service provider such as DropBox in order to be able to synchronize their passwords across other platform and some suggested other preferable methods like Wi-Fi sync or accounts e.g. iCloud and Google Drive:

"*My understanding is that I must use Dropbox to sync the vault on mobile. Since I don't use my Dropbox on my work computers, this makes complete sync impossible (Review)*"

"*Then, they took away WiFi sync and added iCloud – except the desktop doesn't support iCloud yet. So there's no real migration path. I don't want to have to install 3rd party dropbox accounts and junk to make this work. WiFi should be included until they get iCloud in the desktop then they can do away with WiFi. But this is terrible and leaves me with mobile devices now that can't sync with my desktop anymore! (Review)* "

Country-Specific Features (Negative Features)

Reviewers pointed out that some features in the password manager are exclusive to a certain community and therefore it affects their experience:

"*I would like to see change would be a better selection of items for a global community rather than this extremely American feel to data capture. So UK NI number, drivers licence etc. Not just UK but other countries (Review)*"

"*App can't cope easily with uk type of banking password structures which cycle at each login, crashes internet explorer frequently requiring a laptop reboot and freezes regularly (Review)*"

They are not supported by other web accounts (Negative Features)

Lack of support from other service providers may affect Smartphone user willingness to rely on these tools for managing their passwords. Some reviews claim that they found applications and web sites that are not supported by the applications such as

"*The only problem is with iOS and more crucially with web and app developers who don't support this. Everyone needs to complain when they come upon web sites that prevent password managers from seamlessly entering passwords and credit card info (Review)*"

Some websites, such as British Gas, do not support the use of any password managers on their login page. This might be a barrier for some to integrate in using these applications.

Uncertainty

Some people don't know enough to deploy these applications. This might be due to usability issues. For example, some users lacked confidence:

"*If you asked me how to get a credential from 1P into any other app, I wouldn't be able to tell you (Review)*"

"*Because I can not understand how I can use it for my account that I use now. I use the google one in my computer because it already pop up and ask me do you want to save your passwords . Even though it can't help me to make a strong ones (Survey)*"

Cost

In some cases in the reviews and the survey, the cost was a barrier to adopt these systems. They stated that they are unready to pay so much for a secure password manger when other password mangers are free. For example this review is found in 1Password in UK Apple Store:

"*I planned to buy it for my partner but the price seems a fair bit higher (Review)*"

"*Being free of charge.(Survey)*"

On the other hand, in some other reviews, users hesitated to trust their passwords to free applications, they believes that free apps were not really free, and some have tracking included. They also feel that most free applications have security weaknesses:

"*Are you sure you trust your password to a free app? Free apps aren't really free, some have tracking included, pesky advertisements, or they might report back to the "mother ship" (Review)* "

Time Commitment (Perceived Effort)

For many users, security is a secondary task required primarily in order to complete their primary task [40]. Therefore, people are less willing to spend time reading about how this tool works or how to use it. Moreover, people do not have time to think about the accounts they have and each associated password. Quotes from the participants' responses suggest that time might be a barrier to adoption:

"*I don't have time to search more about it ;so it better leave it (Survey)*"

"*I don't have time to find my accounts and each password and give them to the password manager (Survey)*"

Control

Some users were concerned about not being able to maintain control over their passwords when using a password manager. This can be explained, according to self determination theory [39] and Pink's Motivation theory [38], by the human need for 'autonomy' when interacting with the digital world. Autonomy is defined as the sense of freedom and control over ones own choices. This can be seen in these responses to the question about the reason for not using these applications:

"*I prefer to keep my password under my control.(Survey)* "

"*Password manager is not good you can lose control of your passwords.(Survey)* "

"*Fear of not being able to have control over my passwords in case it's being attacked or I forget the master key.Fear of being under the control of this app developer. (Survey)*"

Moreover, due to the fact that some of these applications do not provide a recovery plan for the master key, some users post negative reviews about not being able to control their passwords:

"*Recovery options terrible..Just set it up. Worked fine until I logged out and could not quite get password right. Now totally inoperable. Cannot login cannot reset cannot delete account and start over. Electronic version of a paperweight. (Review)*"

"*What if I forget the master password? (Review)*"

D. Reprise of Adoption Factors

Section II-3 identified a number of adoption factors from the literature, as summarised in Table I. Our findings confirmed a number of contextual, psychological and sociological factors but did not detect anything that hinted at an interest in new technologies impacting adoption. We did not explicity test for hedonic or age-related factors. This does not mean that they are not influential, only that they did not emerge from our analysis. In fact, we believe that they could provide a fruitful avenue for further attention since they have proved influential in other contexts, and might well encourage adoption in this context too.

V. Discussion

We identified a number of factors influencing password manager app adoption in different phases of the application lifecycle. A number of these confirm the findings of [41]. Certainly lack of awareness was a strong theme in both studies. People will not even embark on the life cycle depicted in Figure 1 if they do not know of the existence of password manager tools. The lack of awareness is puzzling since these applications have been available since 1999 [42]. Due to the sensitivity of password data and with so few people using them, it is unlikely that they are hearing about the apps from friends and family. So, how would people become aware of these apps?

Some of the reviews said adopters recommended the password manager to others, so if a certain critical mass of people start using them, many more will probably follow. Also, some of reviewers spoke about hearing about famous people using password managers and said that they adopted them as a consequence. There is a clear need for effective marketing if more people are to adopt these tools.

However, even if people become aware of the apps, they might still not embark on a search process to consider installing one. Many people mistakenly think their current password practice is secure [43]. Some participants believed that they did not need security support tools because they only used one password for all their accounts. It seems that, in addition to making people aware of these password manager apps, we should also work on disseminating "good practice" with respect to password behaviour so that they understand their current behaviour is making them vulnerable to attack.

This study revealed factors that might deter adoption even if users have heard about the app, and were sufficiently interested in using the tool. A number of our respondents did not understand how this application worked and was used. Due

TABLE I
ADOPTION AND REJECTION FACTORS IDENTIFIED IN THIS STUDY

	ADOPTION Factors	REJECTION Factors
Contextual	Time, Ease of Use, Perceived Usefulness, Perceived Effort Amelioration, Experience	No perceived usefulness, Negative Features, Cost, Perceived Effort
Psychological & Sociological	Subjective Norms, Social Need, Security, Privacy	Not wanting to be first, Privacy Concerns, Security Concerns, Competency, Control, Mastery, Uncertainty

to the critical nature of the data manipulated by password managers, users need to be able to trust these systems and they need to know how their passwords are secured and stored, at the very least. It is unfortunate that most of the existing applications in App stores fail to report how these password manager actually work. Anaylew reports that Apple consumers consider the description and the screenshots in App Store Product Pages when they are interested in buying an application [44]. One reviewer suggested the use of video clips to improve the user experience. Yet most of existing password manager applications in Apple and Google play stores only provide a description of how the application is used. A few provide screenshots of the application interface and they mostly focus on demonstrating the features provided by these tools. They seldom explain how the data is secured. Only a few provide demonstration videos: 1password and mSecure in the Apple store and DashLane and RoboForm in Google Play store.

Other users felt that such a password manager would violate their basic human needs of autonomy, mastery and competency. Humans need to retain control [45, 38] and password management is no different. It might be that in trying to be helpful by taking away all password-related concerns these apps make people feel that they have lost the sense of control they need. Password managers might need to work on giving people a sense of control during operation.

We should also briefly consider the hedonic quality of these apps, mentioned by [21] as an adoption factor. No one in our surveys and reviews spoke about the app being "enjoyable", yet this is clearly something people want. They spoke about being reassured, the reduction of effort, the relief of not having to manage passwords, but no mention was made of enjoyment. Hassenzahl *et al.* polled 548 people and reported that hedonic quality was strongly associated to positive experience of an app [46]. This is yet another non-functional quality that app developers could pay attention to, in order to improve adoption.

Future research should consider the following research directions:

SEARCH: How can password managers be advertised more effectively to build up a critical mass of users who could, in turn tell other users about this kind of application?

DECIDE: How should password manager apps be described in the app stores so as to engender trust in users engaged in the decide phase of the life cycle?

TRY: Two questions arise. (1) How can password managers be designed so as to give the user a sense of retaining control over his/her passwords? (2) How can password managers be designed with enjoyment in mind?

VI. LIMITATIONS AND FUTURE WORK

There are some limitations to this study that have to be acknowledged. In the first place, we deployed snowball sampling to recruit respondents, so our sample can not be considered representative of the entire population. Hence the factors this exploratory study revealed will have to be confirmed with a wider-ranging study, consulting a more representative sample.

The online survey did not consider cross-cultural differences. This is relevant because people might well be influenced in their adoption decisions by country- or culturally-specific factors. For example, in some Nordic countries the eID is used as a country-wide two-factor authentication method. A cross-cultural study is needed to ensure the validity of adoption and rejection factors in other cultures.

We did not collect demographics in the online survey. We did this to encourage full discloure, but this also meant we could not explore gender or age differences in responses. Future studies will need to pay attention to these factors.

The study did not attempt to weight the impact of the different factors on adoption and rejection, nor did we attempt to map factors to actual usage. These aspects will have to be explored in follow-up studies.

VII. CONCLUSION

Password managers can ameliorate password management difficulties experienced by Smartphone users. Cost is no bar to their use, since many are free. Yet, despite the obvious benefits, widespread adoption has not occurred. We examined online reviews of password managers and elicited opinions from 352 respondents. A number of factors impacting adoption were identified. Poor advertisement and a failure to reassure potential users about the trustworthiness of these applications could well explain the poor uptake of these tools. Moreover, the analysis reveals that designers should pay more attention to the user experience. The factors reported in this paper can help developers to design and market systems to encourage adoption.

ACKNOWLEDGEMENT

We want to thank Rosanne English for her very helpful comments on an earlier draft of this paper.

TABLE II
A REVIEW OF SMARTPHONE PASSWORD MANAGER APPLICATIONS

	LastPass	1Password	iCloud Keychain	DashLane	mSecure
Synchronisation	Premium	Dropbox, iCloud, Local Folder ,Wifi	only Apple devices	Optional	Optional
Cloud	Yes	Optional	Yes	Optional	Optional
Auto Populate	Optional	Optional	Optional	Optional	Optional
Credentials	Email Address for Cloud Account	None	Email & Phone Number	Email	Email for Backup
Storage	Own Cloud Service	Local Device	Cloud	Local or Dashlane Servers	Local or Cloud
Encryption	AES 256-bit	AES 256-bit	AES 128-bit	AES 256-bit	Blowfish 256-bit
Generator	Optional	Optional	Optional	Optional	Optional
Authentication	Premium	Fingerprint, one-time (Pro)	No	Fingerprint	N/A
Recovery	Email Hint	Hint display after 4 wrong passwords	No Recovery	Reset Account	Password Hint
Password Strength	8 Character	None	4 Character	8 Character with 3 types	None
Cost	Free or 8.99/year for premium	Free or Pro (7.99)	Free	Free or Premium (29.99 a year)	iOS:7.99 Android:6.99
Rating	Google play: 4.6 (62350 rating) US: 3.5 (2476) UK: 3.4 (294 ratings)	App store: UK: 4.5 * (2322 Ratings) US: 4.5 (14912 Ratings) Google play: 4.3 (17033 rating)	N/A	UK: 4.4 (985 rating) US: 4.4 (10605 Ratings) Google play: 4.5 (30599 rate)	US: 5 (27 Ratings) UK: 4.4 (1339 ratings) Google play: 4.5 (9275)

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[2] P. Hoonakker, N. Bornoe, and P. Carayon, "Password authentication from a human factors perspective: Results of a survey among end-users," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 53, no. 6, pp. 459–463, 2009.

[3] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance," in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, pp. 461–470, ACM, 2014.

[4] H. S. Al-Sinani and C. J. Mitchell, "Using CardSpace as a password manager," in *Policies and Research in Identity Management*, pp. 18–30, Springer, 2010.

[5] P. Gasti and K. B. Rasmussen, "On the security of password manager database formats," in *Computer Security–ESORICS 2012*, pp. 770–787, Springer, 2012.

[6] A. Das and H. U. Khan, "Security behaviors of smartphone users," *Information & Computer Security*, vol. 24, no. 1, pp. 116–134, 2016.

[7] N. O. Alshammari, A. Mylonas, M. Sedky, J. Champion, and C. Bauer, "Exploring the adoption of physical security controls in smartphones," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 287–298, Springer, 2015.

[8] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

[9] S. Furnell, "Why users cannot use security," *Computers & Security*, vol. 24, no. 4, pp. 274–279, 2005.

[10] N. Alkaldi and K. Renaud, "Why do People Adopt, or Reject, Smartphone Security Tools?," in *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). Frankfurt, Germany*, July 19-21 2016.

[11] A. A. Al-Daraiseh, D. Al Omari, H. Al Hamid, N. Hamad, and R. Althemali, "Effectiveness of iPhones Touch ID: KSA case study," *Editorial Preface*, vol. 6, no. 1, 2015.

[12] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A usability study and critique of two password managers.," in *Usenix Security*, vol. 6, 2006.

[13] W. Prata, A. de Moraes, and M. Quaresma, "Users demography and expectation regarding search, purchase and evaluation in mobile application store," *Work*,

vol. 41, no. Supplement 1, pp. 1124–1131, 2012.

[14] G. Häubl and V. Trifts, "Consumer decision making in online shopping environments: The effects of interactive decision aids," *Marketing science*, vol. 19, no. 1, pp. 4–21, 2000.

[15] M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer, "Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage," in *Proceedings of the 13th international conference on Human computer interaction with mobile devices and services*, pp. 47–56, ACM, 2011.

[16] S. Nikou, "Mobile technology and forgotten consumers: the young-elderly," *International Journal of Consumer Studies*, vol. 39, no. 4, pp. 294–304, 2015.

[17] M. Hassan, R. Kouser, S. S. Abbas, and M. Azeem, "Consumer Attitudes and Intentions to Adopt Smartphone Apps: Case of Business Students," *Pakistan Journal of Commerce and Social Sciences*, vol. 8, no. 3, pp. 763–779, 2014.

[18] H. . Yang, "Bon appétit for apps: young american consumers' acceptance of mobile applications," *Journal of Computer Information Systems*, vol. 53, no. 3, pp. 85–96, 2013.

[19] A. Y.-L. Chong, "A two-staged SEM-neural network approach for understanding and predicting the determinants of m-commerce adoption," *Expert Systems with Applications*, vol. 40, no. 4, pp. 1240–1247, 2013.

[20] T. Tsu Wei, G. Marthandan, A. Yee-Loong Chong, K.-B. Ooi, and S. Arumugam, "What drives Malaysian m-commerce adoption? An empirical analysis," *Industrial Management & Data Systems*, vol. 109, no. 3, pp. 370–388, 2009.

[21] A. K. L. Kit, *UTAUT2 influencing the behavioural intention to adopt mobile applications*. PhD thesis, Universti Tunku Abdul Rahman, 2014.

[22] L. Dennison, L. Morrison, G. Conway, and L. Yardley, "Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study," *Journal of medical Internet research*, vol. 15, no. 4, p. e86, 2013.

[23] J. M. Vaterlaus, K. Barnett, C. Roche, and J. A. Young, ""Snapchat is more personal": An exploratory study on Snapchat behaviors and young adult interpersonal relationships," *Computers in Human Behavior*, vol. 62, pp. 594–601, 2016.

[24] L. Piwek and A. Joinson, ""What do they Snapchat about?" Patterns of use in time-limited instant messaging service," *Computers in Human Behavior*, vol. 54, pp. 358–367, 2016.

[25] B. Xu, P. Chang, C. L. Welker, N. N. Bazarova, and D. Cosley, "Automatic Archiving versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pp. 1662–1675, ACM, 2016.

[26] D. G. Taylor, T. A. Voelker, and I. Pentina, "Mobile application adoption by young adults: A social network perspective," *International Journal Of Mobile Marketing*, no. 2, pp. 60–70, 2011.

[27] J. Cho, M. M. Quinlan, D. Park, and G.-Y. Noh, "Determinants of adoption of smartphone health apps among college students," *American journal of health behavior*, vol. 38, no. 6, pp. 860–870, 2014.

[28] S. Thavalengal and P. Corcoran, "User authentication on smartphones: Focusing on iris biometrics.," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 87–93, 2016.

[29] M. Sandholzer, T. Deutsch, T. Frese, and A. Winter, "Predictors of students self-reported adoption of a smartphone application for medical education in general practice," *BMC medical education*, vol. 15, no. 1, p. 1, 2015.

[30] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Its a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Symposium On Usable Privacy and Security (SOUPS 2014)*, pp. 213–230, 2014.

[31] Google, "Google Play Store." Accessed: 25th Nov 2015.

[32] Apple, "iTunes Apple Store." Accessed: 25th Nov 2015.

[33] E. Ha and D. Wagner, "Do Android users write about electric sheep? examining consumer reviews in Google Play," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pp. 149–157, IEEE, 2013.

[34] D. Yoganathan and S. Kajanan, "Designing Fitness Apps Using Persuasive Technology A Text Mining Approach," in *Proceedings of the 18th Pacific Asia Conference on Information Systems*, 2015.

[35] G. Hofstede and M. H. Bond, "Hofstede's culture dimensions an independent validation using Rokeach's value survey," *Journal of cross-cultural psychology*, vol. 15, no. 4, pp. 417–433, 1984.

[36] A. Bowling, "Mode of questionnaire administration can have serious effects on data quality," *Journal of public health*, vol. 27, no. 3, pp. 281–291, 2005.

[37] K. Renaud, R. Blignaut, and I. Venter, "Smartphone owners need security advice. how can we ensure they get it?," in *CONF-IRM - Cape Town, South Africa*, 18-20 May 2016.

[38] D. Pink, "Drive: The Surprising Truth About What Motivates Us," *New York: Penguin Group, Inc*, vol. 138, p. 240, 2009.

[39] R. M. Ryan and E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.," *American Psychologist*, vol. 55, no. 1, p. 68, 2000.

[40] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.," in *Usenix Security*, vol. 1999, 1999.

[41] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A socio-technical investigation into smartphone security," in *International Workshop on Security and Trust Management*, pp. 265–273, Springer, 2015.

[42] Roboform.com, "Password manager." Accessed: 15 th April 2016.

[43] B. Ur, S. Bees, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?," in *CHI*, 2016. To Appear.

[44] R. Ayalew, "The Paradox of Overfitting," Master's thesis, Human Computer Interaction Programme, Uppsala University, 2011.

[45] M. Hassenzahl, "User experience (UX): towards an experiential perspective on product quality," in *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine*, pp. 11–15, ACM, 2008.

[46] M. Hassenzahl, S. Diefenbach, and A. Göritz, "Needs, affect, and interactive products - facets of user experience," *Interacting with Computers*, vol. 22, no. 5, pp. 353–362, 2010.