Strathprints Institutional Repository

Perceived Risk and Sensitive Data on Mobile Devices[1]

Apollonia Lazou and George R S Weir[2]

Department of Computer and Information Sciences, University of Strathclyde, Glasgow G1 1XH, UK
[1]george.weir@cis.strath.ac.uk

Abstract. This paper reports on a survey to investigate the behaviour and assumptions of smartphone users, with reference to the security practices adopted by such users. The primary objective was to shed light on the level of information security awareness in smartphone users and determine the extent of sensitive information such users typically hold on these mobile devices.

Keywords: Mobile devices, smartphones, data security, perceived risk.

1 Introduction

The advent of mobile technologies in the form of smart phones, personal organisers and other portable computing devices allows for the greater integration of such technologies across a wide range of activities - work, recreation, social interaction and personal pursuits. Individuals who choose to incorporate technology into their daily activities may enjoy many benefits. Gartner predicted that smart phones would be favoured by mobile workers [1] and, since the turn of the century, we have seen an explosive growth in the mobile media market of smart phones, personal digital assistants (PDAs) and other similar integrated devices [2].

Today's professionals commonly use their mobiles for a variety of personal information management activities such as organising contacts, creating and maintaining schedules, corporate calls, mobile banking, on-line purchases, web surfing and e-mail access. In addition, smart phones offer a wide range of functionalities and applications, including word processors and spreadsheets. With its many benefits, such technology also presents many challenges, particularly the growing demand for data and information security and the need to assure that data is protected against criminal misuse. An increasing amount of information is being stored on mobile devices, with the alarming suggestion that over 80% of new and critical data is stored in this context [3].

The risks with portable data storage and manipulation are considerable. Identity fraud, estimated to cost the UK economy more than £1 billion each year, is on the rise

[1] Reprinted from Cyberforensics: Issue and Perspectives. Edited by G. R. S. Weir. Glasgow, UK. University of Strathclyde Publishing. 2011.
[2] Corresponding author.

[4]. According to Schreft [5], in 2006 the time and costs incurred in order to resolve issues in identity theft may have cost the US economy as much as $61 billion. With millions of people becoming victims of fraud each year, identity theft has become the fastest growing crime in the US and UK. To make matters worse, mobile devices are by nature more vulnerable to theft and accidental loss than larger systems in fixed locations. In 2001, the UK Home Office reported the theft of over 700,000 handsets [6] and security experts regularly predict and warn of future attacks against mobile devices. In this context, we performed a brief survey of surveys to gain a perspective on smartphone users. The resultant insight then fed as a basis for comparison into our own user survey.

2 Related Work

An earlier survey that questioned commuters in London revealed that 4.2m Britons store data on their mobile phones that can be used for identity theft in the event that their phones were stolen [7]. According to security firm Credant, who conducted the survey, only six in ten smartphone users employ a password to control access to their phones. This survey also found that 99% of people use their phones for business in some way, despite 26% of them being told not to. The increased usage of smartphones has seen an associated growth in the types of information that pass through handsets, and it is now common for individuals to store sensitive information and work-related details on their portable devices. The Credant survey also found that more than a third of respondents frequently used their phones for sending and receiving business related e-mails, with more than three-quarters using their handsets to store business contact details. More worryingly, nearly a quarter of respondents stored customers' information as well. Not surprisingly, Credant warn that lost or stolen smartphones may lead to theft of personal information, sufficient to carry out identity fraud.

Indications of the types of information stored on mobile phones are shown in Table 1, below. The storage of personal information is on the rise, with 16% of people storing their bank details and nearly 25% storing PIN numbers and passwords.

Table 1: Sensitive Data Stored On Mobile Phones

Personal	**Business**
16% - Bank account details	77% - Work-related names/addresses
24% - Pin numbers/passwords	23% - Customers' information
11% - Social security/tax details	30% - Use mobile as a work diary
10% - Store credit card information	17% - Work-related documents

Source: Credant Technologies

In 2006, a survey by mobile security firm Pointsec questioned 248 IT professionals at Infosecurity [8] and exposed major security issues:

- Only 20% of removable devices in the workplace were secured with passwords or encryption;

- On average 56% of employees were using their memory sticks to download corporate information and this has increased by 25% in relation to the previous year;
- 65% of survey respondents were aware of the potential dangers associated with removable media and storage devices;
- The majority of employees used their memory sticks to store corporate data, such as contracts, proposals and other business documents, including customer information. 22% of these would even store customer's names, addresses, presentations, budgets and many other documents;

Perhaps reflecting the associated risks, this survey also found that 12% of organisations ban the use of media storage devices in the workplace.

In 2009 Sophos conducted a survey to reveal whether smartphone users encrypted the data stored on their phones [9]. Astonishingly, only 26% of these users answered yes. 50% did not use any protection methods with a further 24% being unsure. Research carried out by Vodaphone UK found that 50% of Britons do not regularly update their passwords on mobile devices [10]. This study also found that nearly two thirds of UK workers store sensitive information on their PDA's and smartphones, accepting that theft of their devices would give potential fraudsters access to this data. A recent YouGov survey [11] found that 9 out of 10 smartphone users in Britain did not secure their devices against crime and identity theft. Furthermore, over half of the respondents had submitted credit card details via their smartphones during purchase transactions and on-line downloads.

3 Our survey

The objectives of our survey were:

- To assess how much sensitive information is stored on mobile devices and determine whether this data could be used to commit fraud;
- To uncover the security practices of smartphone users;
- To determine the level of security awareness in smartphone users;
- To reveal any correlations that may arise between age, gender, education, smartphone variety, occupation and level of awareness.

Toward these objectives, we analysed four main perspectives: (i) security practices and concerns; (ii) information stored on mobile devices; (iii) on-line activities and associated threats; (iv) user awareness. The instrument for this was an on-line with respondents drawn from a wide range of backgrounds. Our sampling scheme was designed to secure a random sample of adults aged 18 or older, who own and use smartphones. The data was gathered from a total of 79 completed questionnaires.

3.1 Sampling Frame

The sampling frame consisted primarily of users from relevant on-line computer discussion groups, e.g., related to mobile forensics. This selection allowed us to achieve sufficient responses, from diverse user backgrounds. The choice of subject-specific forums ensured that the questionnaires were circulated quickly across a diverse user population. Furthermore, the individuals in such forums were thought likely to be owners of smartphones and have a working knowledge of mobile devices, current models and their functionalities. The purpose of the research was explained to potential participants. The strata were constructed such that the resulting sample would represent a broad range of ages, occupational and educational backgrounds. For example, the breakdown by age group is shown in Table 2, below.

Table 2. Survey Age Groups

Age	Survey Records
18-25	46
26-35	21
36-65	12
>61 years	0

3.2 Questionnaire Design

Participants were asked to complete a structured questionnaire of 30 multiple choice questions. The survey was kept simple, short in length and could be completed in around 5 minutes. Some questions were obligatory and respondents could choose to skip other questions, dependent upon previous answers. To ensure that all aspects of the survey instrument worked as expected, pilot testing was performed prior to making the on-line survey available.

3.3 Data Collection

The use of an on-line questionnaire eliminated interviewer effects and variability, significantly reducing non-random interviewer error. The questionnaire was programmed to restrict respondents from submitting a response, unless all required fields had been completed. Requests for participants were sent to three on-line forums, including university and workplace-related networks. The on-line survey link was continuously available for a period of twelve days.

To be eligible to participate in the study respondents had to be age 18 or older and be the owner of a mobile storage device or smartphone. We were mainly interested the following types of device: iPhone, Symbian, Android, Blackberry and PDA. These were considered the most popular mobile storage devices available on the market at the time of our survey.

3.4 Final Sample Dispositions and Response Rates

The table below shows the final dispositions generated by the survey. In total, there were 93 responses to the questionnaire, some of these selectively omitted. 15.18% of the survey results were not suitable to the research analysis. More specifically, the survey produced 7.2% of all responses to be incomplete and 5.37% to belong to the Non-Eligibility category. A non-eligible response is a complete survey where the participant has entered a non-smartphone mobile device in response to Question 5 of the questionnaire, thus the surveys are discarded. It also represents any surveys found to have inconsistencies. For instance, in some surveys the respondent has answered 'No' to Question 7 'Do you use a password on your mobile device' and then still completed the following questions 8, 9, 10 and 11 which are related to set passwords on the mobile devices. Any inconsistencies were discarded from the final results. Incomplete responses are those where participants answered some or most questions but did not complete the survey.

Table 3. Survey Responses

Total Number of Responses	93
Number of Completed Surveys	79
Incomplete Surveys	7
Non-Eligible Responses	5

4 Results

The age profile of our survey participants was: 58.22% in the age group 18-25; 26.58% in the age group 26-35; 15.18% in the age group 36-65; and 00.00% in the age group >61 years. Of these participants, 64.29% were male and 35.71% were female. The main occupational fields represented were Admin/Secretarial/PA, Education, Engineering/Technical, IT/Telecommunications and Sales (see Table 4).

The majority of participants were employed in the IT and Telecommunications sector. Most of the sample set (57.14%) had education to post-graduate degree level. The next largest group (35.71%) had education to the level of undergraduate degree and the remaining group (7.14%) was in higher education.

Table 4. Occupation Fields Analysis

Occupational Field	**% Survey Records**
Admin/Secretarial/PA	2.27
Education	16.84
Engineering/Technical	9.58
IT/Telecommunications	67.29
Sales	1.12

The majority of survey respondents own an iPhone (Table 5) with the second most popular mobile device being the Android. All survey respondents answered 'No' to

Question 6 of the questionnaire and thus, none of the participants have ever been victims to identity theft.

Table 5. Device Ownership Analysis

Mobile Device	Survey Records	% of Survey Records
iPhone	53	67
Symbian	2	2.5
Android	11	14
Blackberry	6	8
PDA	2	2.5
Other	5	6
Total	79	100

4.1 Security Concerns

The survey found that at 53%, more than half of mobile device users do not use passwords to protect their devices. This finding is very similar to the research carried out by Sophos, who found that 50% of mobile device users do not protect their devices with passwords. However, this particular research aims to offer additional insight into user security implementations and is highlighting further limitations that were found in the remaining 47% who did use passwords. The survey reveals that 100% out of the users who set passwords do not use both capitals and small letters in their passwords, and, furthermore, only 19% of users mix characters and numbers together. This raises many security concerns, as strength of password is vitally important in the efficient protection of sensitive data and important information. In addition, only 27% of users regularly update their passwords, again, leaving them vulnerable to security attackers. On the positive side, the survey found that 0% of users used personal information as part of their password, i.e. date of birth, place of birth, address, phone number, mother's maiden name, pet name etc) which is considered to be a general good security practice.

In addition to these findings, the study identified a worrying 78.57% of survey respondents who do not use data encryption on sensitive and important information stored on their mobile device. Particularly when considering identity theft, this is one of the biggest security risks and could easily be prevented by simple encryption methods. In addition, 16.24% of users do not regularly install system updates and upgrades leaving them very vulnerable to system attacks and many more threats. Amongst these risks, 7.14% of survey respondents willingly click on links sent in SMS or MMS messages, originating from unknown senders. Be it through a different infection route to, i.e. e-mail attachments, SMS and MMS messages remain a hugely popular way of spreading malicious code onto mobile devices and better care should be taken to avoid opening any links or attachments sent from unknown senders. At the very least, system updates and upgrades should not be ignored because they offer enhanced and up to date security.

Lastly, when asked whether or not they had ever had a virus on their mobile device, all 79 respondents answered no. On one hand, this would imply that the threats for some of the mobile device securities mentioned in this research are still very minor and do not have a great impact on users. On the other hand there is very little way to know how accurate these results are. For example, some of the respondents may have a virus on their mobile device and be completely unaware of it. Although some ways to identify infections are mentioned as part of this study, the fact that 87.71% of survey respondents do not use anti-virus software could mean that even if a virus was present on the device, it might go undetected until a virus scan is performed. Furthermore, malicious code is often designed to be well disguised and some Trojans or infections only show up during the virus scan.

Overall, many survey respondents had a poor level of awareness relating to mobile security as well as bad security practices. For this reason, many of the participants would be at great risk of some security breach, and through the many available infection routes, the mobile device does not need to be lost or stolen for this damage to occur. The final question of the survey is thus inconclusive, due to the fact the evidence appears to be quite contradictory because the majority of respondents do not have anti-virus software installed on their mobile devices, which could result in a malicious piece of code going undetected or unnoticed. In addition, the overall level of awareness is so low that even common indicators of a virus infection, e.g., skulls appearing on the mobile device screen, may pass unnoticed. However, if in fact all 87.71% of respondents have indeed never had a virus this would raise doubt on the reality of threats in the mobile world.

Key points from our survey are summarised below:

- 53% of survey respondents do not use passwords on their mobile device

From the remaining 47% who use passwords:

- 0% of survey respondents use capital and small letters
- 81% of survey respondents do mix characters and numbers together in their passwords
- 73% of survey respondents do not regularly update their passwords
- 87.71% of survey respondents do not use anti-virus software on the mobile device
- 78.57% of survey respondents do not use data encryption on sensitive and important information stored on their mobile device
- 16.24% of users do not regularly install system updates and upgrades onto their mobile device
- 7.14% of survey respondents click on links sent in SMS or MMS messages from unknown senders

4.2 Information Stored on Mobile Devices

Our survey indicated that a wide range of sensitive personal and business information is regularly stored on respondent's mobile devices. Respondents confirmed storing the following details:

- PIN numbers
- Passwords
- Bank Account Details
- CreditCard Information
- Home Address
- Home Telephone Number
- Work Related Documents
- Work Related Names and Addresses
- Customer Information
- Work Diaries

None of the respondents stored Social Security or Tax details on their mobile devices. This may reflect the low frequency with which such information would be retrieved. In contrast, the percentages of respondents who store 'frequent use' personal and business information are listed in Table 6 (below).

Table 6. Sensitive Data Stored On Mobile Phones

Personal	**Business**
29.27% - PIN numbers	3.78% - Work Related Documents
29.27% - Passwords	11.14% - Work Related Names & Addresses
9.32% - Bank Account Details	2.44% - Customer Information
2.44% - Credit Card Information	9.76% - Work Diary
9.76% - Home Address	
42.63 - Home Telephone Number	

Our findings show that mobile storage devices often contain highly sensitive information, both personal and business related. Nearly 30% of respondents store PIN numbers and passwords on their device and 9.32% store Bank Account Details. A smaller proportion, 2.44%, stores Credit Card Information also. It is important to note that while some of the information mentioned above may not be of much use to someone on its own, however, if used in combination with other information stored on the phone, it can be used for identity theft. Even if no sensitive data was stored on the device, the survey reveals that nearly half of respondents store their home telephone number, which alone increases their chances of identity fraud. If a fraudster has information on the person's workplace, or corresponding bank, they could use the home phone number and pretend to be calling from one of these organisations, in the hope of deceiving their victim to reveal further sensitive information.

4.3 Mobile Devices and On-line Activity Threats

The findings of the survey reveal that 7.14% of respondents manage their finances by mobile device. At 92.86%, the majority of participants, do not manage their finances by mobile, however, as internet usage through these devices increases, this number is

set to become larger. Many respondents, specifically 82.57%, access the internet from their mobile device.

When asked whether or not the internet browser used on their mobile device stored passwords, only 17.27% of respondents answered no. With 64.55% of respondent's internet browsers saving passwords, and, alarmingly, 18.18% not knowing, serious security concerns are raised. If a fraudster does get hold of a device and can access stored passwords, this would grant access to many services the user has previously used. For example, if on-line banking or any on-line purchase has been made, the fraudster may have access to bank account details. Furthermore, many people use the same password for different services. This in turn may grant access to other areas of the individual's life, greatly increasing the likelihood of identity theft or identity fraud. To make matters worse, when asked whether or not cookies, cache files and browsing history were regularly deleted an alarming 82.73% of survey respondents answered No, while 17.27% of survey respondents answered Yes.

Cache files can make websites available offline and often hold all of the information that was present when saved. They also save passwords, user names and account numbers which a user may have input whilst using an internet banking site. In addition, cache files take up lots of space. Cookies and browsing history serve a similar purpose. Undoubtedly, this is a significant security risk, particularly if the mobile device were to fall into the wrong hands. To demonstrate this exposure, survey, participants were asked which of the following applications were used from their mobile device:

- Facebook
- PayPal
- On-line Banking
- E-mail

These are all applications that can be easily accessed if a browser has stored the passwords.

According to the survey, Facebook at 59% of respondents, and E-mail at 64% of respondents, are the most widely used applications by mobile device users. If fraudsters had access to e-mail they could very easily gain access to other important information. For example, many e-mails are in the form of confirmation for on-line purchase transactions and contain sensitive banking details, including postal addresses. Furthermore, many e-mails are electronic confirmations of user names and passwords for various web-sites and this information would help enable identity theft and identity fraud.

Facebook has often been associated with security liabilities involving user information. In this study we found that:

- 50.77% of respondents display their date of birth on Facebook
- 43.62% of respondents display their location on Facebook
- 19.38% of respondents display information on their place of work on Facebook
- 7.69% of respondents display their home address on Facebook

- 15.82% of respondents display their telephone number on Facebook

All of the above information is relevant and useful for identity theft and subsequent identity fraud. More than half of participants display their Date of Birth on Facebook, which is often found as a security question for banks or other organisations. In combination with other information that can be retrieved through on-line stored passwords and pages, including Location, Place of Work, Home Address and Telephone Number that is available on some Facebook pages, as demonstrated through this study, all this information creates huge opportunities for fraudsters. Although PayPal and On-line Banking were found to be used a lot less than Facebook and E-mail, these applications still present huge risks. Both contain highly sensitive information on banking account details and can easily be used to enable fraud.

Other findings of the study relating to security risks reveal that:

- 38.36% of survey respondents download third-party applications from unverified sources
- 19.18% of respondents bypass system security warnings that advise on potential risks associated with software downloads or the visiting of un-trusted websites
- 18.82% of survey respondents click on links or download e-mail attachments from unknown senders

The risks associated with the downloading of unverified third-party applications or e-mail attachments are significant, particularly since the user is authorising code or application to run on their mobile device. Although the numbers are relatively low, there is still a considerable number of users, the large majority of these of university level education, putting themselves at risk in this fashion. This shows that many people are aware that their activity may pose security risks but choose to engage in these either way.

The survey found that at 56%, more than half of the respondents use their mobile devices to connect to Open Access Points. This study is particularly concerned with highlighting the security risks posed by internet access through public areas, which were discussed in previous chapters. Thus, there was a strong interest to explore the level of precautionary protection measures taken by open access point users. Alarmingly, the results of the survey indicate that users have a very poor level of awareness in this specific area and that the majority of people do not protect themselves adequately, leaving them vulnerable to all sorts of malicious attacks. The results found that:

- 86.92% of survey respondents do not use encryption to encode traffic
- 59.14% of survey respondents do not disable Bluetooth and device discovery features when not in use

In combination with other bad practices, such as accepting downloads from unknown senders and many more, open access points can spread harmful code and applications

to devices, or have sensitive information stolen or accessed, posing serious threats for identity theft.

4.4 User Awareness

User awareness is very poor amongst the questionnaire participants. The survey found that respondents are particularly unfamiliar with Vishing and Pharming. However, even when users were asked if they understood Phishing and Social Engineering, less than half answered no. The following associated data was gathered:

- 41.94% of survey respondents understand and are familiar with Phishing
- Only 6.45% of survey respondents understand and are familiar with Vishing
- Only 12.90% of survey respondents understand and familiar with Pharming
- 38.71% of survey respondents understand and familiar with Social Engineering

It is evident that stronger emphasis needs to be placed on user awareness, in particular the types of attacks that exist in the mobile world and all security risks involved. If awareness is raised, users will be in a position to make better choices to protect their devices, personal information and themselves against identity theft and other fraudulent activities.

Lastly, the survey found that the majority of respondents do not have anti-virus software installed onto their mobile device.

- 87.71% of survey respondents do not have anti-virus software installed on their mobile device
- A very small 5.14% of survey respondents do have anti-virus software installed on their mobile device
- 7.14% of survey respondents do not know whether or not their mobile device had anti-virus software installed

These findings, again, indicate some lack of user awareness. The fact that a proportion of users do not know whether or not their mobile device has anti-virus software is a serious concern. Furthermore, the large majority of users are leaving their mobile devices susceptible to many sorts of security risks by not using anti-virus software. Mobile devices nowadays are more along the lines of mini computers and need to be treated and protected accordingly.

5 Recommendations

The risks associated with the storage of personal information lead us to recommend that users take advantage of the security features available on their mobile devices. This includes enabling protection through setting ‘strong’ passwords or pass-phrases. Many people use simple dictionary words for passwords or a word that is easy to

guess if somebody knows you, i.e. mother's maiden name, place of birth, pet's name and so on. If the phone provides the option, then data encryption should be used. At the very least, this will prevent people from making calls, if a phone has been lost or stolen. Furthermore, banks report a massive growth in "phishing" sites, fake websites that are designed to look exactly like the official site, in order to re-direct unsuspecting victims to fraudulent websites. One recommendation is to avoid following links contained within e-mails and instead to visit official websites directly.

5.1 Credit file

There is a clear need for each individual to be proactive when it comes to the risk of identity fraud and there are many actions that can be taken to help protect each person's identity. Firstly, individuals may regularly monitor their personal credit file to check for unauthorised changes, particularly in the event where a person has lost documents or a personal storage device (e.g., in a burglary). This can prevent the credit record from being negatively affected if fraudulent activities take place, through timely disclaiming of responsibility. Insurance is another option which can assist in monitoring and resolution of liabilities relating to the credit record.

Often, being declined for credit is the first indication that a person may have fallen victim to identity fraud. In this case, the credit file has already been damaged and there is serious work to be done in order to regain credibility. The first step is to try to discover the extent of the problem. This is possible by requesting a copy of the credit file from a UK credit reference agency such as Experian, Equifax or Call Credit. A statutory report can be examined in order to check for new account openings, changes of address and so on.

If any suspicious activity is noticed then the company involved in the transaction should be contacted straight away, notifying them that identity theft has taken place. It is important to note that while debt can be written off, the victim still needs to ensure that their credit file is restored to the position prior to when the fraud occurred. This means making sure the company agrees to contact the relevant credit reference agency to make them aware of the situation and requesting that this agreement is confirmed in writing. Usually, this can be a lengthy and time consuming process and in some extreme cases, legal advice may be required to erase personal liability. The real hassle begins when a victim realises multiple new accounts have been opened, which is very often the case.

If more than one company is involved, each of them needs to be contacted individually and the same lengthy process repeated in each case. In some cases this includes communication with banks or mobile phone companies used by the identity thieves, with which the victim has no prior relationship.

Aside from taking up enormous time and effort to resolve identity theft, the impact on the affected individual can be financially and emotionally draining. Finally, in order to ensure identity theft does not reoccur, the credit file needs to be checked on a regular basis and for additional assurance a protective registration can be filed with CIFAS, protecting the victim from future fraud.

5.2 Reducing Risks

The most important preventative measure to protect and stop data loss is to use encryption on sensitive information stored on laptops and other removable storage devices. Data is encrypted with a password and unless the password is known, the data cannot be deciphered or used. Data encryption should ideally be used in combination with other security measures. In the case that all other protective steps have failed, encryption will ensure that even if a hacker manages to gain access to sensitive data, the format would be un-readable. Thus, they would be unable to use the information or compromise its confidentiality. Another very important measure is to discourage 'risky' activities, such as the transfer of unencrypted data through electronic mail or onto USB sticks and other storage devices.

In order to reduce potential risk regular screening is essential. High quality and reliable anti-virus internet website technology is required to detect malware contained in websites that have been hacked, but also to perform regular scans in order to effectively and rapidly respond to newly emerging malicious domains and URL's. Aside from this, users should ensure that basic security and proxy settings are in place and up to date. Common sense is also required. Users should generally avoid trying to gain access to suspicious looking links, especially if this involves overriding a security filter or warning. Suspicious and malicious websites often include sites that host inappropriate content and caution should be practiced when redirected to other sites or when bombarded with pop-up windows.

There are many steps that can be taken to mitigate risks involved in attacks, with particular emphasis on user education. By their behaviour, users appear largely unconcerned or unmotivated by security risks with mobile devices. There is evidently a need to be aware of risks and gain an understanding of new threats and new forms of attacks. Furthermore, some understanding of the threats of fraud may ensure that individuals take appropriate measures to protect themselves, their personal information and their mobile devices.

References

1. Jones N., Smartphones to be favored as thin clients by mobile workers. Gartner Research Report G00127690, 27 May, 2005.
2. Cozza R, Mitsuyama N, De La Vergne HJ, Liang A, Nguyen TH, Market trends: smartphones, worldwide, 2006. Gartner Research Report G00143276, 12 September, 2006.
3. Allen M., A day in the life of mobile data. Mobile Security, British Computer Society. Available from: http://www.bcs.org/content/conWebDoc/2774 [Accessed 11 June 2011].
4. CIFAS, The anonymous attacker. A special report on identity fraud and account takeover, October 2009.
5. Schreft, S.L., Risks of identity theft: can the market protect the payment system, Federal Reserve Bank of Kansas City Economic Review (Fourth Quarter), pp. 5–40, 2007.
6. Harrington V, Mayhew P., Home office research study 235: mobile phone theft. Crown Copyright, 2001.
7. Kahn Charles M., Roberds William, Credit and identity theft, Journal of Monetary Economics 55 (2008) pp. 251-264, 2008.

8. Watson I., Securing portable storage devices, Information Security Forum, Network Security, p.11, July 2006.
9. Sophos security report 2010. Available from: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf [Accessed 11 June 2011].
10. Mobile phone security. Available from: http://www.prudentminds.com/mobile-phone-security.html [Accessed 11 June 2011].
11. Beware the blabbermouth smartphones, Sunday Times, News Review, June 2010.