Trust and Security Risks in Mobile Banking

Monica Messaggi Kaya

Kellogg College
University of Oxford

March 2013

A dissertation submitted in partial fulfilment of the requirements
for the degree of Master of Science in Software Engineering

Abstract

With the development and growth of mobile technologies, mobile phones enable users to perform a number of different tasks with their devices: from sending simple text messages, checking e-mails and browsing the internet, to running elaborated applications. Nowadays, the mobile phone platform creates great opportunities for businesses, especially due to its capabilities and population coverage: the number of mobile subscriptions approaches global population figures. In order to explore such opportunities, most banks have already launched their mobile applications and/or re-designed mobile version of their websites. One of the benefits of using mobile banking is the possibility for users to carry out bank transactions, such online payments or transfers, at anytime and anywhere. Expectations for the adoption of mobile banking were high; however, it represents about 20% of mobile phone users at the present. One factor has been recognised as being a strong reason for users not to adopt mobile banking: their concerns about security. This dissertation focuses on the relationship between the trust users have in mobile banking and the security risks that the use of mobile devices potentially pose. A questionnaire was created in order to gather users' perception of security about mobile banking, and its results compared with recognised security issues.

Acknowledgements

To my husband, who patiently waited and supported my crazy hours of work and study. To my beautiful daughter Ayla, having a bit less of mommy during weekends so I could complete this work. To my parents, for their support and motivation through all stages of my education. To my sister, always ready to revise my text, point mistakes, make suggestions and offer 'pick-me-ups'; thank you for accompanying me on this journey. To many friends and other family members who understood that I couldn't spare the time for them, but still spared their time for me, giving words of motivation and wisdom. To Ivan Flechais for his patience, motivation and follow-up helping me to complete this dissertation.

Contents

List of Figures

1 Introduction

Mobile technologies evolved with the introduction of smartphones. With the implementation of operating systems in mobile devices, a range of possibilities for research and development were created, including the introduction of new hardware capabilities: bigger screen size, keyboard input, full web browser on mobile, motion sensors and location-based functionality to mention a few.

Nowadays, a mobile device is one of the most "carried around item" used as a "memory dump" for telephone and e-mail contacts, agenda, reminders and to-do lists. Also commonly used to check e-mails, browse the latest news, search nearby points of interest, online shopping, access social media connecting with family and friends, and to run a diversity of applications.

SMS (Short Message Service or simply text message) is one of the most used mobile application allowing communication exchange between device users, between customers and institutions which provide alerts, news, verification codes (as a way to recover passwords and authenticate users) and other services.

The launch of app stores triggered an ongoing process of application development and deployment. The mobile phone platform creates great opportunities for businesses, especially due to its capabilities and population coverage: the number of mobile subscriptions approaches global population figures [18]. The fact that the number of existing mobile devices is almost the same as the global population doesn't necessary mean that devices used are the latest models and have the latest features; businesses exploring this market have to consider this situation in order to reach a wider population offering services via WAP-browsers and via SMS where smartphones are unavailable.

Mobile banking can be defined as the use of mobile phone to access a bank account; receive debit/credit alerts and statements via SMS; check balances, recent transactions and basic operations using a menu by accessing a bank website via mobile browser; or transfer funds and pay bills using an application on a smartphone. Many banks offer one or more of these options [37].

In this dissertation, the term "mobile banking" embraces the above definition and summarises the use of financial services or transactions using one of the following methods: SMS (as is the case of M-Pesa in Kenya), online banking (using a browser installed on the mobile device) and a mobile banking application (app developed by the bank institution).

In previous years, most banking transactions were done only interacting with the bank staff at its branch, following by the use of additional services provided by ATMs (Automated Teller Machine, or simple cash points). With the introduction of online banking, the convenience of performing banking transactions outside branch opening hours gained many adopters. Online customers started to trust the new medium when banks presented security measures to access their bank account, including PIN (personal identification number), security questions and PINsentry machines. The use of online banking to access account information, through a browser on a PC, is somehow a common experience for a considerably large audience in many countries, and customers are fairly comfortable with its use [9]. One of the benefits of using mobile banking is the possibility for users to carry out bank transactions, such online payments or transfers, at anytime and anywhere, saving physical trips to ATMs and costs associated with

them. Expectations for the adoption of mobile banking were high; however, it didn't follow the same pattern as online banking, representing about 20% of mobile phone users at the present. One factor has been recognised as being a strong reason for users not to adopt mobile banking: their concerns about security.

The similarity of smartphones and computer operating systems allowed many security exploits to be adapted and deployed on mobile devices, such as: malware, phishing schemes, Trojan horses, man-in-the-middle attacks, rootkits, denial of services and others.

In general, computers users are more aware that they need an antivirus software, password-protect their computers and profiles, perform backups, not install software or open files that come from unknown sources or they do not trust. However, some studies found a difference in behaviour regarding security understanding when using computers and when using mobile devices. Despite that mobile devices are normally with their users throughout the day, the lack of knowledge or even care regarding possible security risks comes as a surprise. In addition, banking institutions that offer mobile applications are not transparent enough regarding the type of security they offer to their customers. The lack of understanding about potential security risks and the protection that is offered is one of the major factors that are making users unsure about mobile banking use.

A questionnaire was created as an attempt to understand the difference in behaviour and to gather a sense of trust in mobile banking. The sample data revealed that more than 70% use mobile applications in general. The vast majority (77%) of users were concerned with security regarding mobile banking services and that is the main reason for not using mobile banking in 40% of the cases while the other 37% are still concerned but use it anyway.

The results of the questionnaire also revealed that only 30% of users carry out banking transactions via mobile browser or mobile banking application. 70% of the ones that carry out mobile banking prefer to use a mobile bank app. A possible reason for that could be because of its ease to use or maybe because of their trust in the mobile bank app which is a direct link to the bank instead of using a browser (third-party) in between the customer and the bank. 40% were unsure about the mobile banking application security level, but when asked about the online banking (using a browser) 92% believed that the level of security provided was medium or high. The sample data shows the sense of trust in online banking is much higher than the one of the banking application.

This dissertation focuses on the relationship between the trust users have (or lack) in mobile banking and the security risks the use of mobile devices potentially pose. In order to achieve the purpose of this research, the document is divided in the following chapters:

Chapter 2 provides a high level background on mobile security.

Chapter 3 presents a list of known mobile security risks and security measures, highlighting some elements relevant to mobile banking including bank application use cases. It also describes human factors in this process and how security measures have influence on user decision to apply or ignore security advice to personal gadgets.

Chapter 4 includes a questionnaire and presents expectations and findings.

Chapter 5 summarises the most important topics covered by the research presenting a conclusion of this project.

2 Background

Mobile banking can be defined as the use of mobile phone to access a bank account; receive debit/credit alerts and statements via SMS; check balances, recent transactions and basic operations using a menu by accessing a bank website via mobile browser; or transfer funds and pay bills using an application on a smartphone. Many banks offer one or more of these options [37].

Mobile banking is being adopted by many users around the world, in some countries more than others. Most of renowned banks offer their applications and websites so users are able to perform banking-related transactions with their devices.

Online banking is well-known and used by a large audience in many countries and customers are fairly comfortable with its use [9]. Various security threats have been found, patched and tested in this environment, allowing some sense of security while using banks online. However, the mobile environment is still fresh and despite some techniques already been applied to make a banking transactions secure via mobile there are still threats and risks involving those transactions that are unknown (or ignored) by the general public.

Despite that users may apply some rules of security when using their computers, they may forget (or ignore) that the same risks also apply to their mobile devices. A simple example is the logging screen on a computer where a password is chosen and used frequently to avoid other people accessing files and other information. A mobile device also has options for locking the screen, but the same user might choose not to add a password or PIN to his mobile for convenience or lack of knowledge that such option exists.

The adoption of mobile applications increases daily, and with its use, the security threats are also increasing. The similarity of smartphones and computer operating systems allowed many security exploits to be adapted and deployed on mobile devices, such as: malware, phishing schemes, trojan horses, man-in-the-middle attacks, rootkits, denial of services and others.

For the technically savvy, some threats are known and precautions could have been taken to prevent possible attacks on mobile phones. One example of exploit could be the use of Bluetooth to access mobile phone's local files, messages and contact information. Malicious software can be downloaded to the phone when a user access a link received via SMS or while visiting a compromised website via mobile browser. Depending on the level of analysis an application receives before entering an app store, malicious code might not be detected and an apparent legitimate application can be distributed through official channels containing code that could perform unwanted tasks in the background and/or remotely access the phone data. Some applications might also use the SMS system or e-mail communication to propagate malware as attachments and these systems are being frequently used to send pictures, music, and other files. Spyware (gathers information about a user without their knowledge) also becomes an issue since people are paying more attention to messages coming to their mobiles and the device becomes a way of make a direct advertising [15] and [40].

The list below points some interesting aspects related to security threats and user behaviour related to mobile phones:

- Mobile devices are very close to its owner/user, usually within a few meters and in gen-

eral on top of a working surface (desk, table, etc.) or near the body (pocket, coat, bag, handbag). With the knowledge that the device is near its user, an exploit that could access the GPS features on the phone and reveal the user's position breaching privacy.

- Mobiles are frequently ON, with the demand of use throughout the day; some exceptions are when its battery is depleted or the user is in a place that requires a different mode of operation (such as airplane mode) or OFF in hospitals, cinemas and other establishments.
- Smartphones offer a series of features and applications often request access to user data, browsing data, contact information, phone dialling capabilities, camera, microphone, movement sensors, GPS location and others. If an attack successfully gains control of hardware features on the phone the camera could be turned on/off; user conversations could be monitored, messages could be intercepted and eavesdropped (listened without consent) with privacy and possible impersonation implications for its user. Gaining access to SMS interface could create potential financial losses for the user if the attacker sends messages to premium numbers.
- Users don't install antivirus on mobile phones very often. With no such detection system a malware won't be detected and other vulnerabilities can be exploited.
- Mobile devices can be lost or stolen (more often than PCs).
- Not often users choose to add PIN or another screen-lock mechanism. A phone without a locking mechanism left unattended can be compromised if an attacker physically holds the phone and installs a malware, by visiting a website for example; leaving an open door for future exploits.
- Mobile users sometimes are unaware of "shoulder surfing" and people observing the users' patterns and passwords being typed without their knowledge.
- Users often make notes on their phone, including passwords to enter in other environments. Bluetooth could be used to access mobile phone's local files, messages and contact information exposing user's personal information, including files containing saved passwords.

The above includes just few of the possible threats and yet many mobile users are unaware of these security treats or they don't think the cost of investing in security is worth compared to the ease of use and fast access to their mobile features. The economical view [16] [42] of the user behaviour related to security could indicate a point of failure. The effort and costs for users to maintain some security elements like passwords [23], reading security related material and following some procedures to maintain their computer/mobile secure might drive their behaviour towards or against security.

If better education was given to mobile users, some preventative measures could be taken without excessive burden to them. Also, once we expose potential risks and highlight possible impacts to the user's privacy or finances (in the case of mobile banking), their behaviour towards security *could* shift slightly and they might take some pro-active measures to prevent issues.

Some of the security areas that could be found problematic are:

- Confidentiality: relates to the prevention of information disclosure to unauthorised individuals or systems. Exploits on mobile devices could disclose personal information to attackers.

- Authentication: it is necessary to validate who are the parties involved on a transaction or communication and if they are who they claim to be. In mobile banking transactions, it is fundamental for users to have the guarantee that the process is carried out by a valid and official bank, not to a fake institution (or individual).
- Electronic payment: concerning the right amount to the correct parties.
- Data protection and privacy: protection of elements such as GPS location, phone conversation, exchange of messages or e-mails, passwords and others.
- Network security: identification of network users, applications and services to allow only authorised users and information passing through the network, test and monitor the network to identify areas of weakness and make adjustments, protecting information from eavesdropping or tampering (unauthorised changes or damage) using encryption technologies (encoding information in a way that only authorised users can read it).
- Access control: who can access a specific item/file/information and what it can do with it.

To this date, despite my computer-related background and current dissertation highlighting some mobile threats, I had never considered installing antivirus software on my own mobile devices. My own thought-process was similar to what some studies [16] highlight that the effort and the cost/benefit of using a security mechanism has to be beneficial enough for the user to adopt it, and I add: to maintain it in the long term.

When I thought about antivirus companies which have mobile security software, two names came to mind: Bullguard and Kaspersky; possibly because of articles read in the past and also banking companies preferring one or another. A quick check on their websites [7] [22] reveals lightweight and affordable solutions and I could identify potential benefits that could deter or mitigate some the threats and security areas mentioned previously.

Bullgard states that offers premium mobile protection supporting most of operating systems (Windows Mobile, Android, Symbian or Blackberry) and the advantages listed are: online account to remotely access your smartphone; mobile security manager to locate phone (via GPS) and to lock, wipe your phone, and edit the parental control module; state-of-the-art antivirus features that work silently in the background; SIM card protection and 24/7 support. These services at a cost £19.95 for one device for one year.

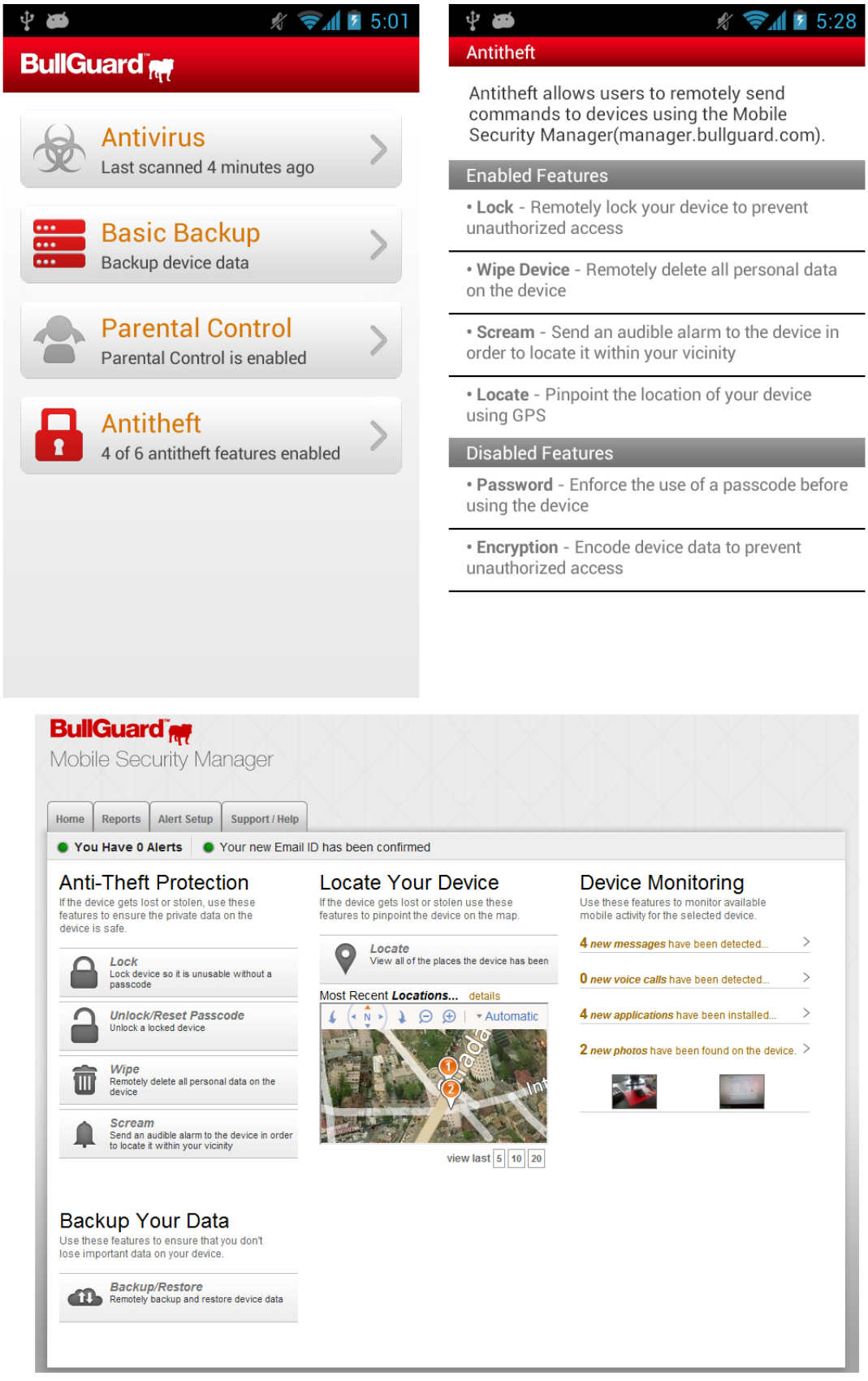

Figure 2.1: Bullgard screenshots of main screen, anti-theft screen and mobile security manager

Kaspersky states that “in addition to delivering world-class anti-malware protection, Kaspersky Mobile Security also includes a wealth of features to help protect your private data and even find your phone if it is lost or stolen”. Features include: locks your missing phone; locates it and wipes data from it - even if the SIM card is replaced; protects against viruses, spyware, Trojans, worms, bots and more; blocks dangerous and phishing websites; filters unwanted calls and SMS texts; hides private communications including contacts, calls, SMS texts and logs; identifies unauthorised users of your smartphone by secretly taking their mugshot (only for Android); enables easy, web-based control of anti-theft features and it is optimised for low impact on battery life. Kaspersky price is currently at £8.95 per mobile phone per year which is quite a competitive price for the list of features it presents. Other companies mostly known for computer antivirus protection also have their mobile solution: Symantec [38] not revealing prices or mobile coverage on their page and McAfee McAfee [28] at a price of $29.99 per year per mobile subscription (approximately £20 at the time of writing).

Considering the benefits that an antivirus for mobile can provide and the low cost of subscription, this solution could be used to deal with some of the threats mentioned previously. The following chapter states in more detail some of known security risks, security measures, concerns of mobile users as well as their associated behaviour.

3 The Security of Mobile Banking

3.1 Mobile Security Risks

Mobile phones increased complexity with their evolution, their operating systems are in many aspects similar to personal computers. Some of the exploits that are used on computers can be also used on mobile phones. In the beginning of the smartphone era was predicted that the exploits on mobile devices would be similar to computers and it wouldn't take long for attackers to develop code capable of that. It took maybe longer than the predictions for serious attacks to happen, the high diversity of the phones and operating systems and the different network topology of the mobile compared to the internet are pointed as some of the reasons [29].

However, vulnerabilities were exploited and attacks were made in various forms: SMS databases stolen, availability attacks were made (where the signal of the mobile or base station was blocked rendering the service unusable), eavesdropping, privacy attacks and others. The following are considered [30] major threats on mobile platforms.

3.1.1 Rootkits

"Rootkits are malware that achieve their malicious goals by infecting the operating system. For example, rootkits may be used to hide malicious user space files and processes, install Trojan horses, and disable firewalls and virus scanners. Rootkits can achieve their malicious goals stealthily because they affect the operating system, which is typically considered the trusted computing base." They can be deployed to smartphones in a fairly simple way, according to [19], and some of the exploits can have serious social impact.

Rootkits can access a number of interfaces and information that are not normally available on a PC, such as GPS, voice, messages, battery and other hardware features. They can compromise privacy and security of the mobile users. Because rootkits install themselves as kernel modules (loaded each time the operating system is loaded) and require root access to infect the operating system, they are harder to detect. They could compromise privacy and security of the mobile users in novel ways that were not available on desktop. The following list presents vulnerabilities a rootkit can exploit when installed on a smartphone:

- User's position (via GPS location) - most mobile users keep phone within their reach and GPS location would be quite accurate information about the user's coordinates.
- Financial damage by sending text messages to premium numbers and hiding that such messages ever existed, this could be exploited in cases where SMS are used for mobile banking transactions (such as in the M-Pesa system).
- Access to passwords and other information that is typed (via keylogger) or saved (accessing the system information, text messages, saved files) – here another potential threat for mobile banking transactions where a keylogger could capture PINs and other information that could be used to steal money (and any other information accessible) from the mobile user.

- Record voice conversations expose sensitive information (for example a company board meeting and their trade secrets exposed to competitors).
- Denial of service via battery exhaustion (turning ON many services and Bluetooth but showing as OFF to user, when in fact it is ON and draining mobile battery – limiting the service to the user in case of need).
- Denial of service for a large portion of a cellular network via attacks using SMS or Bluetooth.

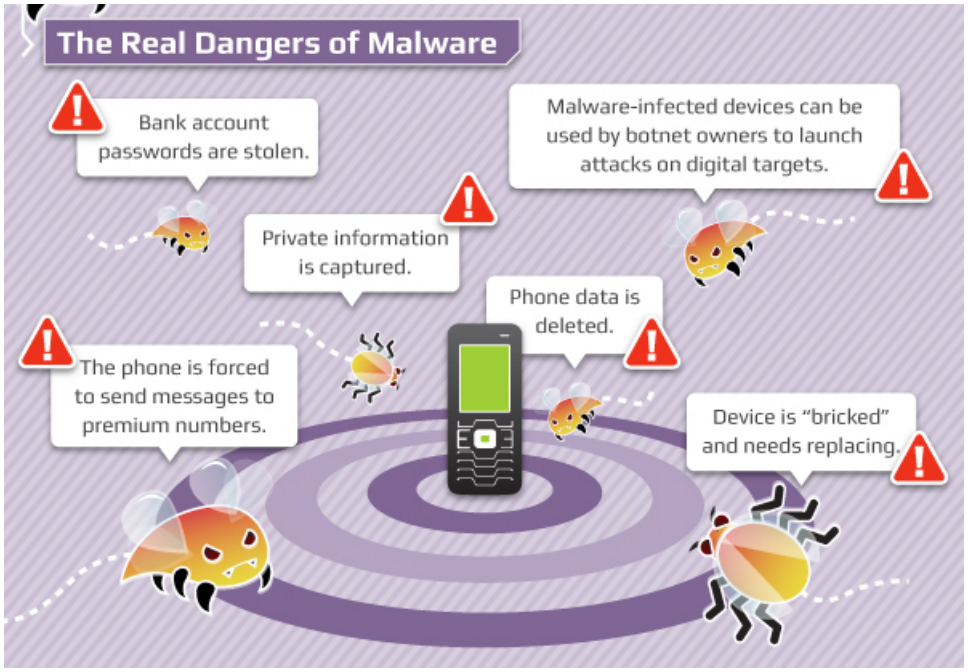

Figure 3.1: Mobile Malware - Growth and real danger [8]

In the case of rootkits, its delivery can be via opening a file, downloading content from malicious websites, open email attachments, spam, or exploiting vulnerabilities of other mobile applications that may already be used/installed by the user. A recent way of delivering rootkits is for the obfuscation of web addresses using QR codes. Depending on the application that reads the QR code, the web address can be explicit and waiting for user confirmation to visit or not the web address, but some other applications redirect the user immediately to the mobile browser and auto-type the address, in an automatic and more difficult way to stop the download of malware depending the speed of connection. Rootkit detection depends on the level of the sophistication of the rootkit itself, but if there is a footprint some malware detection tools might find a rootkit installed. However, because they affect the integrity of the operating system, is accepted that detection mechanisms must reside outside the control of the operating system they monitor.

3.1.2 Web-Based and Network-Based Attacks

Web-based and network-based attacks are performed using the mobile browser, where malicious websites, or compromised legitimate websites trigger the attack if the mobile runs a vulnerable version of the operating system.

"A typical web-based attack works as follows: an unsuspecting user surfs to a malicious webpage. The server on which the page is hosted identifies the client device as running a potentially vulnerable version of the operating system. The attacking website then sends down a specially crafted set of malicious data to the web browser, causing the web browser to run malicious instructions from the attacker. Once these instructions have control of the web browser, they have access to the users surfing history, logins, credit card numbers, passwords, etc., and may even be able to access other parts of the device (such as its calendar, the contact database, etc.)." [30]

3.1.3 Social Engineering Attacks

Social engineering attacks try to make the user disclose information. Phishing (often an email or SMS that directs user to a website that looks and feel like the legitimate one but it is a fake and has the intention to collect user credit card information, passwords and other details); other social engineering technique is to entice the user to install an application on the phone that may contain malware.

3.1.4 Resource Abuse Attacks

Resource abuse attacks misuse the network. The two most common such abuses are the sending of spam emails from compromised devices and the use of compromised devices to launch denial of service attacks on either third-party websites or perhaps on the mobile carriers voice or data network.

3.1.5 Data Loss

Data loss occurs when a person or attacker removes sensitive information from a protected device or network without proper authorisation. This loss can be either unintentional or malicious in nature.

3.1.6 Data Integrity Threats

In a data integrity attack, the attacker attempts to corrupt or modify data without the permission of the data owner.

Some infographics can be an interesting way of show data and pass a message in a visual way. Sometimes they overwhelm the viewer with either too much information or their representation is not relevant enough. The following infographic created by Bullgard [8] illustrates well some of the mobile threats mentioned previously.

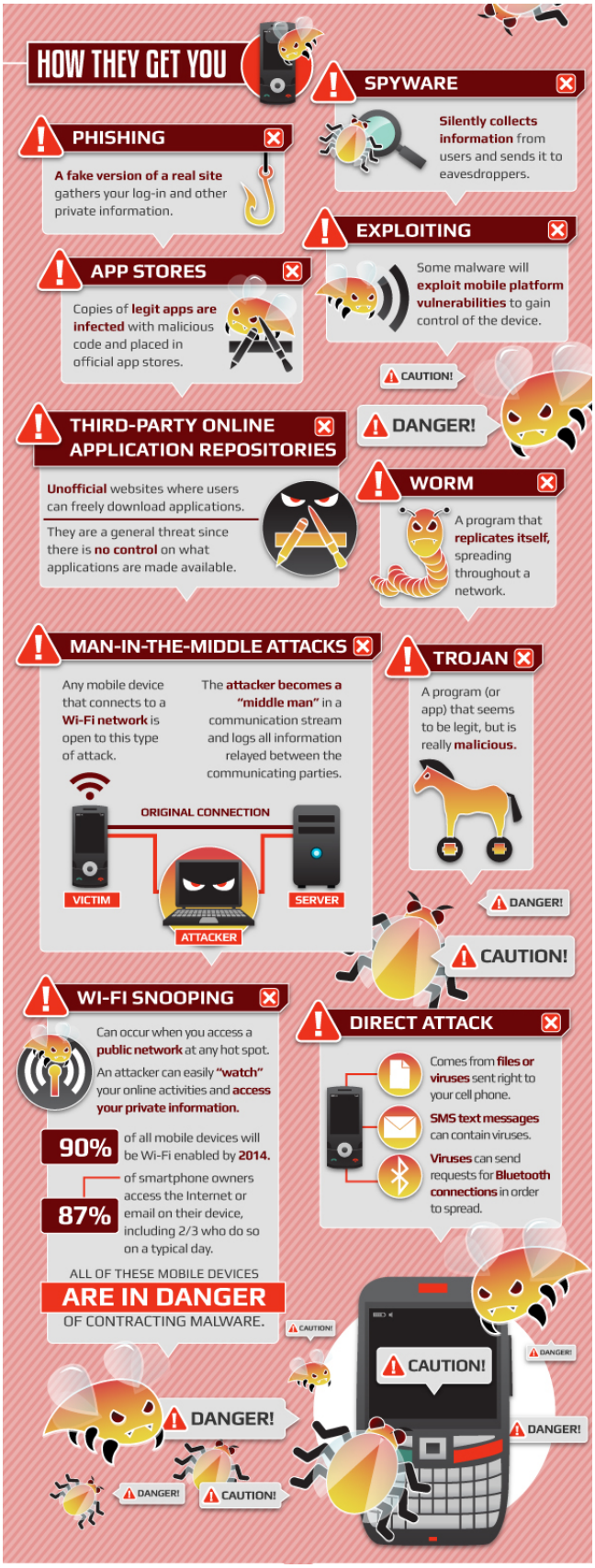

Figure 3.2: Mobile Malware - How do they get you [8]

3.1.7 Mobile-Based Branchless Service

Extending financial services to low-income population in developing countries was an extraordinary step in mobile banking. Highly used in Kenya and other countries, a vast population that doesn't have regular bank accounts can rely on mobile phone to send and receive money, pay for goods deposit, withdraw and transfer money.

Despite being a great advance for the population, the system is not end-to-end secure. According to [32] one shortcoming of today's branchless systems is that they rely largely on network-layer services for securing transactions and do not implement any application-layer security. M-Pesa, which is the pioneer branchless banking serves over 50% of Kenya's adult population and uses a custom-made SIM Tool Kit (STK) program to protect transaction messages exchanged between client phones and the server. Nokia Money, M-PESA, and Smart Money are all based on GSM/3G networks which are vulnerable to message intercepting and the threats to this system are eavesdropping (accessing private messages without consent), spoofing messages (impersonating a legitimate person or institution with intention to collect their data via SMS) and the ability of performing man-in-the-middle attacks (an attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker and any sensitive information in between the parties is intercepted).

3.2 Mobile Security Measures

According to [11] the mobile banking association highlighted the following main security issues that should be addressed in order to encourage the adoption of mobile banking:

- Data transmission must be secured: for the confidentiality, the connection between the bank and the device should be encrypted.
- Application and data access must be controlled: before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed.
- Data integrity must be provided: any critical data to the mobile phone must be protected against unauthorised modification.
- Loss of device must have limited impact: the mobile banking service should be designed so that there is limited impact when customers lose their mobile phones.

To prevent man-in-the-middle attacks, communication encryption can be used [29].

Protecting the data if a mobile phone is lost or stolen is a frequent issue and one suggestion is to make non-volatile memory encrypted and a secure store for cryptic keys. Remote device management and remote firmware update mitigate the user's involvement, and possibly choosing not the most appropriate option in these cases.

Operational systems may handle phone data and processes in different ways and they may present different security aspects. The designers of iOS and Android based their security implementations on five elements [30]:

- Traditional Access Control: seeks to protect devices using techniques such as passwords and idle-time screen locking.

- Application Provenance: each application is stamped with the identity of its author and then made tamper resistant (using a digital signature). This enables a user to decide whether or not to use an application based on the identity of its author.
- Encryption: seeks to conceal data at rest on the device to address device loss or theft.
- Isolation: attempt to limit an applications ability to access the sensitive data or systems on a device.
- Permissions-Based Access Control: grants a set of permissions to each application and then limits each application to accessing device data/systems that are within the scope of those permissions, blocking the applications if they attempt to perform actions that exceed these permissions.

A proactive way of detecting malware was done by Apple with the process of testing and analysing the apps that were submitted to their app store before release to public. The aim is to detect malicious code and stop the app with a possible malware being distributed.

The iOS's security model was considered well designed overall and proven largely resistant to attacks [30].

- iOS's encryption system provides strong protection of emails and their attachments, and enables device wipe. However, thus far has provided less protection against a physical device compromise by a determined attacker.
- iOS's provenance approach ensures that Apple vets every single publicly available app. While this vetting approach is not foolproof, and almost certainly can be circumvented by a determined attacker, it has thus far proved a deterrent against malware attacks, data loss attacks, data integrity attacks, and denial of service attacks.
- iOS's isolation model prevents traditional types of computer viruses and worms, and limits the data that spyware can access. It also limits most network-based attacks, such as buffer overows, from taking control of the device. However, it does not necessarily prevent all classes of data loss attacks, resource abuse attacks, or data integrity attacks.
- iOS's permission model ensures that apps cannot obtain the devices location, send SMS messages, or initiate phone calls without the owner's permission.
- None of iOS's protection technologies address social engineering attacks such as phishing or spam.

Each Android app runs within its own virtual machine and each virtual machine is isolated in its own process. This model ensures that no process can access the resources of any another process (unless the device is jailbroken. While Java virtual machine was designed to be a secure system capable of containing potentially malicious programs, Android does not rely upon its virtual machine technology to enforce security. Instead, all protection is enforced directly by the Linux-based Android operating system.

Android's security model is primarily based on three of the five security pillars: traditional access control, isolation, and a permission-based security model. However, it is important to note that Android's security does not simply arise from its software implementation. Google releases the programming source code for the entire Android project, enabling scrutiny from the broader security community. Google argues that this openness helps to uncover aws and leads to improvements over time that materially impact the platforms level of security (this

claim appears to be true as there have been less than two-dozen vulnerabilities discovered in the Android platform since its release, an extremely low number) [30].

Android security model is a major improvement over the models used by traditional desktop and server-based operating systems, it has two major drawbacks. First, its provenance system enables attackers to anonymously create and distribute malware. Second, its permission system, while extremely powerful, ultimately relies upon the user to make important security decisions. Unfortunately, most users are not technically capable of making such decisions and this has already led to social engineering attacks [30]. To summarise:

- Android's provenance approach ensures that only digitally signed applications may be installed on Android devices. However, attackers can use anonymous digital certificates to sign their threats and distribute them across the Internet without any certification by Google. Attackers can also inject malicious code into legitimate applications and then redistribute them across the Internet, signing them with a new, anonymous certificate. On the plus side, Google does require application authors wishing to distribute their apps via the official Android App Marketplace to pay a fee and register with Google (sharing the developer's digital signature with Google). As with Apples registration approach, this should act as a deterrent to less organised attackers.

- Android's default isolation policy effectively isolates apps from each other and from most of the devices systems including the Android operating system kernel, with several exceptions (apps can read all data on the SD card unfettered).

- Android's permission model ensures that apps are isolated from virtually every major device system unless they explicitly request access to those systems. Unfortunately, Android ultimately relies upon the user to decide whether or not to grant permissions to an app, leaving Android open to social engineering attacks. Most users are unequipped to make such security decisions, leaving them open to malware and all of the secondary attacks (for example DDoS attacks, Data Loss attacks) that malware can launch.

- Android recently began offering built-in encryption in Android 3.0. However, earlier versions of Android (running on virtually all mobile phones in the field), contain no encryption capability, instead relying upon isolation and permissions to safeguard data. Thus, a simple jailbreak of an Android phone or theft of the devices SD card can lead to a significant amount of data loss.

- As with iOS, Android has no mechanism to prevent social engineering attacks such as phishing attacks or other (off-device) Web-based trickery.

In general, a the varied aspects of security should be considered about mobile phones: the type of security that is build in with each operating system used, the understanding of security from the user's perspective and the ecosystem where the device lives, the latter refers to the multiple connections the device has with cloud-based services (enterprise and/or private email, calendar, contacts, digital content such as music and video, backup services and other settings).

3.2.1 The Security of a Mobile App

Mobile bank apps provide a direct link from the device to the bank, without having to go through any additional browser or third-party application. This means banks have much better control over the security and connection of customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption and two-factor authentication that meets the institution's unique needs.

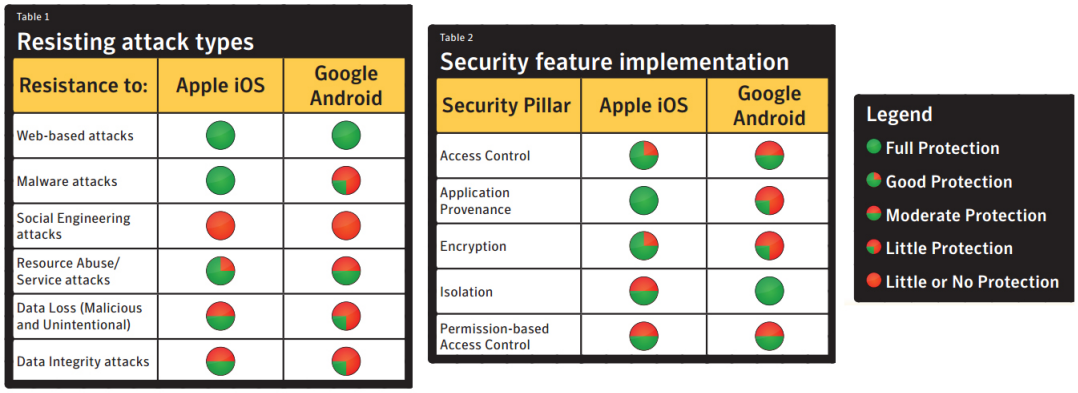

Figure 3.3: iOS vs. Android: Security overview

Even if someone is able to obtain a customer's phone, they will still be required to put in a username and password, and if available, provide a second factor of authentication, in order to gain access to the accounts.

Along with these two factors of authentication, many banks have started implementing a third method of security: a profile of a customer's actions. Banks and other financial institutions are able to monitor a customer's actions when banking via a mobile app, creating a profile of those interactions.

Another plus to using a mobile application is the fact that most smartphones and tablets can now be cleared or reset from remote locations. Thus, if someone steals or obtains a mobile device, the customer can use his or her computer or any other device with an Internet connection to clear any data and apps from the device, eliminating the possibility that someone else can use the phone to access the customer's account.

As customers become more familiar with mobile banking app security and learn to trust a bank's mobile app brand, they will be more willing to use these tools [39].

3.2.2 General Recommendations for Security

Besides the recommendations listed previously a few precautions can make mobile banking safer, they are not only mobile-banking related but also general use of smartphones [26].

- Do not use public Wi-Fi when banking via mobile device, opt for the 3G or 4G connectivity of the own smartphone. Although those algorithms can be hacked, any respectable mobile commerce site will have SSL encryption in place for further protection.
- Download applications from official bank website. If the bank redirects to an app store, check if the developer's name is also the bank's name.
- Be aware of phishing emails that mimic your banks look and feel. Be familiar with the bank website so fakes can be discerned. Typos and problems with design choices are giveaways.
- Do not to click on links in a suspicious email, type your banks URL in a browser and login from there.
- Though SMS is the easiest way for banks and customers to communicate, this channel is relatively unsecure and should not be used for money transfers or logging in.
- Install mobile antivirus which will protect against malware and lock or wipe your device in the event it is misplaced or stolen.

- Remember that the security precautions for smartphone and tablet banking are similar as those for your PC. We often take more security measures on our computers than mobiles, but we need to be aware that mobiles are constantly with us and need similar if not more consideration regarding security.

Natwest made a simple but straightforward page [5] with general security tips that are listed below:

- Do not share password.
- Don't store passwords in your device.
- Add password or PIN to access your device/tablet.
- Only download apps from official app stores.
- Don't use your device unattended when logged on.
- Watch out for people looking over your shoulder.
- Consider using a reputable brand of antivirus software on your mobile banking device.
- Be cautious about opening links contained in SMS messages or emails.
- Don't download content from or visit sites unless you are sure that the site is reputable. This is to safeguard against installing malicious software.
- Be wary of using insecure and untrusted Wireless networks.

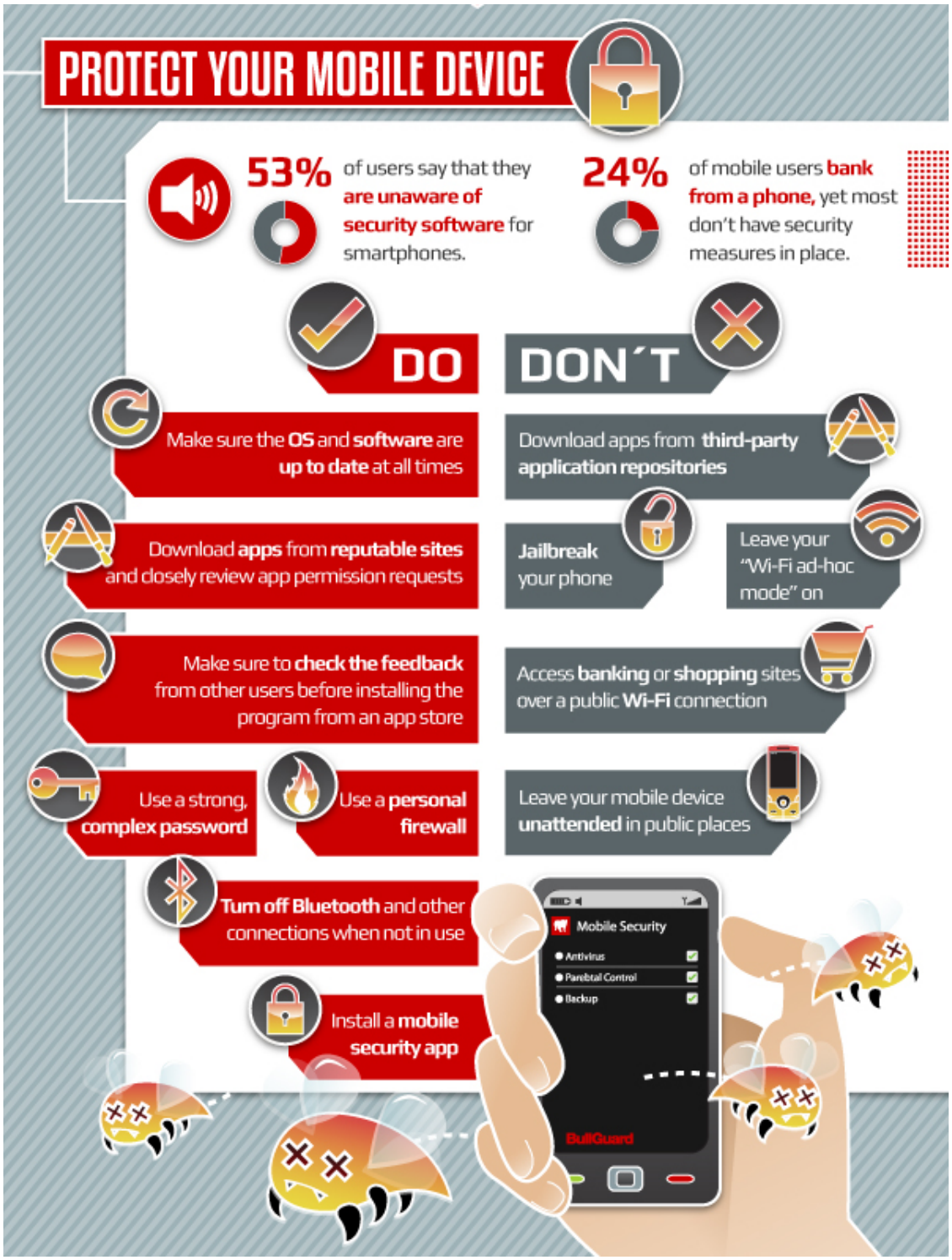

Figure 3.4: Protect your mobile device [8]

3.3 Use Cases of Mobile Apps (Barclays and Natwest)

Both institutions offer free software protection (antivirus) for its customers and pages with general tips on how they can protect themselves against common security problems.

3.3.1 Barclays Mobile App

I found relatively disconcerting search for information regarding the mobile security app on the Barclays website and not find any deeper explanation on types of security applied to it. There are a couple of links that lead to a general page on online security that Barclays use, but nothing related only to its mobile app. On the link about "What we're doing to protect you" [3] is a generic statement about the PINsentry, their free software offer (Kaspersky), data encryption, timed log out and deactivation of login details (in case of consecutive incorrect attempts).

If you read the Terms and Conditions for the software [2] you can find a little bit regarding encryption and other licences that the app uses. However, nothing much reassuring from the bank, except a section on their "Barclays Mobile Banking app" page [1] where states:

Why should I use Barclays Mobile Banking?

- It's free to download and easy to use, 24 hours a day.
- You can check the latest balances of your accounts, view your most recent transactions, transfer funds between your accounts and make payments to existing payees.
- Use the branch locator to find your nearest Barclays branch or cash machine.
- You can order statements choose paper or online statements, large print or Braille.
- If youre an Online Banking customer and you've upgraded to PINsentry, you can now use the Mobile PINsentry function in the app in the same way as you would use your PINsentry device.
- Get access on up to 3 devices.
- See your Barclays Personal & Business accounts, as well as your Barclaycard Personal accounts, in the app.

Steps while using the Barclays Mobile app:

Installing

If using Android, users can download the App “Barclays Mobile Banking” from Google Play – the app is freely available.

When first running the app various images are displayed designed to guide you through the process of authentication. The first image shows the three ways you will need to authenticate: your own details, your mobile phone and your card.

The second image displays a warning on Virus Protection and states that Barclays customers can get free copies of Kaspersky Mobile Security – this is not very reassuring for those installing the app but is clearly designed to reduce unauthorised access.

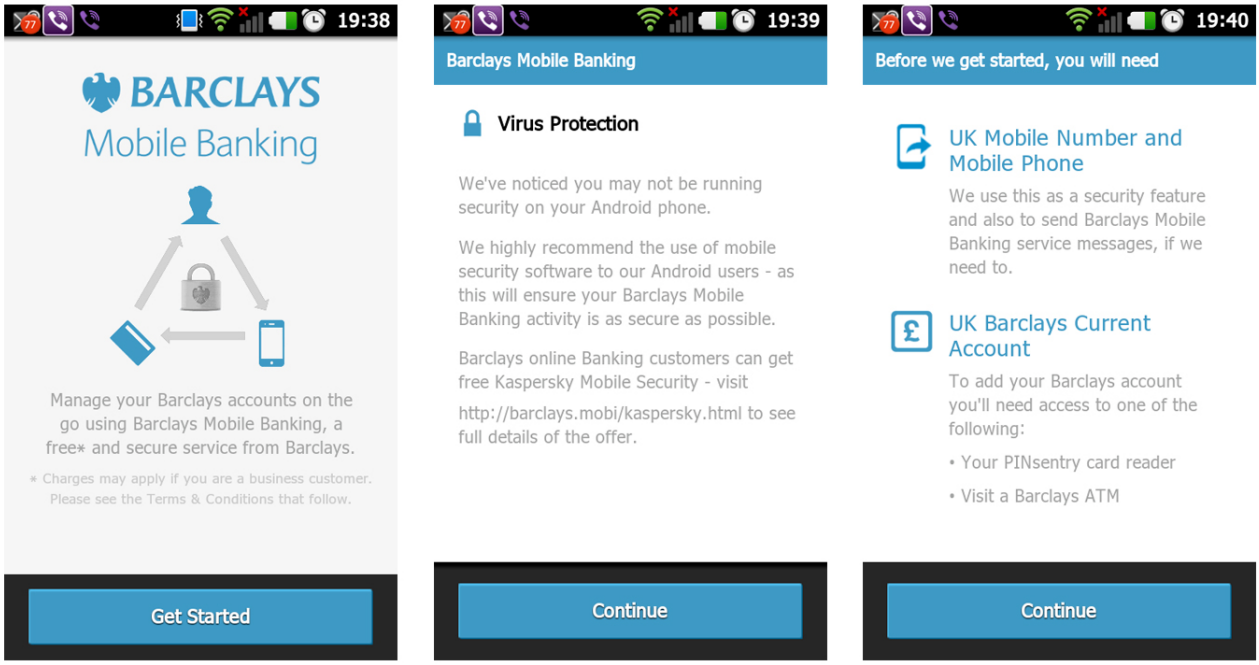

Figure 3.5: Barclays Mobile App - Authentication

The first step towards authorisation is to create a "passcode" which in this case is a five digit number – it's interesting to note that they use a five digit code here but a four digit code for cards. You are then asked to verify this number again.

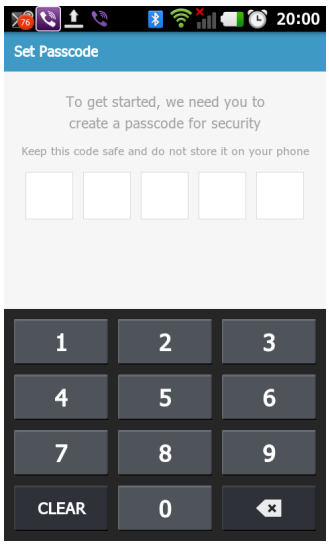

Figure 3.6: Barclays Mobile App - Passcode

The next step is to enter your details. This includes (a UK registered) mobile number, account details and name. You are then asked to confirm the details and to accept their Terms and Conditions which you can see in full within the app. The app will not work if the details you enter are not precisely the same as those stored by Barclays (Entering a misspelled name for instance produces a cryptic error code which you are asked to resolve by phoning them direct).

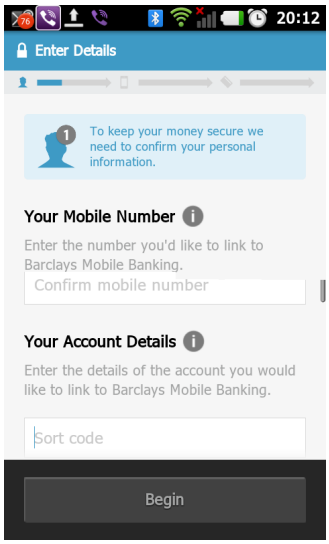

Figure 3.7: Barclays Mobile App - User details

Once your details are correctly accepted the Barclays app automatically sends you a six digit code via SMS to the mobile number you choose previously. This does not necessarily have to match the mobile number of the device you are installing the app on.

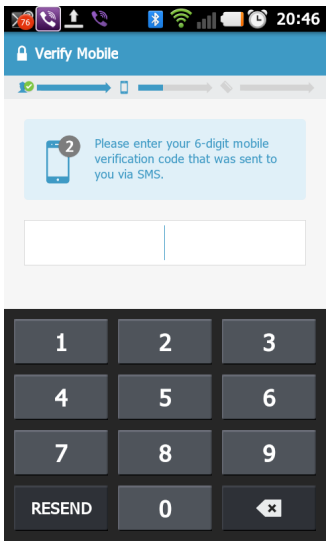

Figure 3.8: Barclays Mobile App - SMS code

The SMS reads:

> *"123456 is your Barclays Mobile Banking mobile verification code for account ****4321 (valid for 24 hours). If received in error please call 03332001014 for help" - SMS from Barclays, 20:35 14/03/2012*

This states the code is only usable for 24 hours but you can request another verification code from within the app. The last sentence may be there to help catch unauthorised access. To enter the code you first need to use the five-digit passcode you originally created within the app and then type in the six-digit number contained in the SMS.

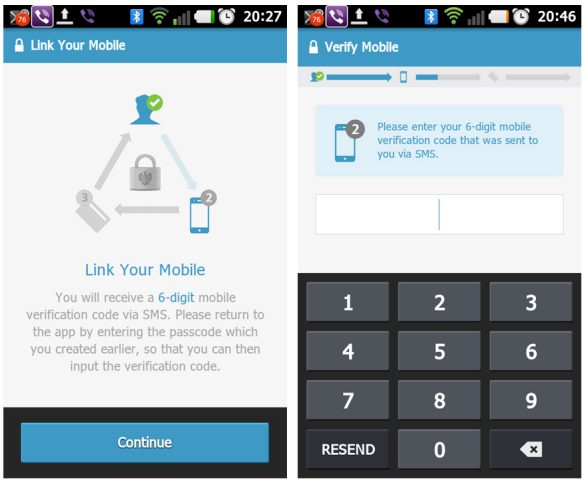

Figure 3.9: Barclays Mobile App - Enter code

Now you are presented to a third mechanism , the Card Authentication. Here you have the option of using PINsentry or visiting a Barclays ATM. The mechanism is effectively the same for both. First you enter you card pin number if using PINsentry machine and then enter a 8 digit number provide. PINsentry or the ATM will then generate an 8 digit number which you enter back into the app.

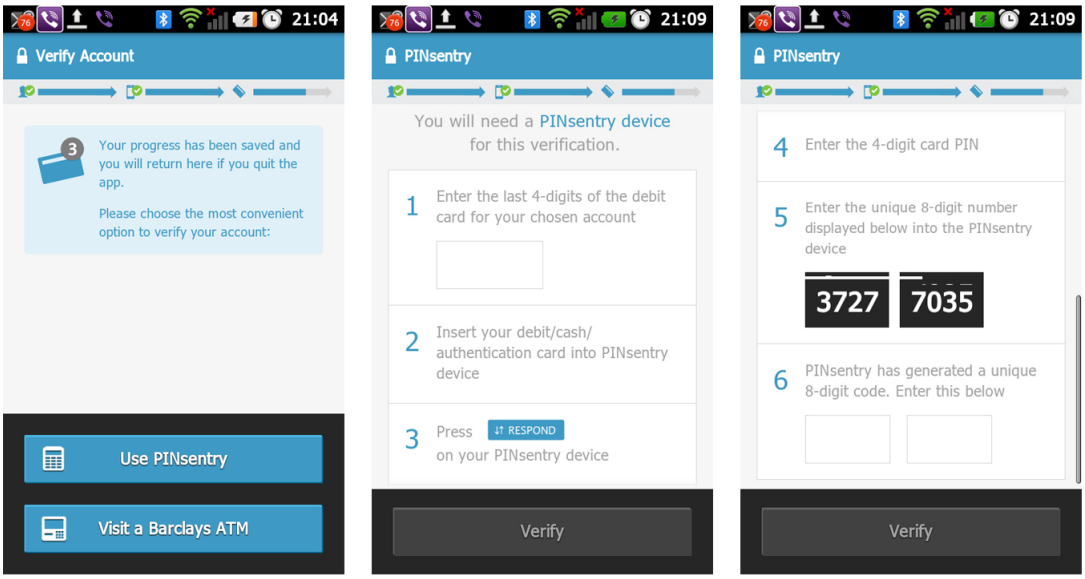

Figure 3.10: Barclays Mobile App - Authentication

Usage

All further access is now controlled only by the five-digit passcode and you will get logged out automatically if you have not used it for more than a minute. You can only do three options in the app:

- See the money coming in and out of your accounts.
- Pay someone you have already added to your account via either online of telephone banking. (There is no way to add any via the app)
- And transfer money between accounts.

However, the app can also act as a PINsentry (called “Mobile PinSentry”) so logging in to the Online banking website is simplified. (In theory this must mean that anyone with access to the app can go online and add themselves as someone you can pay, meaning the restriction within the app becomes redundant!)

The simplicity of the app is a positive factor, and after the initial setup you only need to use the five digit code and you can see your account details instantly. As I mentioned on the Background chapter I’ve never thought about security issues on mobile, although I do try avoid mobile banking (via browser) on a public network (I usually use it via 3G).

Barclays do have another app called “Pingit” which lets you send money via a phone number.

Additionally

Barclays do try to encourage the use of their app by stating online:

> *“When you use Barclays Mobile Banking, you will automatically be protected in the event of fraud We’ll cover any resulting loss, no matter how much money is taken from your account.”*

Barclays, http://www.barclays.co.uk/MobileBankingProtection/MobileBankingProtection/P1242622865207 accessed at 20:00 14/03/2013

However this information does not appear when you download or install the app.

3.3.2 Natwest Mobile App

Natwest was a bit more transparent regarding where to find the security information about mobile application [4] , however still not very clear about methods:

How we help to protect you

- We know how important it is to provide protection for your money. That's why security is at the heart of mobile banking.
- You are covered by the Online and Mobile Security Promise, our commitment to you in the event of fraud.
- Our rigorous registration process validates your details before you can use the service. The registration process is certified by Verisign, the global name in secure e-commerce.
- Access to the mobile banking application is password protected. Your passcode is uniquely linked to the mobile banking application on your device. This means only your passcode works on your application.
- We use sophisticated encryption technology for secure data transfer to and from your mobile device.
- We only settle for the same security standards you'd expect from our other services. We regularly test, update and validate our systems using independent experts to ensure we keep it that way.
- For advice on using you mobile phone safely see our Mobile Security Hints and Tips page. For advice on keeping your money and identity safe, visit our Security Centre.

3.4 People Factor

Users of the mobile technology encounter many different services and devices to interact with when doing banking: branches, ATMs, mobile payments via SMS, online banking using browsers (PC or mobile) and banks own mobile applications.

Deciding whether to use or not the mobile device to facilitate banking transactions takes into consideration many factors such as lifestyle, age, economic background, level of literacy and computer skills. While for some people the inclusion of technology in their lives is a natural occurrence, especially for the newest generations, many others might still be reluctant to use mobile for banking activities.

3.4.1 Demographics of Mobile Banking

Mobile banking is being used worldwide. In the United States, it is growing at fast pace, especially after 2007, the year that Apple introduced the iPhone and App Store to the market.

According to Deloitte's research [12], approximately 10% of mobile phone users conduct some banking transactions by phone. Among these users are the members of "Generation Y", people who were born between 1979 and 1994, these youngest adult consumers represent the fastest growing segment of today's workforce and 25% of the global population:

- Early technology adopters: Generation Y consumers are digitally sophisticated and hyper-connected to one another. Half send an average of 50 text messages per day, 97% are active on Facebook and other social networking sites and 80% are active online banking users. Smartphone users, including many Generation Y consumers, are three times more likely than consumers with traditional feature phones to use mobile banking and more importantly are significantly more active users behaviour that translates into greater loyalty, stickiness and, eventually, stronger banking relationships.

- Significant earnings capacity: While Generation Y consumers currently earn approximately $215 billion annually, their annual income is expected to reach $3.4 trillion by 2018. Additionally, this generation are expected to inherit more than $1 trillion over the next decade making them an attractive target market with an increased appetite for banking services.

- High-growth/high-potential market: In the United States, approximately 20 to 25 million Generation Y consumers will potentially become new banking customers over the next five years.

While the members of Generation Y are leading the charge in the adoption of all things mobile, is expected that consumers from previous generations would increase their usage of mobile banking as it becomes an established and familiar channel. Based upon Deloitte's analysis, there is a belief that mobile banking will surpass online banking as the most widely used banking channel by 2020 if not sooner. And, as mobile banking grows, so, too, will opportunities for banks to increase revenues and gain operating efficiencies.

The questionnaire distributed as part of this dissertation indicated that from the 30% of users that perform mobile banking transactions, the majority belong to the 25-39 age band, which matches Deloitte's research expectations.

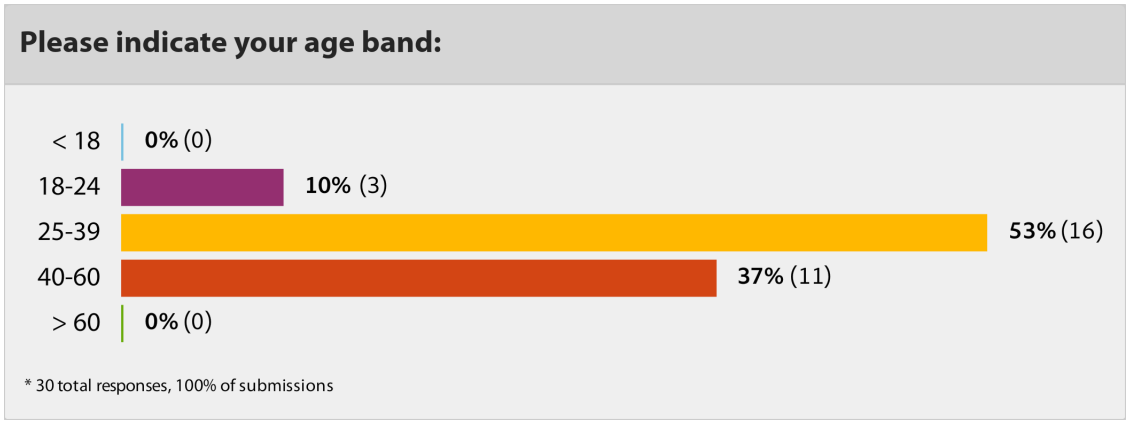

Figure 3.11: Users that perform mobile transactions by age

According to a study [36] a person's lifestyle can inuence on their choice of using a mobile banking application. In China, was found that people with high financial contentment consciousness care more about their career development and would like to spend more time on their work rather than on learning new things. The results showed that consumers with different lifestyles have different preferences over a number of identified mobile services.

In many papers and works about security, people are often mentioned as the weakest link. If security becomes a burden to the users, they will circumvent it to make it fits to their needs. Low motivation and poor understanding of the threats leads users to circumvent password security policies. If a password is too long and difficult to remember, they would write it down and put in places of easy access, so they can use it again. If a system requires change of password frequently, users tend to use sequences or same passwords over again, with minimal change.

Security advices are rejected or ignored because of the amount of information and rules of security that sites and programs require can be quite overwhelming especially if we consider the amount of services we now use that require passwords: web emails (multiple emails, multiple passwords), the various social networks, browser testing tools, banks, work computer, personal computer, mobile devices (if locking screen), parental controls on computers or TVs, and these are just a few examples. In general user performs a calculation of cost/benefit almost automatic in their heads when deciding whether to follow security advice or not [16].

The goal of security advice is to protect user from certain attacks. Password strength rules protect them from brute-force and guessing attacks. URL reading protects them from phishing attacks. Identifying certificate errors protects them from man-in-the-middle or web-spoofing attacks. If the user follows the advice the hope is that he will reduce or eliminate the risk of being a victim. However, if the effort to follow security advice is higher than the benefits, users won't follow. Despite claims of insecurity on mobile banking users are willing to use simple mechanisms such as the mobile number or PIN for authorising micro payments. For macro payments and account transfers higher security is required and wireless adaptations of PKI and TLS/SSL have been developed to enhance the security of mobile transactions [31]

3.4.2 Mobile Banking in The Developing World

According to [20] "the spread of mobile phones across the developing world is one of the most remarkable technology stores of the past decade". It was found that there were more headsets than bank account services to the population. With that information in mind new opportunities were created to give people access to financial services, as mobile banking, mobile transfers and mobile payments. For the users in developing countries the appeal of these mobile services less about convenience and more about accessibility and affordability.

In these countries the time and money saved because of the use of mobile banking were also significant: “A Kenyan coffee farmer uses SMS banking once a month to check his bank balance; he gets one deposit per month from one of his buyers; the 30 shillings he spends on the SMS saves him a 200 shilling trip to the ATM; he has memorized the exact code he needs to send a text message to the ATM ” [13].

In South Africa the lack of trust and unawareness were among the primary reasons why people were reluctant to use mobile banking services, but the benefits surpassed the lack of trust for many of its users. There are different types of challenges that may inuence a user’s decision to adopt or no a mobile banking application, mostly based on the trust or mistrust of a combination of the following:

- Interface design (how many steps necessary to do the banking, size of buttons, fields, labels, and others).
- People coming to banking for the first time via handset (and getting use to the idea of “virtual money”).
- The use of other financial systems (formal or informal) and the reluctance to change to the ’unknown’ system.
- The self (being able to use the system).
- The technology (mobile and security layers/mechanisms).
- The network (where their funds travel).
- The channels (representative of institutions who control their money).
- The institution (the bank or other company providing the service).

Some of the benefits for the use of mobile banking are:

- Easy to use.
- Anytime and anywhere.
- Accessible for a wider audience.
- Cost of transfers via mobile banking are generally less expensive than alternatives on poor households and paying a lower fee is a positive impact [20].

3.4.3 Alleviate the Fear, Educate the User

According to [39] helping users to reduce their fears about mobile banking should be a priority for financial institutions; and to achieve that education of their customers on the security used for mobile banking apps is one of the steps.

After my brief search on mobile security for Barclays and Natwest mobile applications, I was surprised on so little information was given about security mechanisms used by these institutions. While I respect the right to hide some of the specifics of the security methods to avoid potential attacks, I see the lack of clarity a way of protect the institution in case something that was promised to work have a security breach in the near future. However this attitude just contributes to the fear of general public since no better information is found in their websites.

Most users want easier and more convenient access to their bank accounts, but they are not aware of how safe it is to use a mobile banking app. In reality, banking via a mobile app is as

safe as walking into a bank and interacting directly with a teller, and it is actually much more secure than banking through a browser on a personal computer. Because banks can control the security on an app much easier than through a browser [39].

When customers use their browser to do their banking, they leave themselves open to malware and man-in-the-middle attacks. In recent bank breaches, hackers could gain valuable information about users' bank login credentials, even their two-factor authentication credentials in some cases, by key-logging and stepping in between a user and his or her bank's website. Even when a bank has strong security, if users' computers are infected with malware or a virus, they may be vulnerable to attack. This same threat is also possible on mobile browsers.

4 A Study in Mobile Banking

4.1 Questionnaire Design

A questionnaire was created to collect information about the target audience and to make visible possible correlation between age, gender, knowledge of computer systems, familiarity with mobile apps and trust in mobile banking.

The expectations were that the sample would indicate a minority of users performing mobile transactions with the banking app, since mobile banking applications are still a new territory in the UK. It was also expected to have a relation between age distribution and trust in mobile banking, with an initial assumption that a younger public with higher computer skills would trust mobile applications more easily than others.

The questionnaire design was broken down in three sections: demographics, general mobile usage and security-related questions. The demographic questions identify gender, age, occupation, education and computer skills. The general mobile usage section identifies if users are familiar with applications in general. Security-related questions were created to identify the trust in the bank as institution providing a service that should be inherent secure; the trust in technology used for mobile banking either via browser, SMS or application; the general perception of security using online banking (mobile or desktop browser); trying also to pinpoint a possible reason why some of the people that answered the questionnaire choose not to use any mobile method for their banking needs.

A number of tools were available to run the questionnaire and collect its answers, most had a free option allowing just one form or a limited number of responses. I chose Adobe Form Central over the others as it allowed me to check live data, monitor the progress, extract results via Excel files (CSV) or PDF files, as well as exporting graphics directly. The control over the full process of survey was interesting, with options for breaking down into pages, skip-logic in case some questions require answers from other questions first, customised messages for final "thank you" page, url redirect (if needed), custom filters for analysing results in graphical form. This tool offered few templates according to the purpose of questionnaire, the designing tools and ease of use were a bonus, all aligned with my personal taste and purpose for this work.

As incentive, an Amazon gift voucher of £25 was offered. Personal experience in filling forms dictated that choice. People are generally more inclined to contribute to a survey if an exchange for their time is offered, and this incentive worked well generating results. For the prize draw specifics, I selected a person randomly using the follow simple method:

- I exported the answers collected from Adobe Form Central (in Excel format).
- Reordered the list by the ones that answered "yes please!" first (some randomness was generated with this step).
- Noted the total number of rows (number of people that asked to be included on prize draw).
- Went to http://random.org and entered the number on their "True Random Number Generator".

- And a number within the band limit was random generated!
- Then, all I had to do is to check who was in the row with that number and the random selection was done.

This method was explicit on the page where the winner was announced. The feedback received from some of the participants was positive, they liked the short survey and the form design/layout and the explanation about how the winner was chosen gave them a sense of fairness.

4.2 Mobile banking questionnaire

The questionnaire started with the following questions related to demographics:

Please indicate your gender:

◯ male
◯ female

Please indicate your age band:

◯ <18
◯ 18-24
◯ 25-39
◯ 40-60
◯ >60

Please indicate your current occupation:

◯ student
◯ employed
◯ unemployed
◯ self-employed
◯ other

Please indicate your highest education level:

◯ primary school
◯ secondary school
◯ graduate
◯ post-graduate
◯ other

How do you consider yourself regarding your computer skills?

◯ basic
◯ intermediate
◯ advanced
◯ expert

◯ other

Then a few questions about general mobile usage:

Do you carry out banking transactions on your mobile device (either via mobile browser or mobile banking app)?

◯ yes
◯ no

Do you use mobile applications, in general?

◯ yes
◯ no

And then the security-related questions:

Do you believe that banks provide enough security on their websites or mobile applications?

◯ yes
◯ no
◯ I don't know

Does your bank provide compensation for losses due to mobile banking fraud?

◯ yes
◯ no
◯ I don't know

For each method of online banking, please indicate how secure you believe each one to be:

Website:

◯ low security
◯ medium security
◯ high security
◯ not sure

Application:

◯ low security
◯ medium security
◯ high security
◯ not sure

Which of the following actions do you believe should be taken in order to increase mobile banking security:

☐ use antivirus
☐ use trusted networks

☐ use trusted websites
☐ use trusted applications
☐ I don't know

Are you concern with data security when using mobile banking?

◯ yes, the main reason that I don't use it
◯ yes, but use anyway
◯ yes
◯ no, I trust in my bank services
◯ no, it is unlikely for a security breach to happen
◯ no

Please indicate who/what you think is responsible for your security while you are using mobile banking:

◯ banks
◯ networks
◯ websites
◯ applications
◯ yourself

Which security aspect are you most concerned with?

◯ Hackers gaining access to my phone remotely
◯ Someone intercepting my calls or data
◯ Losing my phone or having my phone stolen
◯ Malware or viruses being installed on my phone
◯ Other

Please indicate if you think the following methods for mobile banking are safe or unsafe:

SMS (text messaging)

◯ safe
◯ unsafe
◯ don't know

Mobile browser similar to the way you access the Internet on your PC

◯ safe
◯ unsafe
◯ don't know

Application downloaded from your phone's mobile app store

◯ safe
◯ unsafe
◯ don't know

How would you currently rate the overall security of mobile banking for protecting your personal information?

◯ safe
◯ unsafe
◯ don't know

Do you wish to be included on a chance to win a £25 Amazon voucher?

◯ yes please!
◯ no, thank you.

In case the person selects NO for the question 'Do you carry out banking transactions on your mobile device (either via mobile browser or mobile banking app)?' then the following question is added at the end:

You indicated that you do not currently use mobile banking. What is the main reason why you have decided not to use mobile banking?

◯ I'm concerned about the security of mobile banking
◯ My banking needs are being met without mobile banking
◯ The cost of data access on my wireless plan is too high
◯ It is too difficult to see on my mobile phone's screen
◯ It is not offered by my bank or credit union
◯ My bank charges a fee for using mobile banking
◯ I don't trust the technology to properly process my banking transactions
◯ I don't have a banking account with which to use mobile banking
◯ It's difficult or time consuming to set up mobile banking
◯ Other

And if the person selects YES for the question 'Do you carry out banking transactions on your mobile device (either via mobile browser or mobile banking app)?' then the following questions were added to the questionnaire on the section of general mobile usage:

Please select how often you access details of your bank account with a mobile phone:
◯ daily
◯ 3-4 times a week
◯ 1-2 times a week
◯ 1-2 times a month
◯ other

Please select the method(s) you use for mobile banking:

☐ website
☐ application
☐ other

And also the following questions on the security-related section:

Relating your mobile banking service, do you...

Trust it overall?

◯ yes
◯ no

Trust in the bank?

◯ yes
◯ no

Trust in the technology of mobile banking?

◯ yes
◯ no

Trust that is secure from fraud?

◯ yes
◯ no

Is it easy to use?

◯ yes
◯ no

What is the top reason you are dissatisfied with your mobile banking experiences?

◯ I am concerned about my personal information being disclosed or have had personal information disclosed as a result of mobile banking
◯ Applications and/or websites for mobile banking are too complicated to use
◯ I have had problems getting the websites or applications to work properly
◯ Banking on my mobile phone takes too long
◯ It is too difficult to see on my mobile phone's screen
◯ The transactions I want to execute are not available
◯ Other
◯ I'm actually satisfied with mobile banking

A preview of the actual questionnaire can be viewed online for a limited-time only (until 15th June 2013) at https://adobeformscentral.com/?f=wR2I798df–m54z-E8PZeQ&preview

4.3 Sense of Trust from Data

With the incentive of an Amazon Voucher, I gathered answers from 101 people in a speedy manner. Observing the live data appearing on the Adobe Form Central was an exciting exercise and an interesting way of observing partial results.

The following graphics show the statistics for the questions asked.

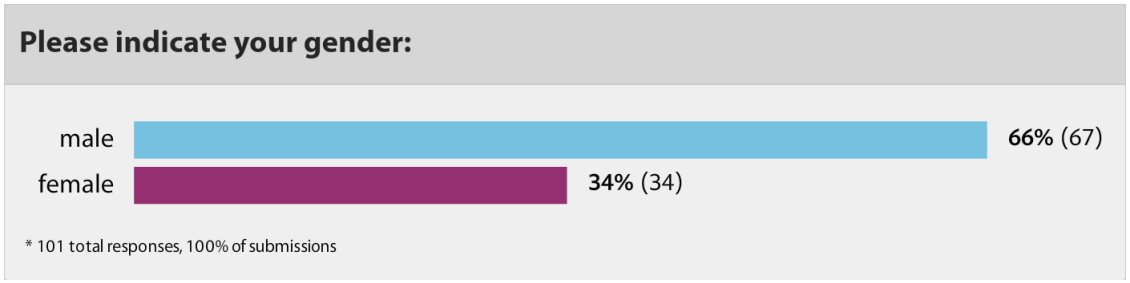

Figure 4.1: Demographic question - Gender

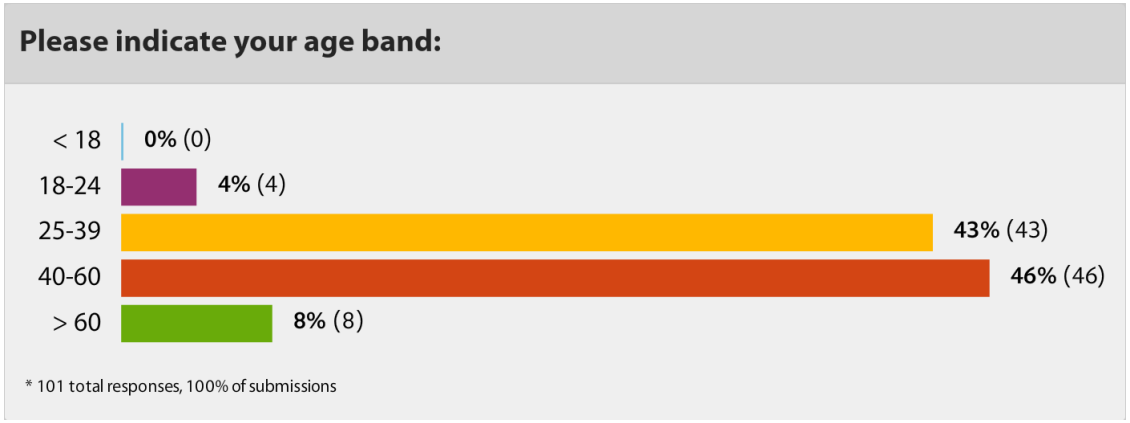

Figure 4.2: Demographic question - Age

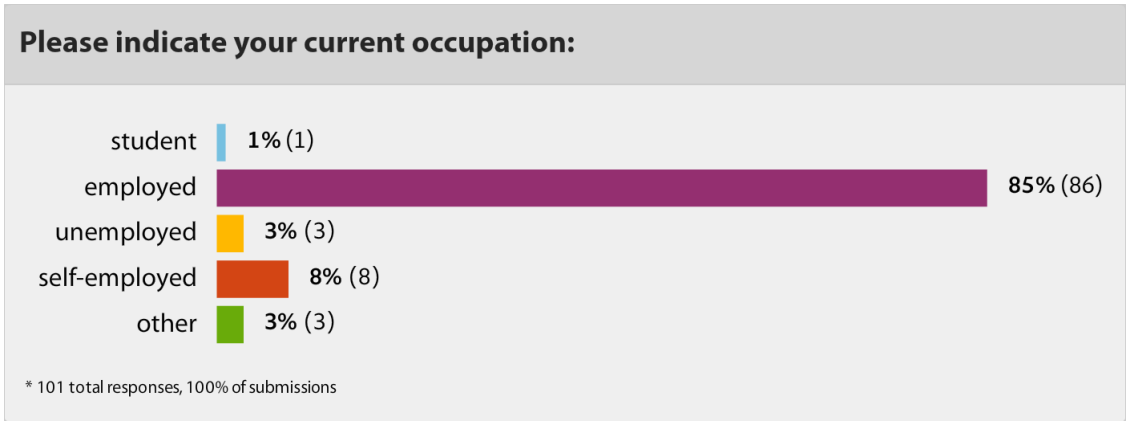

Figure 4.3: Demographic question - Occupation

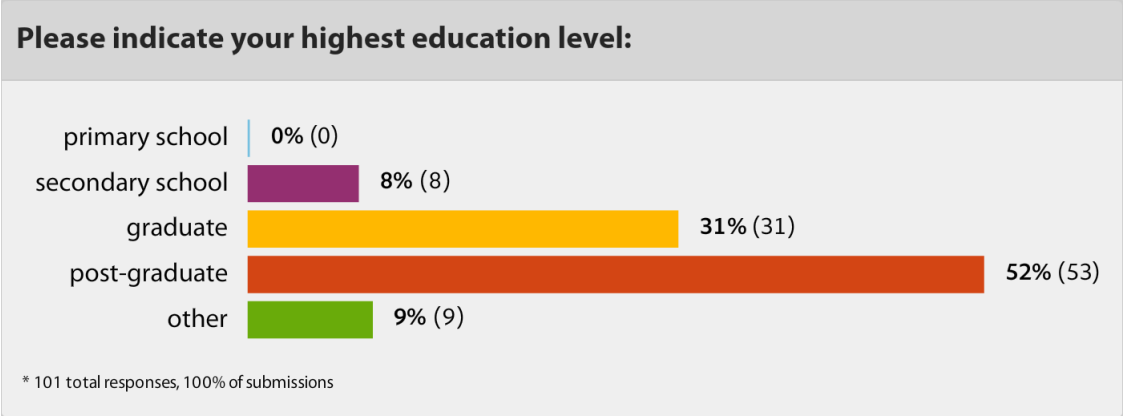

Figure 4.4: Demographic question - Education level

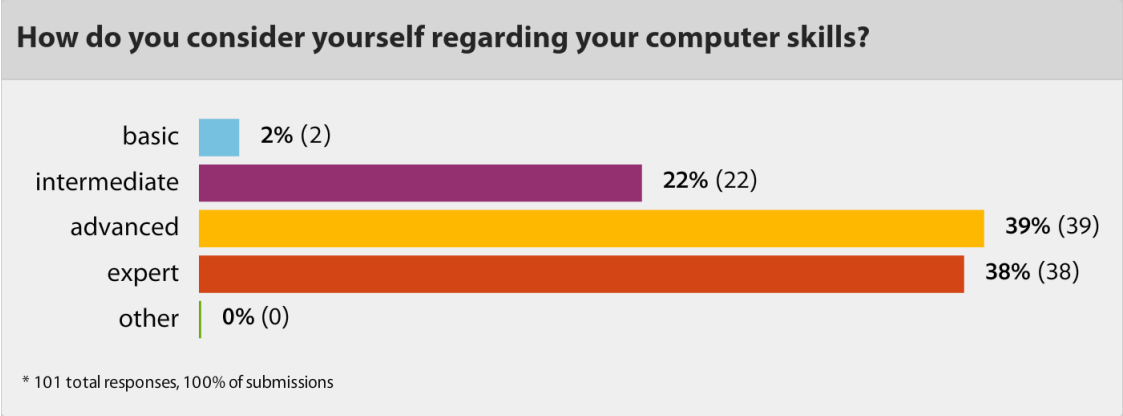

Figure 4.5: Demographic question - Computer skills

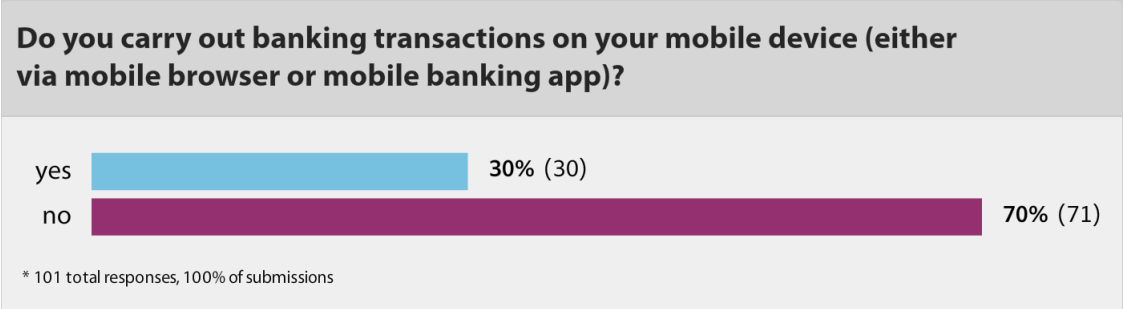

Figure 4.6: Mobile usage question - Use o mobile for banking purposes

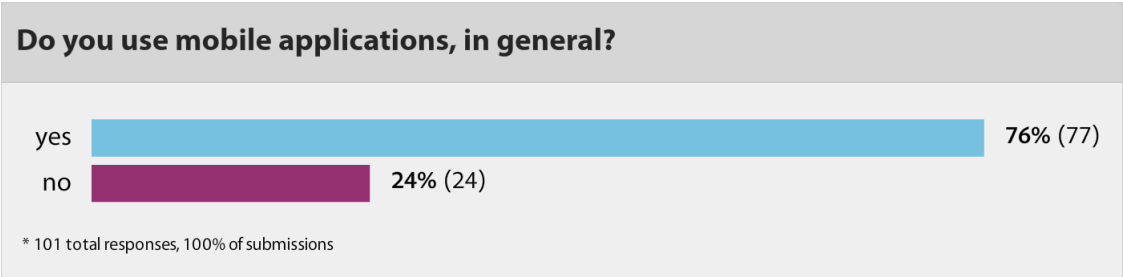

Figure 4.7: Mobile usage question - Use of mobile applications in general

At this point it is interesting to notice that, despite users' familiarity with apps, only 30% of them access mobile banking.

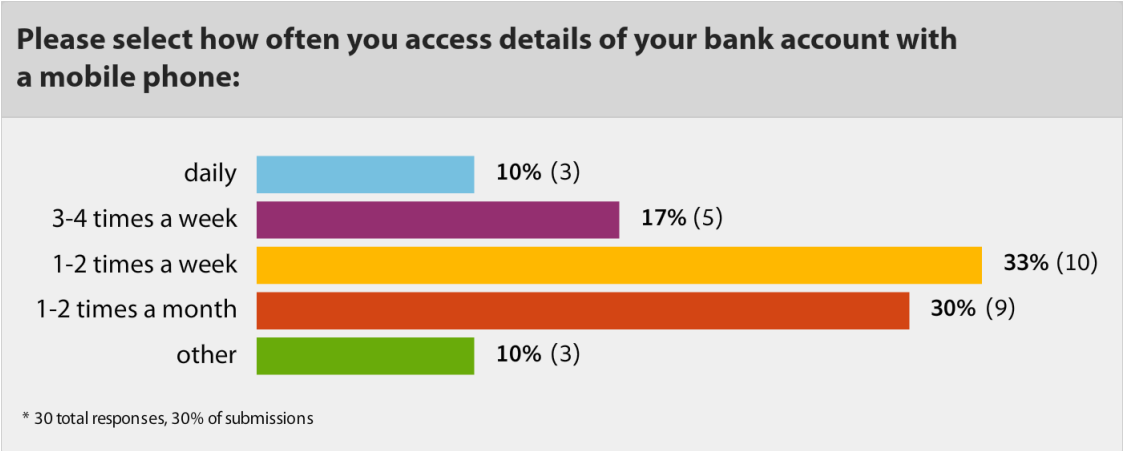

Figure 4.8: Mobile usage question - Access of bank account via mobile

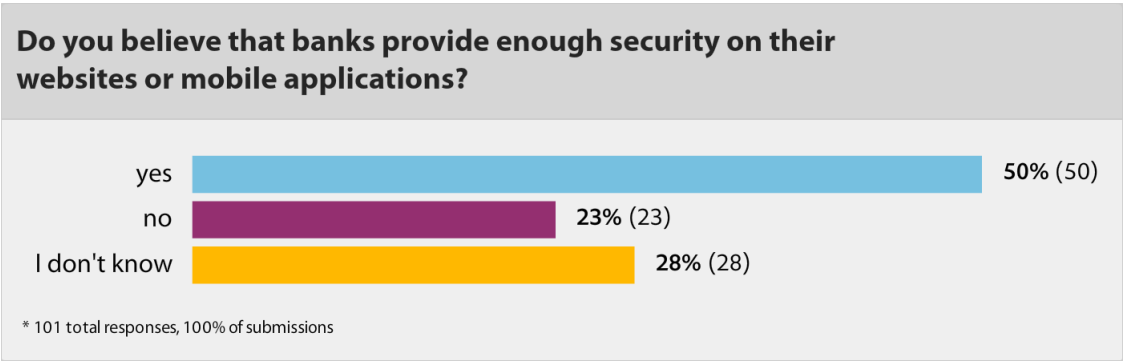

Figure 4.9: Security question - Security offered

The trust in the bank's ability to provide security, as shown in the graph above, is considering the whole set of answers. Filtering the results to only select people who use mobile banking shows that 80% of responses were YES, 13% don't know if the banks provide enough security and 7% answered NO. The later reects the belief that banks do not provide enough security but nevertheless the mobile banking was used by the two individuals (7%).

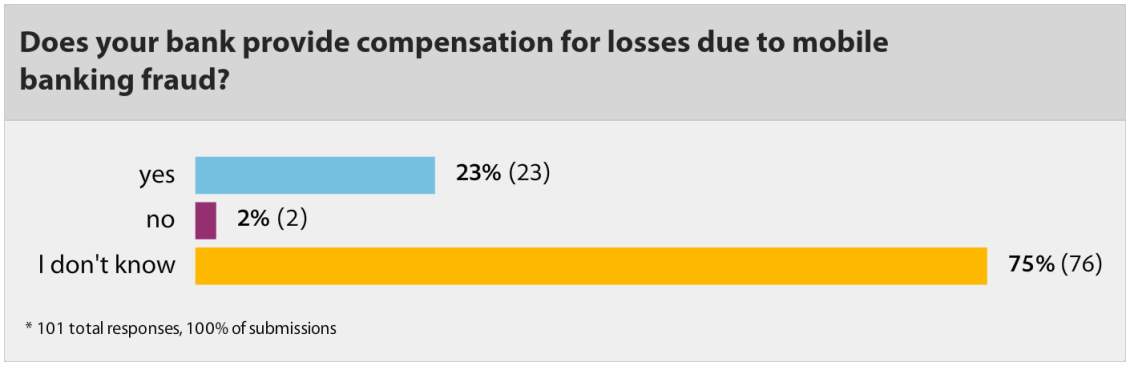

Figure 4.10: Security question - Compensation for losses due to mobile banking fraud

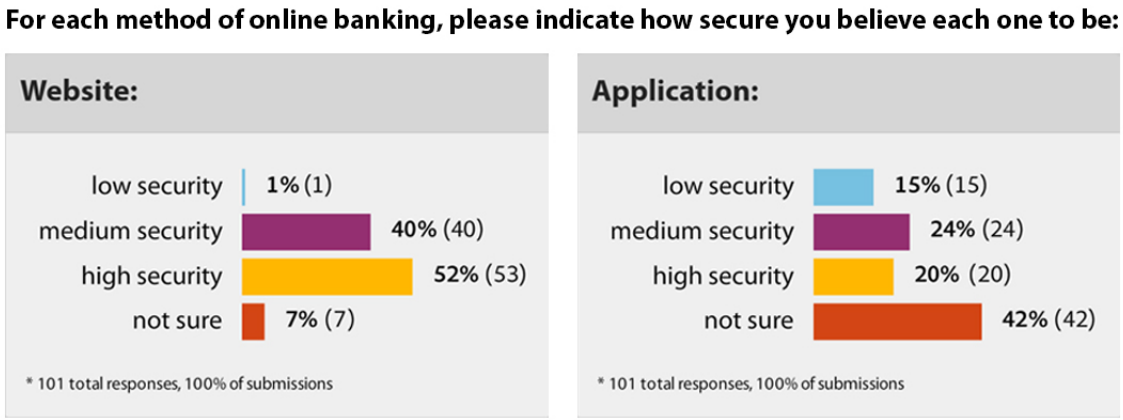

Figure 4.11: Security question - Website and Application security levels

These results could indicate that trust in online banking via website is a method established for longer in user's life and possibly the reason why receives a higher level of trust than applications. However, for the same question, only considering mobile banking users, the "website" option received similar levels of trust, but the "application" received 77% of responses indicating medium or high security. In the light of the previous chapter, we can see that the sense of security on each medium wouldn't reflect the current situation, as online banking exposes the users to a larger range of possible threats than an app.

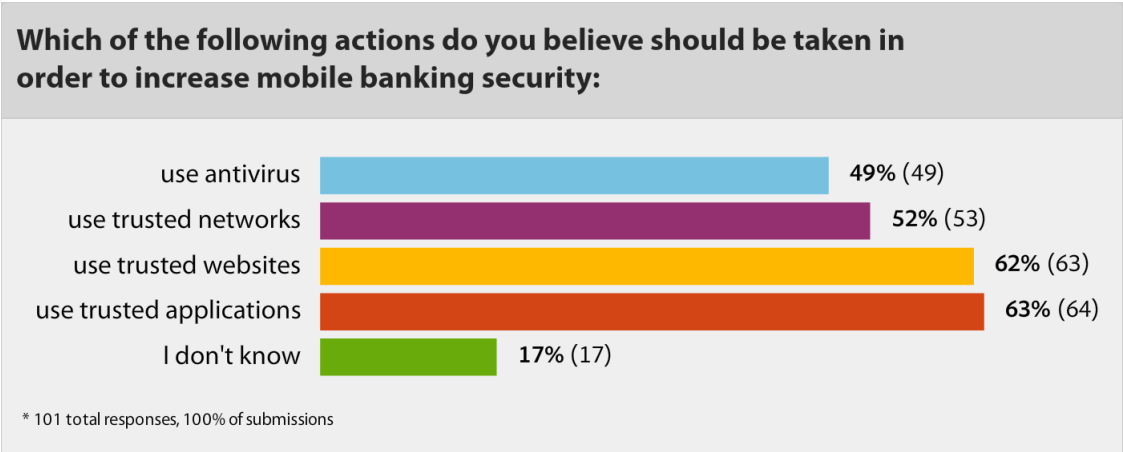

Figure 4.12: Security question - Actions to increase mobile banking security

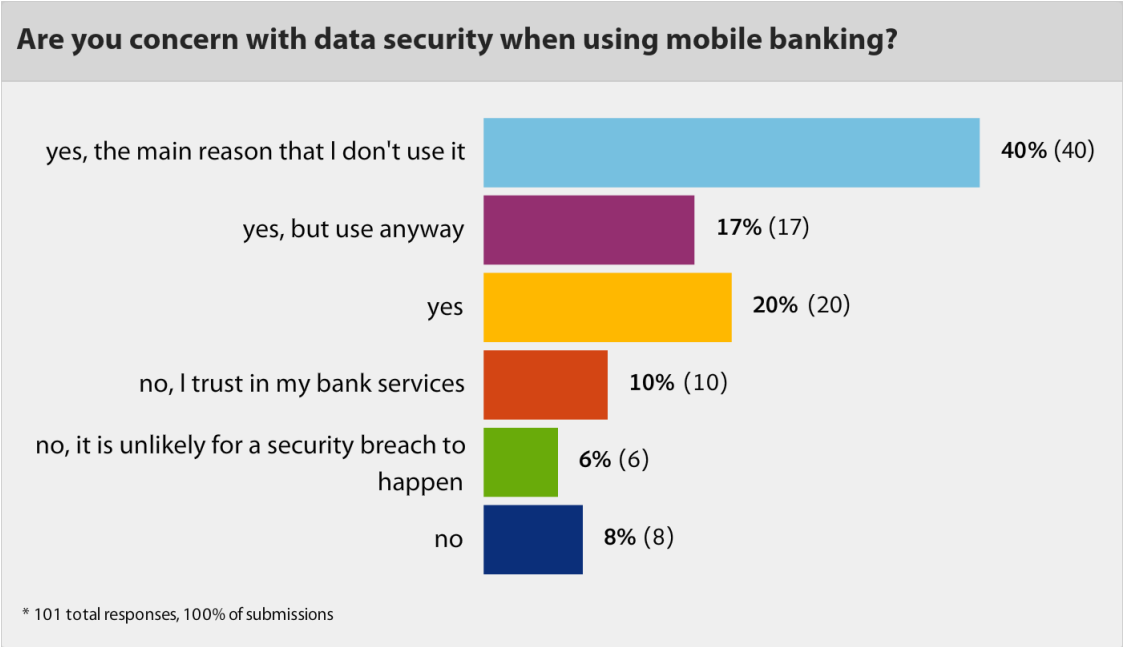

Figure 4.13: Security question - Concern with data security using mobile banking

This is the first question where results could point for a possible reason why people don't use mobile banking. It only mentions data security as concern in the question phrase, which could be slightly misleading. However, figure 4.17 solely addresses the possible reasons for not using mobile banking giving more insight into user perceptions. It is quite interesting to notice that even in between people with higher education, higher computing skills there is a lack of understanding of real threats and a naive trust that "everything is going to be ok" and "it is unlikely for a security breach to happen"; to my surprise that 6% of users think that. Maybe considering that threats don't reach a massive number of users at one time that perception is not so naive.

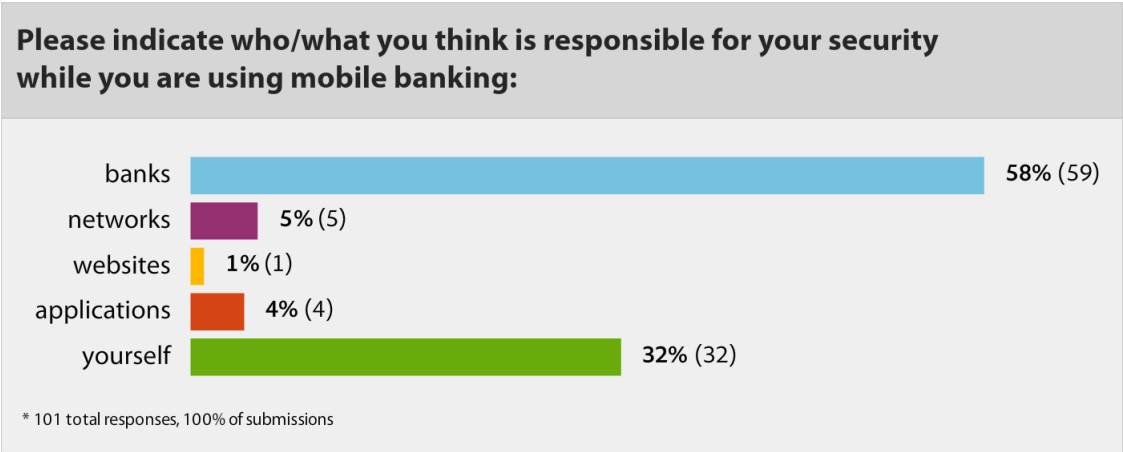

Figure 4.14: Security question - Security responsibility

A vast majority believes that banks are the main responsible for security while using mobiles for banking purposes, followed by the sense of personal responsibility from 32% of users. That was an interesting result consolidating that users would rely on banks for the security of their applications however they are not eliminating the responsibility that they also have including the choice of mobile device and network, installation of antivirus or protect mobile screen with password

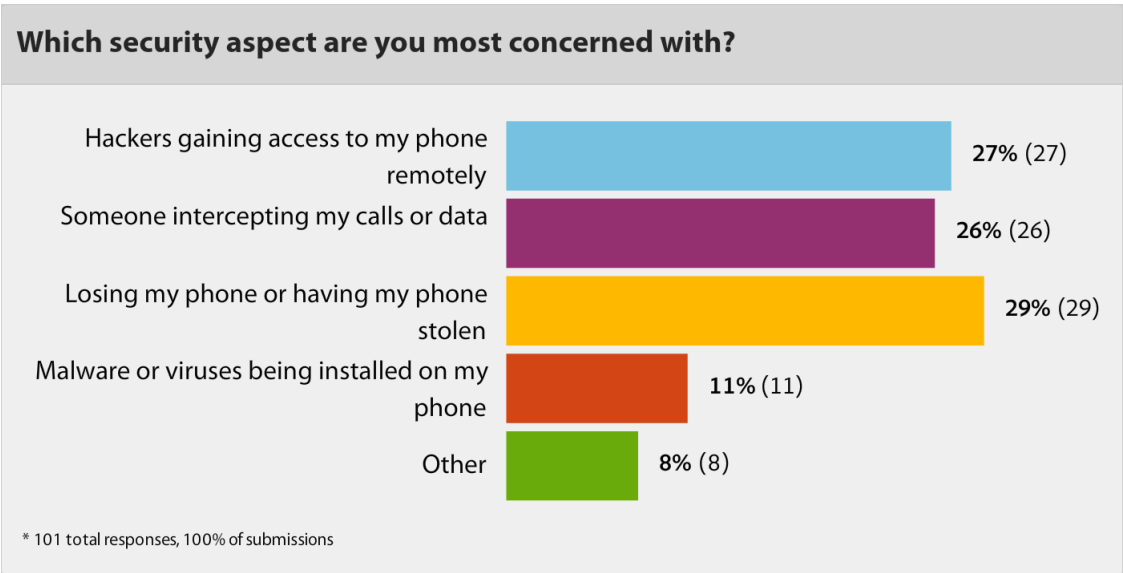

Figure 4.15: Security question - Top security concerns

I was expecting that one of the concerns would be more prominent than others but the, now, top three concerns show quite a good distribution and division of opinions.

The top two reasons for not using mobile banking were “security concerns” and “traditional banking already covering users’ needs”. Perhaps, since users have easy access to internet, they don’t feel the need of another tool/method for bank transactions.

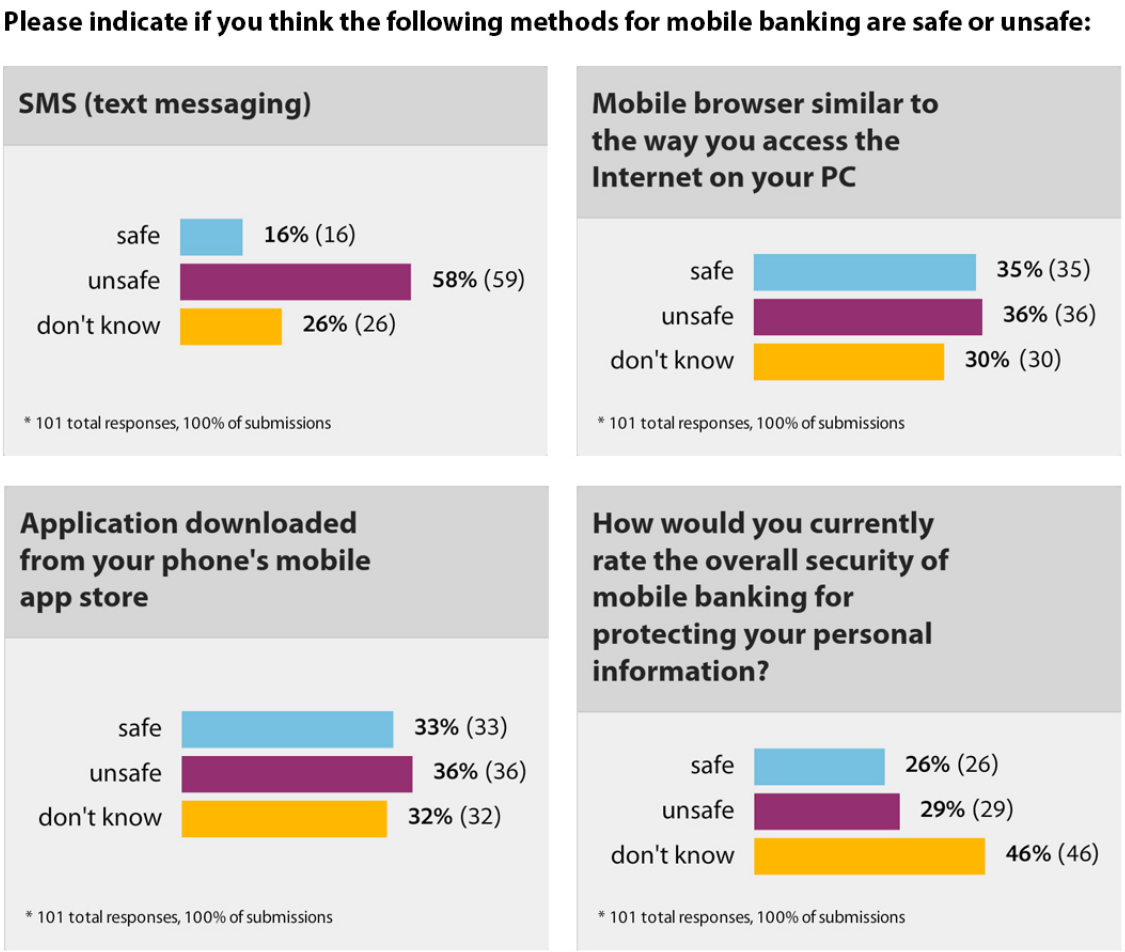

Figure 4.16: Security question - Mobile banking methods: safe or unsafe?

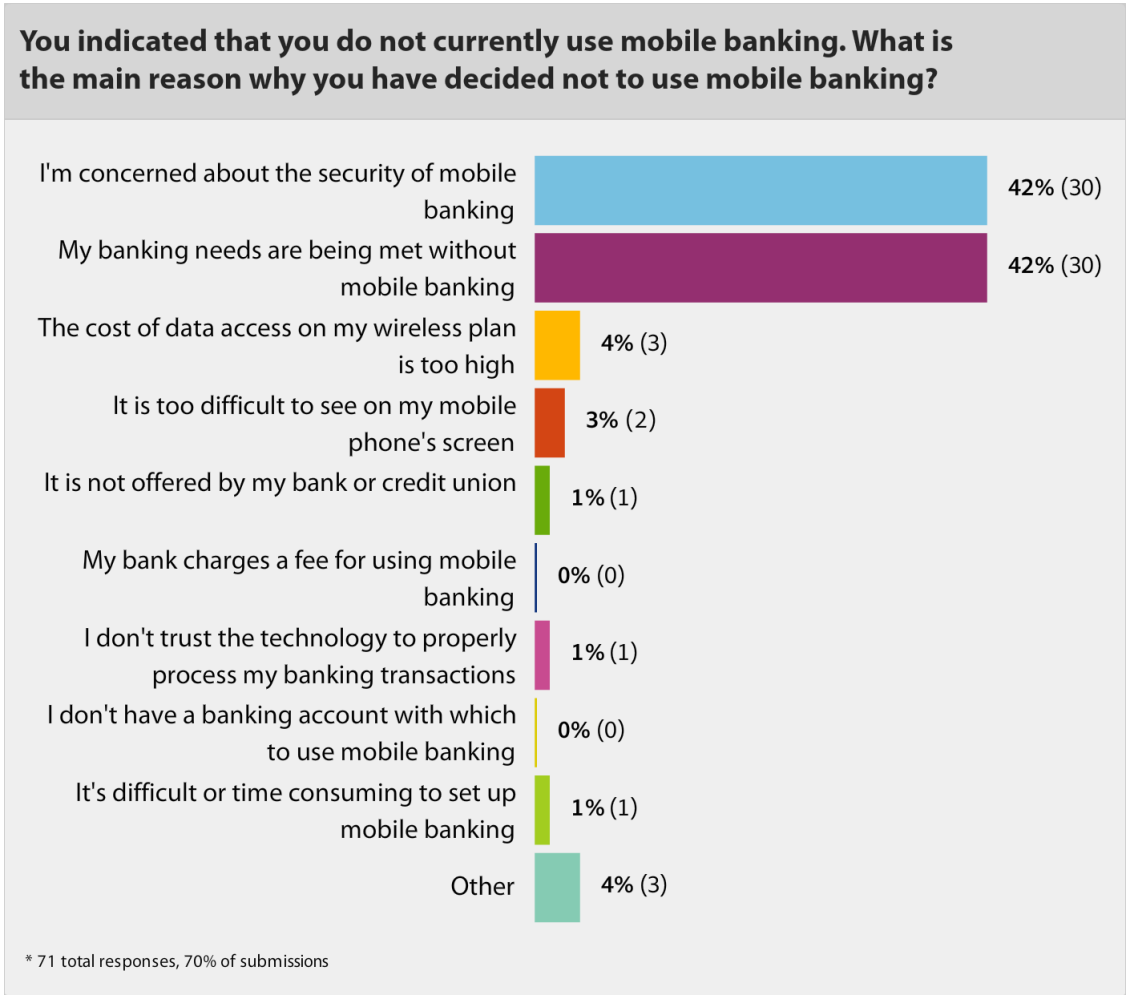

Figure 4.17: Security question - Main reason for not using mobile banking

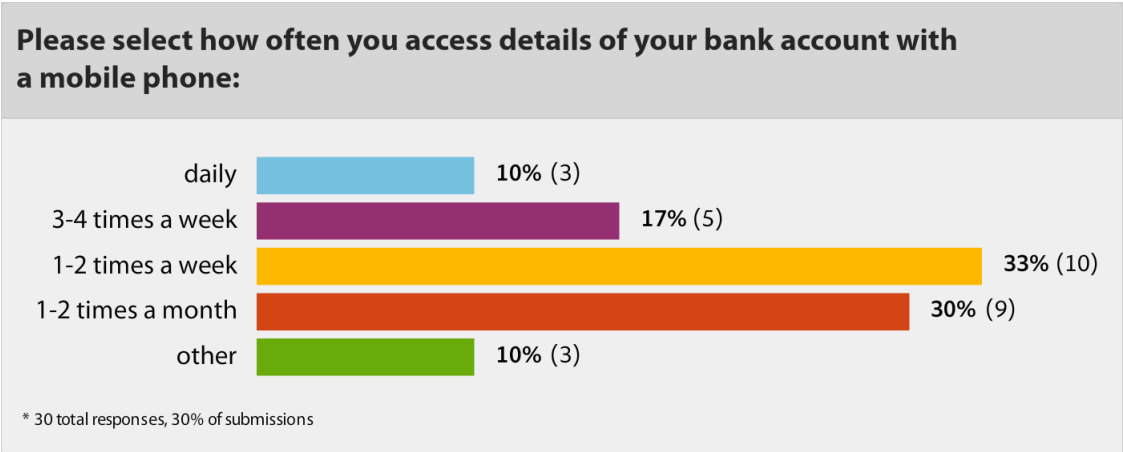

Figure 4.18: Mobile usage question - Access of bank account via mobile

The frequency of access showing 10% daily use and 17% 3-4 times a week seems high. Perhaps due to the easy use and access, users would check their balances more often. Still the majority (66%) access mobile banking from 1 time a week to 1 time a month, analysing the raw data I especulate if that could be because of finantial maturity of the sample - above age 25 - that possibly have more financial control over expenses and don't feel the need of checking account with higher frequency.

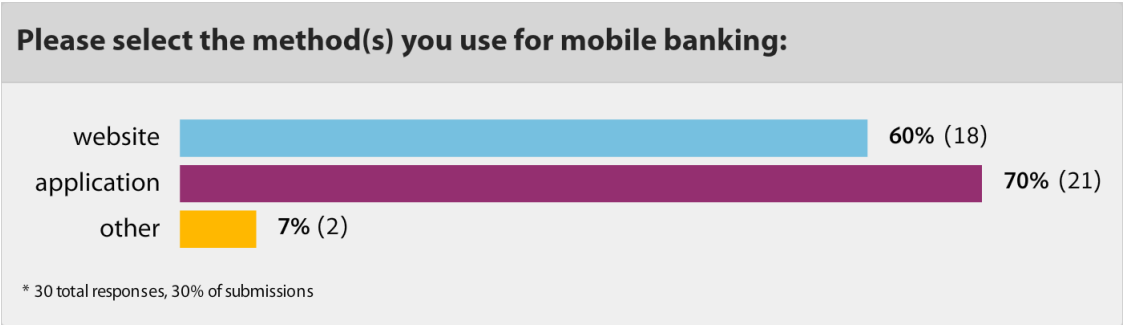

Figure 4.19: Mobile usage question - Method used to access bank account

Analysing the raw data I could see that in 10 answers (approximately 30%), users access their mobile banking with both website and application methods.

YES answers were expected to be the majority of the graphics in this section. Users answering NO to each of the options still carried out mobile banking, possibly because of its ease of use.

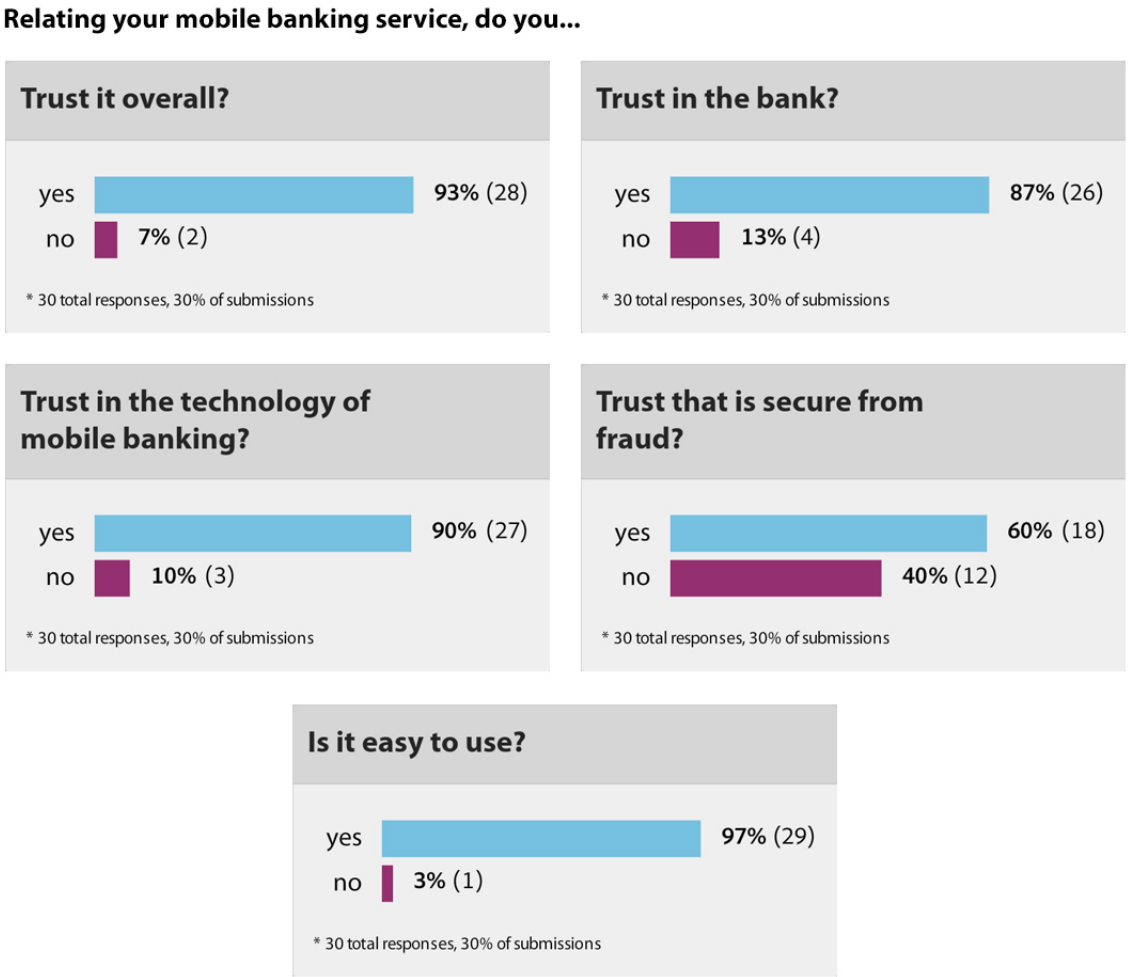

Figure 4.20: Security question - Mobile banking trust and ease of use

4.4 Reflection

This dissertation was a great opportunity to render myself more literate regarding mobile banking.

The security modules I attended during the Software Engineering Programme tackled security in many ways. Bank applications were fairly new at the time so security elements specific to mobile aspects were not covered. However, security risks and measures are applicable to both smarphones and computers due to their operating systems and browsers similarities, providing me with foundation knowledge.

SPR RIS PLA DES

Research and a questionnaire were the methods used to analyse users' trust in mobile banking. There were some papers mentioning trust in mobile applications and links related to mobile banking but some of them reected results from 2 to 5 years ago, not representing the current situation. I kept the questionnaire short and visible all in one page to motivate volunteers to answer it completely and not to abandon the form during the process.

The tool of choice for this task was also important. I wanted a tool that could make the process of running the questionnaire and collecting its answers seamless, easy to use, with good layout and with possibilities of filtering results prior to exporting data to different formats. Adobe Form Central gave me this exibility and the process of accompanying partial results was quite exciting, observing expectations unfolding in graphics on screen.

The decision to give a voucher to volunteers that contributed to this work came from my own experience on filling forms and having hope to be selected for the prize. It is an exchange of "favours", they give their time and opinion while the owner of the questionnaire offers some token of gratitude. I believe this choice yields faster results when time is limited.

Looking back on the whole experience, I can see elements that if done differently could have given richer answers and insights on the mobile banking experience. For start, the questionnaire was run over a short period of time, only two days. Considering that I received 101 answers, I wonder how many more answers I would be able to collect if the questionnaire was run for two weeks instead.

The method of dissemination of the questionnaire was not diverse enough. I distributed it within the University of Oxford and, regardless of being a diverse environment, would bias some of the answers such as age group and education. This was counter-balanced with social media distribution (Twitter and Facebook) which tapped into a more diverse group but, since messages in this medium could be diluted with the "noise" of other messages, I wonder if I should have asked "how did you came across this form?" or if I should have added an identifier for each method of distribution.

Some of the questions selected could have been written in a different way or were dependent of other factors that I didn't take into account. For example, when asking if the user carried out banking transactions on mobile device, this was the first question on mobile usage section and I didn't consider that, despite minimal chance of happening, maybe a user doesn't have a mobile phone and the remaining questions would be irrelevant for him/her. On the question asking who or what the user thinks is responsible for security while mobile banking, it would be clearer to ask who/what they think is "most" responsible because there is a combination of factors and not a single-choice as presented.

Perhaps if I had added a free text field on questions where the "other" option was available, I would discover some other concerns or aspects that were not asked. Some users replied directly to me with suggestions that were valuable. One simple option that I overlooked is to add a free text "other comments" at the end of the questionnaire to gather suggestions, frustrations, doubts about the questionnaire or the topics themselves.

One of the suggestions pointed exactly that:

> *"A free text comments field at the end of the questionnaire for further observations would be useful. For instance I would like to say: 'I don't use mobile banking BECAUSE I am a security administrator and I KNOW network security is not completely watertight'. However, banks are not at all open about security measures and therefore how can I trust them?"*

This suggestion relates to one of the points on my dissertation where mentions that Barclays and Natwest give general suggestions on how users should behave or protect their devices. They mentioned how security (the term "security" in its broader aspect) is used in their applications and websites to reassure its customers that is safe to bank with them. However, I couldn't find technical specifications about encryption, network security, password policies and other elements of security that are being used. With this statement I am not requesting the banks to openly publish the level of security applied and sensitive information that can be used against them and their customers, but more information would be beneficial for the users that are technically aware and want to know the risks and measures taken by their banks. On the other hand, I am favourable of transparency in the use of applications and websites, where the banking, when possible should keep security checks and "annoyances" to a minimum (still maintaining security), so it is hard to have a balance there.

Another feedback was:

> *"Just a thought one item you have not asked about, which is in common use in internet banking, is the validation of transactions with a portable card reader which uses your PIN and generates a one-time code to validate transactions. I might consider mobile banking if it was secured with a dongle that uses personal data not stored on my phone or generally available."*

I found this suggestion very interesting because it adds another layer of security without asking the user to put cards in gadgets, enter PIN, generate tokens etc. which it was mentioned in many other works about resistance of adoption or compliance, and the cost that security adds to the user's tasks. Taking away part of the burden for the user to remember strong passwords/passphrases and adding a "transparent" layer or security could facilitate the adoption of mobile banking considerably.

Yet, another suggestion coming from email:

> *"Asking whether mobile banking is 'safe or unsafe' is very hard to answer truthfully – nothing is 100% 'safe' (from what?), it's always a risk/benefit analysis."*

This was a good point, it seems now that my question was incomplete (maybe was my inexperience in creating forms). The questionnaire was used to gather feedback on trust in mobile banking and if the users would trust that security was properly implemented to allow them to use mobile banking. For a quick survey, I still think the questions give the idea needed for the context of this dissertation. However, if further research is done, maybe a more appropriated way would be give examples of levels of security or examples of treats that banks address to guide the users answering the question.

An interesting comment was made:

> *"I said no to voucher, because I don't want my name associated with my answers = potential security treat"*

– the comment was made in a very friendly and humorous manner but did ag that perhaps the link to the answers should have been clearly identified as not anonymous (or offer other

solution). I could track back the answers related to a specific individual the way the form design was made. If I had a redirect from the end of the form to a secondary form which would gather names that wished to be entered on the prize draw would be more appropriate. Not only a separated form but also eliminating the timestamps on the entries (otherwise the identification would be still possible).

This last email finished with:

> *"I do worry though about banking on-line – and wonder just how the bank would respond if somebody hacked into my account, somehow via my accessing it. It's convenient of course – but people are very clever these days."*

Some of the banks offer compensation, but I didn't explore the terms and conditions for such, and they could vary from bank to bank. The top security concerns figure 3.19 illustrates that concern is high, even among the users of mobile banking.

Another question that could have been asked related to this aspect is:

> *"if your bank offers fully compensation for any financial loss resulted from mobile banking, would you still be worried to use their mobile services?"*.

5 Conclusion and Future Work

Mobile phones have become one of the most used mechanisms of communication worldwide. With the development and growth of mobile technologies, this device evolved and many models can now perform a multitude of tasks: from the communication using voice and video calls, text messages and multimedia messages, to assist its users in areas of entertainment, productivity, social networking, internet, news and many other categories. A vast range of possibilities are open for development and businesses.

In order to explore such opportunities and with the number of devices pairing with the number of global population, most banks have already launched their mobile applications and/or re-designed mobile version of their websites. Mobile banking is reaching larger populations, many of which don't have access to smartphones but to older phones that can still use the SMS interface to perform banking transactions. Users are adopting mobile banking (using mobile browser, SMS or bank app) in a much slower rate compared to other application categories. Nevertheless is an exciting opportunity for people that didn't have banking access and it is a growing business for banks and financial institutions.

In general, people trust methods that are already familiar and established in their lives; aversion or reluctancy to change is understandable since it causes extra effort: the learning of a new technology or process; the costs related to them; the lack of understanding of benefits, and the potential threats that can 'scare' them away.

Mobile banking is not different. The results of a security breach can cause financial loss, distress and many other social impacts in the user's privacy. There is an indication that mobile banking is being adopted in many countries and within certain groups, either because of need: in the case of the "unbanked" in Kenya, with 14 million of users to date [35], or because of a higher understanding on the security measures applied by banks and the trust on mobile banking applications platform. Overall trust in mobile banking is still shy and this medium is not yet established considering only 20% of its adoption in more than ten years of mobiles running compact versions of operational systems.

Cost-effectiveness for users is important, in many studies barriers or extra steps to perform tasks, despite these steps could ensure security to mobile banking use, it will delay users' adoption. Business institutions and the development community shouldn't overlook the fact that simply reinforcing security policies that don't consider user needs will ended up drive them away.

A mobile user may have a basic understanding of security risks while performing mobile banking but overloading the process with security measures that are not transparent to the user won't increase rate of mobile banking. And despite the existing threats, some users still ponder about the convenience and access of mobile banking and will perform mobile transactions even if they fear privacy breach or financial loss.

Helping users to reduce their fears about mobile banking, providing clear communication to customers on how they provide security and a safety net (compensation for losses due mobile banking fraud) should be part of the banks' strategy for mobile banking spread. General education about mobile risks and ways of mitigating and deterring them could contribute to user's understanding, but keeping in mind that elements of security should be tranparent on

the process of using mobile applications or mobile banking in general, in the sense that banks should provide the security mechanisms that have lower impact on the user's behaviour.

In the light of the research for this dissertation, I would like to consolidate the following findings.

Applications can be considered safer than accessing banking account through a web browser. Apps provide a direct link from the device to the bank, without having to go through any additional browser or third-party applications. This means banks have better control over the security and connection with customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption, two-factor authentication and other elements to redeem the application secure for use.

Actors that influence mobile banking security:

- The self - user, customers.
- The technology - mobile device itself including its operation system, security layers and mechanisms.
- The network - communication channels.
- The channels - method to access mobile banking (i.e. application or browser).
- The institution - the bank.

Main concerns about mobile banking security can be addressed by:

- Installing mobile antivirus which will protect against malware and enable users to lock or wipe the device in the event it is misplaced or stolen.
- Download applications from official app stores.
- Adding a PIN or another screen-lock mechanism.
- Keeping OS updated.
- Do not use public Wi-Fi when banking via mobile device, opt for the 3G or 4G connectivity of the own smartphone. Although those algorithms can be hacked, any respectable mobile commerce site will have SSL encryption in place for further protection.
- Be aware of phishing emails that mimic your banks look and feel. Be familiar with the bank website so fakes can be discerned. Typos and problems with design choices are giveaways.
- Don't click on links in a suspicious email, type your banks URL in a browser and login from there.

And understand your bank's policy regarding mobile banking. If the bank provides a safety net and it is clear to its customers, the latter could improve the trust in mobile banking and in mobile banking applications.

> *"When you use Barclays Mobile Banking, you will automatically be protected in the event of fraud We'll cover any resulting loss, no matter how much money is taken from your account" [6]*

Some interesting findins about mobile banking applications and sense of security collected from questionnaire, however this study can be consider an initial work to explore the need for security and the trust of users in mobile banking. Future works could explore a wider audience and diversity of people, explore even more socio-economical factors that could influence mobile banking adoption and in terms of security a creation of elements that could remove the complexity layer from the user side and facilitate the process.

Bibliography

[1] Barclays Bank. Barclays mobile banking app. http://www.barclays.co.uk/BarclaysMobileBanking/BarclaysMobileBankingapp/P1242609123821, 2013.

[2] Barclays Bank. Barclays mobile banking app software terms & conditions. http://www.barclays.co.uk/MobileBankingServices/BarclaysMobileBankingappsoftwaretermsnbspnbspconditions/P1242610562319, 2013.

[3] Barclays Bank. What we're doing to protect you. http://www.barclays.co.uk/Helpsupport/Whatweredoingtoprotectyou/P1242560037946, 2013.

[4] Natwest Bank. Banking safely on your mobile. http://www.natwest.com/personal/online-banking/g2/banking-safely-on-your-mobile.ashx, 2013.

[5] Natwest Bank. Mobile security hints and tips. http://www.natwest.com/personal/online-banking/g2/banking-safely-on-your-mobile/hints-and-tips.ashx, 2013.

[6] Barclays. Mobile banking security & protection. http://www.barclays.co.uk/MobileBankingProtection/MobileBankingProtection/P1242622865207, 2013.

[7] Bullguard. Bullguard mobile security. http://www.bullguard.com/products/bullguard-mobile-security/android-security.aspx, 2013.

[8] Bullguard. Mobile security & malware protection - infographic. http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-security-what-you-need-to-know.aspx, 2013.

[9] comScore MMX. 1 in 4 internet users access banking sites globally. http://www.comscoredatamine.com/2012/06/1-in-4-internet-users-access-banking-sites-globally/, 2013.

[10] Pete Daffern. Mobile banking is more secure than online banking. http://www.businessweek.com/debateroom/archives/2012/02/mobile_banking_is_more_secure_than_online_banking.html, 2012.

[11] Dasun Weerasinghe, Veselin Rakocevic, Muttukrishnan Rajarajan. Security framework for mobile banking. In *MoMM '10 Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, pages 421–424, 2010.

[12] Deloitte. Mobile banking - A catalyst for improving bank performance. Technical report, Deloitte, 2010.

[13] Jonathan Donner. Re-examining m-banking: Linking adoption, impact, design, and use. http://www.jonathandonner.com/jdonner_mbanking_adoption_impact_use_lb.pdf, 2008.

[14] Eduardo Fernández-Medina, Manu Malek, Javier Hernando, editor. *SECRYPT 2009, Proceedings of the International Conference on Security and Cryptography, Milan, Italy, July 7-10, 2009, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications*. INSTICC Press, 2009.

[15] David Haskin. Prepare for mobile security threats. http://www.pcworld.com/article/132420/prepare_for_mobile_security_threats.html, 2007.

[16] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW '09: Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, New York, NY, USA, 2009. ACM.

[17] Amir Herzeberg. Payments and banking with mobile personal devices. pages 53–58. ACM, 2003.

[18] ITU. The world in 2013 - ict facts and figures. http://www.itu.int/ITU-D/ict/facts/material/ICTFactsFigures2013.pdf, 2013.

[19] Jeffrey Bickford, Ryan O'Hare, Arati Baliga, Vinod Ganapathy, Liviu Iftode. Rootkits on smart phones: Attacks, implications and opportunities. In *HotMobile '10 Eleventh Workshop on Mobile Computing Systems and Applications*, pages 49–54, February 2010.

[20] Jonathan Donner, Camilo Andres Tellez. Mobile banking and economic development: Linking adoption, impact and use. In *Asian Journal of Communication, 18(4)*, pages 318–322, 2008.

[21] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison. Security of mobile banking. Technical Report CS06-05-00, Department of Computer Science, University of Cape Town, 2006.

[22] Kaspersky Lab. Kaspersky mobile security. http://www.kaspersky.co.uk/kaspersky_mobile_security, 2013.

[23] Martin Lee. The security of password reset questions. Msc Dissertation, University of Oxford, 2008.

[24] John Lyle, Shamal Faily, Ivan Flechais, Andre Paul, Ayse Goker, Hans Myrhaug, Heiko Desruelle, and Andrew Martin. On the design and development of webinos: a distributed mobile application middleware. In *Proceedings of the 12th IFIP WG 6.1 international conference on Distributed applications and interoperable systems*, DAIS' 12, pages 140–147, 2012.

[25] John Lyle, Andrew Paverd, Justin King-Lacroix, Andrea Atzeni, Habib Virji, Ivan Flechais, and Shamal Faily. Personal pki for the smart device era. In *9th European PKI Workshop: Research and Applications*, 2012. To Appear.

[26] Tracy Mardigian-Kiles. Mobile banking trends: Find out what is hot and how to stay protected. http://www.webroot.com/En_US/consumer/articles/mobile-banking-trends-find-out-what-is-hot-and-how-to-stay-protected, 2013.

[27] UTalk Marketing. Mobile banking can improve customers' opinion of uk banks. http://www.utalkmarketing.com/pages/Article.aspx?ArticleID=18953, 2010.

[28] McAfee. Mcafee mobile security. http://home.mcafee.com/store/mobile-security, 2013.

[29] Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy (SP)*, pages 96–111, 2011.

[30] Carey Nachenberg. A window into mobile device security. Technical report, Symantec, 2011.

[31] Niina Mallat, Matti Rossi, Virpi Kristiina Tuunainen. Mobile banking services. In *Communications of the ACM - New architectures for financial services, Vol. 47, No. 5*, pages 42–46, May 2004.

[32] Saurabh Panjwani. Towards end-to-end security in branchless banking. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, pages 28–33, March 2011.

[33] Germán Retamosa and Jorge E. López de Vergara. Assessment of mobile security platforms. In Eduardo Fernández-Medina, Manu Malek, Javier Hernando [14], pages 127–132.

[34] Ron Shevlin, Gwenn Bezard, Judith Fishman. The impact of mobile banking: A case for mobile marketing. Impact note, Aite Group LLC., April 2011.

[35] Safaricom. M-pesa customer and agent numbers. http://www.safaricom.co.ke/images/Downloads/Personal/M-PESA/m-pesa_statistics_-_2.pdf, 2012.

[36] Shang Gao, Zhihao Chen, Wenying Zheng, Wenyan Zhou. An exploratory study on lifestyles and the adoption of mobile services in china. In *MoMM '12 Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, pages 249–252, December 2012.

[37] SWIFT. Mobile payments. Technical report, SWIFT, 2010.

[38] Symantec. Symantec mobile security. http://www.symantec.com/en/uk/mobile-security, 2013.

[39] Tim Matthews Symantec. Don't be afraid of mobile banking apps. http://www.banktech.com/channels/dont-be-afraid-of-mobile-banking-apps/240006734, 2012.

[40] Blake Wiedman. Mobile security threats and prevention. http://www.governmentsecurity.org/articles/mobile-security-threats.html, 2009.

[41] R. Kainda With C. Bangdao, A.W. Roscoe. The missing link: Human interactive security protocols in mobile payment. *Proceedings of the 5th International Workshop on Security, IWSEC*, 2010.

[42] Zheng Yan, Valtteri Niemi, Yan Dong, Guoliang Yu. A user behavior based trust model for mobile applications. In *ATC '08: Proceedings of the 5th international conference on Autonomic and Trusted Computing*, pages 455–469, Berlin, Heidelberg, 2008. Springer-Verlag.