Behaviour & Information Technology, 2014
Vol. 33, No. 12, 1347–1360, http://dx.doi.org/10.1080/0144929X.2014.934286

Taylor & Francis
Taylor & Francis Group

Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users

James Imgraben, Alewyn Engelbrecht and Kim-Kwang Raymond Choo*

Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Mawson Lakes Campus, SA 5095, Australia

(*Received 17 August 2012; accepted 9 June 2014*)

Smart mobile devices are a potential attack vector for cyber criminal activities. Two hundred and fifty smart mobile device owners from the University of South Australia were surveyed. Not surprisingly, it was found that smart mobile device users in the survey generally underestimated the value that their collective identities have to criminals and how these can be sold. For example, participants who reported jail-breaking/rooting their devices were also more likely to exhibit risky behaviour (e.g. downloading and installing applications from unknown providers), and the participants generally had no idea of the value of their collective identities to criminals which can be sold to the highest bidder. In general, the participants did not understand the risks and may not have perceived cyber crime to be a real threat. Findings from the survey and the escalating complexities of the end-user mobile and online environment underscore the need for regular ongoing training programs for basic online security and the promotion of a culture of security among smart mobile device users. For example, targeted education and awareness programmes could be developed to inform or educate smart mobile device users and correct misconceptions or myths in order to bring about changes in attitudes and usage behaviour (e.g. not taking preventative measures such as strong passwords to protect their devices). Such initiatives would enable all end users (including senior University management who use such devices to access privileged corporate data and accounts) to maintain current knowledge of the latest cyber crime activities and the best cyber security protection measures available.

Keywords: cyber crime; smart mobile devices; security survey; mobile security; phishing; malware; unauthorised access

1. Introduction

Just as information and communications technologies (ICT) have provided new opportunities for governments and businesses to operate and expand their presence and reach, ICT also presents opportunities for those with criminal intentions (Choo 2011a; US GAO 2012). Although industry sectors such as the banking and financial industry tend to be the target of choice for cyber criminals and organised crime groups, vulnerabilities in any particular environment and technology, such as smart mobile devices (e.g. iPads and iPhones), could potentially be exploited by criminals (Choo 2011b; Martini and Choo 2013; Quick and Choo 2013c).

The widespread adoption of ubiquitous smart mobile devices and their capacity to act as a general purpose computing platform make them ideal candidates for mobile commerce (m-commerce) particularly mobile money transfer services (e.g. mobile banking, mobile payments and mobile remittance) (Choo 2013). With the increasing popularity of smart mobile devices, it is likely that cyber criminals such as malware authors will start targeting such devices, and the number of malware targeting mobile devices is increasing (McAfee 2013).

Information such as login credentials and account information (as well as other sensitive or private data stored on these devices) are the target of mobile malware attacks – similar to attacks targeting our computers and laptops. For example, a report by Symantec explained that:

> [w]ith the number of vulnerabilities in the mobile space rising (a 93.3% increase over 2010) and malware authors not only reinventing existing malware for mobile devices but creating mobile specific malware geared to the unique opportunities that mobile devices present. 2011 was the first year that mobile malware presented a tangible threat to enterprises and consumers. (Symantec 2012, 14)

F-Secure also reported an increasing number of malware targeting popular smart mobile devices, particularly Android devices, and more worrying is the trend in more sophisticated malware – '[i]n Q1 2012, malware authors are focusing on improving their malware's techniques in evading detection, as well as exploring new infection methods' (F-Secure 2012, 5).

*Corresponding author. Emails: raymond.choo@unisa.edu.au; raymond.choo@fulbrightmail.org

A study of 1260 Android malware application samples by Zhou and Jiang also found that such malware 'are rapidly evolving and existing anti-malware solutions are seriously lagging behind' (Zhou and Jiang 2012, 96). The risk is not just to the owner of the smart mobile devices, but also to the organisations they work for and to other organisations connected to the Internet. In the latter scenario, for example, smart mobile devices can be used to launch DDoS attacks against governments and corporate networks. The ease with which erased data on such (stolen/misplaced) devices can be recovered using forensic software, such as Micro Systemation XRY (http://www.msab.com/) and CelleBrite UFED Kit (http://www.cellebrite.com/mobile-forensic-products.html), also increases their attractiveness to criminals (Martini and Choo 2013; Quick and Choo 2013a, 2013b, 2013c; Tassone et al. 2013).

1.1. Our contributions

Although it would be pleasing to be able to cite comprehensive statistics on patterns and trends in malicious cyber activities particularly incidents involving smart mobile devices, this remains an elusive goal as such activities are generally unreported and undetected. As far as we are aware, no similar academic survey of smart mobile device users has been undertaken, particularly in Australia and in a higher educational institution setting. As noted by Hooper, Martini, and Choo (2013), the vast majority of reports on patterns and trends in smart mobile devices (and malicious cyber activities) disseminated (and in turn cited) are generally from the commercial sector and may not include details such as the research methodology or provide access to the raw data. The 'diversity of methods used to collect information on cyber incidents can produce widely different results . . . [and] this facilitates extrapolations about the scale of the problem and the cost of cyber crimes' (Guinchard 2011, 78).

This paper seeks to contribute to a better understanding of this ever-evolving threat landscape by providing a snapshot of the:

(1) prevalence and types of smart mobile device usage by academic staff members and students at the University of South Australia (UniSA)
(2) prevalence, nature, costs and impacts of smart mobile device-related incidents
(3) the type(s) of user awareness and education/training needed.

While the survey responses were small in number, by comparison to the number of smart mobile devices as a whole in Australia (and worldwide), the survey provides a good indication of the risks associated with smart mobile device usage.

Technical solutions can provide effective protection against security threats, but alone cannot provide a comprehensive solution (Choo 2014). Cyber criminal activities such as phishing will continue to evolve into new forms, while continuing to exploit human factors (e.g. social engineering) and human factors are likely to remain one of the weakest links in attempts to secure systems and networks. As individual ICT end users, we need to be even more vigilant online and if we do not undertake measures to protect ourselves online, we would be easy targets for the less sophisticated cyber criminals – the lowest hanging fruit.

We understand the importance of user awareness and education/training in mitigating cyber threats such as phishing. Therefore in our survey, appropriate educational materials were suggested to participants, based on their responses in the survey, with the aim of facilitating the making of informed decisions regarding their smart mobile device security practices in the future (see Figure 12 in Section 4). Several participants who responded to the survey in person indicated that the post-survey feedback, particularly on the phishing examples, was educational and helped them understand and learn how they could improve their security practices. These educational materials were sourced from authoritative and reliable websites including the Australian Government SCAMwatch website (http://www.scamwatch.gov.au/), Australian Government Stay Smart Online website (http://www.staysmartonline.gov.au/), and corporations upon which the phishing emails are usually based (e.g. eBay security centre and PayPal fightphishing websites).

In addition, if the participant indicates that he/she has lost a device, say in Sydney, in the last financial year, but did not report the loss, the survey website would recommend the individual reports the incident to his/her financial institution and NSW Police Fraud and Cybercrime Squad. Links to SCAMwatch's 'Banking and online account scams' page were also provided to the participant. By encouraging participants to report incidents to law enforcement and other competent agencies (e.g. the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority), this research has the potential to increase mobile security incident reporting rates.

1.2. Outline

The rest of this paper is organised as follows. We document the survey design in Section 2. Section 3 presents the results of the survey, and the last section concludes the paper and looks at future work to take forward this paper/survey's analysis and conclusions.

2. Survey

2.1. Survey design

The survey comprised five main sections, each representing one of the main threats that users of mobile devices are generally exposed to: (1) general security (Loss/Theft), (2)

malware, (3) unauthorised access, (4) Wi-Fi and Bluetooth Security and (5) phishing. The questions relate to the 2010–2011 financial year (1 July 2010 to 30 June 2011) unless otherwise specified.

Participants were recruited for the survey through the UniSA (undergraduate students, postgraduate students and academic staff members). In order to ensure an even distribution of participant's technical backgrounds, participants from a number of different schools within the University were approached including Computer and Information Science (Mawson Lakes and City West campuses), Mathematics (Mawson Lakes and City West campuses), Education (City West and Magill campuses), and Business, Law and Health Sciences (City West and City East campuses).

Surveys were distributed to participants both in person (i.e. paper surveys distributed to students at Mawson Lakes campus, City West campus, City East campus, and Magill campus) and through an online survey hosted by the University. All information was gathered anonymously. However, to ensure that all participants were able to obtain feedback on their responses (educational materials), paper survey participants were provided a unique participant ID. The unique participant ID could be used by the respective participant to access the feedback page from the Survey website at a later stage – see Figure 12 in Section 4, but it will not be possible to associate participants with their survey responses.

2.2. Participants

2.2.1. Demographics

A total of 250 responses were received. The majority of participants were students and aged 35 and below – see Table 1, which is perhaps explained by the independent, yet related, 2011 Australian Communications and Media Authority-commissioned consumer survey, which states that the 'ownership of 3G-capable phones and smartphones [in Australia] declines with age' (ACMA 2012, 6). As participants were able to select one or more smart devices, the number of devices exceeds the number of participants as shown in Figure 1. All percentages in this paper have been rounded to one decimal place.

Table 1. Demographics for the participants of the survey.

Age	Total (250)
18 and younger	37 (14.8%)
19–25	95 (38.0%)
26–35	59 (23.6%)
36–50	38 (15.2%)
51+	21 (8.4%)
Gender	**Total (250)**
Male	138 (55.2%)
Female	112 (44.8%)
Education	**Total**
Undergraduate	126 (50.4%)
Postgraduate	54 (21.6%)
UniSA academic staff members	70 (28.0%)

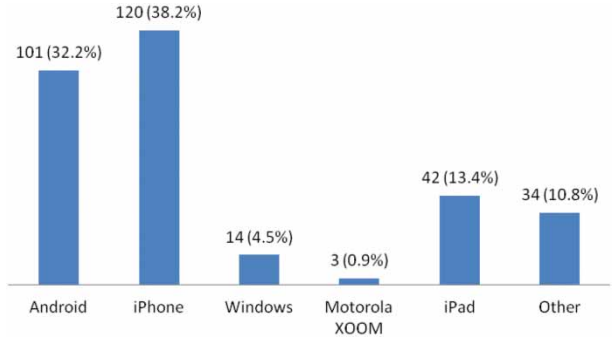

Figure 1. Types of smart mobile devices.

2.2.2. User behaviour

Of the two most popular smart mobile devices owned by the participants – see Figure 1, iPhones (and iPads) are generally known to be a 'more secure and manageable [device] in the consumer mobile segment' due to Apple's strictly regulated ecosystem while Android devices were found to be 'widely exposed to malware and data loss' (Ohaya 2006). For example, a report by McAfee found that in the first quarter of the 2012 calendar year, there was 'a large increase in mobile malware. The jump was targeted almost solely at the Android platform . . . Android threats now reach almost 7,000, with more than 8,000 total mobile malware in our database' (McAfee 2012, 4).

In total, 33.2% of the participants reportedly used their smart devices for 1 to 2 hours a day and the second largest group, with 21.2%, was using their devices for more than 4 hours a day. Undergraduate students (58.7%) made up the majority of those using their devices for more than 4 hours a day, followed by postgraduate students (24.1%) and staff (17.2%). Of those that used their phone for more than 4 hours, iPhones were the preferred devices (54%), followed by iPads (24.4%) and finally Android devices (21.6%). When looking at the participants that use their phones less (less than 1 hour a day), Android devices are preferred (44.7%) over iPhones (28.9%) and iPads (13.1%).

The most common usage types for a smart device listed by participants are shown in Figure 2. Phone calls, SMS and Internet access top the list. Participants were also using their devices to access sensitive personal information such as credit card details to purchase applications (or apps, as they are commonly known) and music, perform mobile banking and use their device as an e-wallet. Social networking is also another popular use of smart devices, with 68.8% of participants indicating that they used some form of social networking (Twitter, Facebook and LinkedIn) on their devices.

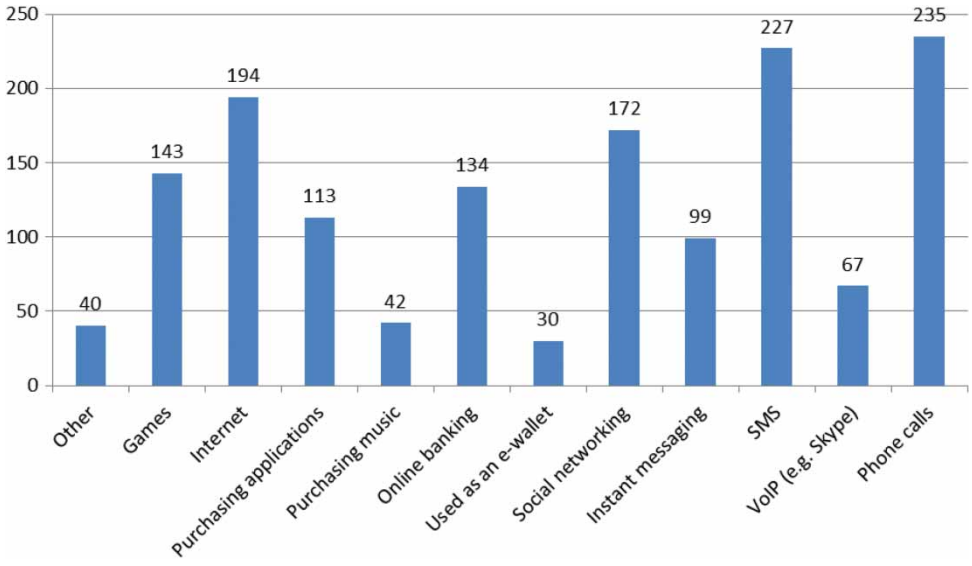

Figure 2. Smart mobile device usage activities.

Younger participants stood out as the main users of social networking, and to determine if there is any association between age and the use of social networking media a two-tailed chi-squared test was performed. A critical χ^2 value of 9.48 was calculated using an alpha of 0.05, resulting in a p-value of 0.0006. The p-value calculated represents the probability of observing a test statistic different than what was observed. This suggested that there is a significant association between the age of a participant and their use of social networking media, with younger participants being more likely to use social networking on their mobile devices. Our observation echoed the findings from the Australian Communications and Media Authority-commissioned consumer survey, which found that 'the majority of people accessing social networking sites via their mobile handset were aged between 18 and 34 years, accounting for 62 per cent of all social mobile users in Australia' (ACMA 2012, 25). This is important to highlight as reports, such as the 2012 report from AVG (2012), suggested that social networking is becoming an important attack vector for cyber criminals and exploited social networking accounts can be used to send malicious links inside its messages and posts.

3. Results

3.1. General security

We asked participants if they used the 'Remember me' feature to save their passwords, login credentials or credit card information. Not surprisingly, close to half of the survey participants reported using this feature, while 46.4% of participants responded that they used the feature to store some form of personal information on their devices (see Figure 3). Of the 116 participants that reportedly used the 'Remember me' feature, 78.4% stored passwords, 76.7% stored login credentials and 21.5% stored credit card information – participants were able to select more than one option, and hence, we present the results as an individual percentage out of 116.

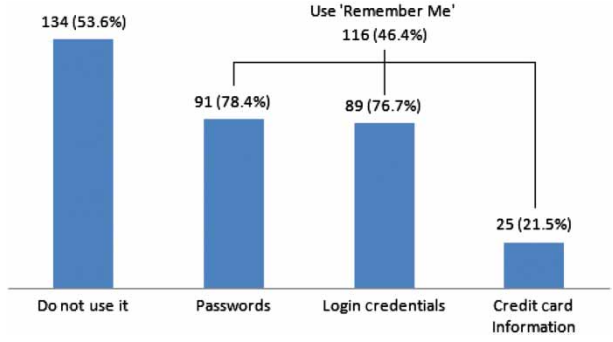

Figure 3. Number of participants using the 'Remember me' feature.

Although the use of smart mobile devices offers many benefits including ease of sending and checking messages and remotely accessing information online, it can also introduce information security risks if not properly protected. It is, therefore, concerning but not surprising that close to half of the survey participants reported not locking their devices (with password). This could perhaps be due to the default (no password) setting in iPhones and iPads (collectively referred to as iOS devices) and these iOS devices comprised 51.6% of all devices reportedly owned by the survey participants. Very few participants chose to lock their SIM card – 67.5% of the participants reportedly did not lock their SIM card with a PIN, and even fewer chose to use an alphanumeric password, despite the latter being more secure than a numeric-based PIN. Figure 4 shows the different locking mechanisms employed by participants to lock their devices.

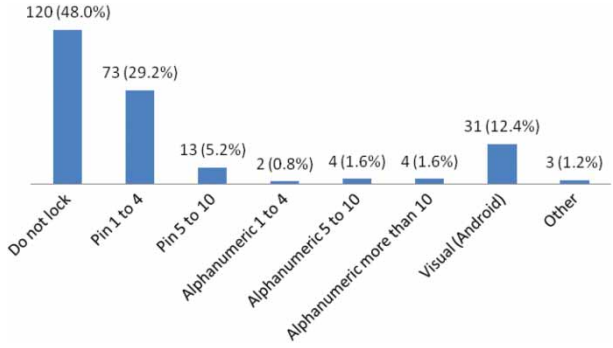

Figure 4. Types of locking mechanisms used by survey participants to lock their devices.

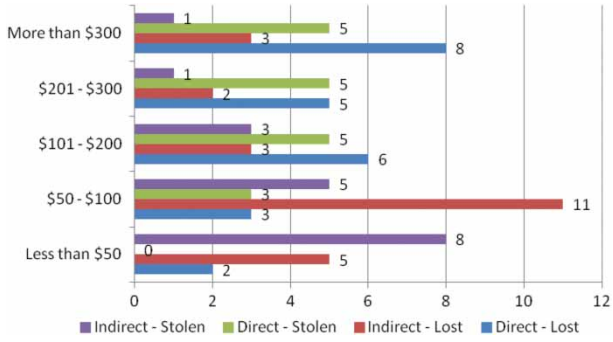

Figure 5. Costs due to lost or stolen device(s).

While it is encouraging that 29.2% of the survey participants reported using a four-digit PIN to lock their devices, various research has shown that this can be brute forced relatively easily using open source tools (Bianchi, Oakley, and Kwon 2012).Users of iOS devices in particular may not realise that the default 4 PIN lock is not the only option available, and that by turning off 'Simple Passcode' they can specify an alphanumeric password of as many characters/digits as they like. Only 30.7% of Android owners make use of Androids' visual method to lock their devices.

A two-tailed chi-square test was performed to determine if the operating system has any impact on whether a locking mechanism was employed by a participant. A critical χ^2 value of 7.81 was calculated using an alpha of 0.05, resulting in a p-value of 0.03. This suggested that there is a moderate association between the variables – the type of operating system a device has and whether a device is locked (or not).

The dangers of not locking and securing one's devices are well documented. For example, data on devices that do not employ any forms of protection such as password and encryption will be accessible to anyone in possession of the devices should they be lost, misplaced or stolen. Unfortunately, the vast majority of survey participants (83.2%) indicated that they did not use encryption software.

Only 24 (9.6%) and 18 (7.2%) participants reported losing their devices or had their devices stolen, respectively. Not surprisingly, recovery of lost and stolen devices was low – only 10 and 4 participants recovered their lost and stolen devices, respectively.

Although the total number of lost and stolen devices is only 42 (out of 314 devices in the survey), we observed that iPhones made up 50%, followed by Android devices at 28.5% and that both male and female participants had the same number of combined lost and stolen devices (50% each for lost/stolen devices). 57.1% of the devices that were either lost or stolen had no locking mechanisms employed, and as such, data stored on these lost/stolen devices would be accessible by anyone finding these devices.

Only 33.3% of participants who lost their devices reported the incident to their telecommunications provider, 12.5% reported the loss to the police and 25% reported the loss to both their telecommunications provider and the police. Only 33.3% of participants reported their device stolen, with the majority of participants (66.7%) choosing not to alert the authorities or their telecommunications provider.

Apart from the risk of identity theft, access to personal and organisational data, the majority of participants also reported incurring high cost from losing their device or having their device stolen (see Figure 5), particularly for undergraduate students who comprised 57.1% of participants who either lost their device or had a device stolen.

The estimated indirect cost was not as high as the direct cost; 45.8% of participants who lost their devices indicated that their indirect cost was between AUD 50 and AUD 100, while 12.5% indicated that their indirect cost was in the range of AUD 300. It is possible that participants may not have included costs of Internet connection and time involved to restore data on the replacement devices in their estimations. Less than half of participants (45.8%) who lost their smart mobile device were reportedly covered by insurance.

Findings from our survey are consistent with various other independent computer security studies – that is, we need to educate and encourage individuals and businesses to come forward and report incidents to law enforcement and other appropriate channels, so that we have a better understanding of the frequency and extent of cyber crime incidents.

3.2. Malware

The rapid increase in smart mobile device users is seen by malware authors as a potential vector for criminal exploitation, with consequences for users, service providers and organisations (AVG 2012; Felt et al. 2011; Juniper Networks 2012; Symantec 2012; Total Defense 2012; TrendMicro 2012), as malware is often designed to steal the owner's login credentials and other personal information.

In total, 46.4% of participants indicated that they use the 'Remember me' feature to save passwords and/or login credentials and/or credit card information on their device, and if their device was compromised by malware, their information could be captured by the malware, sent back to the attacker and be used to impersonate the owner of the device.

We found that only 9.6% of participants indicated that they had malware on their smart mobile devices during the 2010–2011 financial year (1 July 2010 to 30th June 2011). This may not be a true indication of actual malware presence as malware can go unnoticed on a system for long periods of time (Chia, Yamamoto, and Asokan 2012; Felt et al. 2011). In addition, malware is not easy to detect for the 'average' smart mobile device user, and most financially motivated malware authors design their malware to stay undetected for as long as possible. Without anti-virus software installed on a smart mobile device, it is almost impossible for a user to detect or be alerted to the presence of malware on their device, unless for example the user receives an exceptionally high bill for premium-rate SMS messages for which the user did not subscribe. In a recent research, Zhou and Jiang found that 45.3% of the 1260 Android malware they studied 'have the built-in support of sending out background short messages (to premium-rate numbers) or making phone calls without user awareness' (Zhou and Jiang 2012, 95).

Devices running Android (the second most popular devices in our survey – see Figure 1) were reported to be the major target of malicious attacks during 2011 (F-Secure 2012; McAfee 2012; Total Defense 2012). In Android devices, apps run in their individual sandboxed environment and permissions are granted by the user on a per-app basis. Security is, unfortunately, as strong as the weakest link. For the:

> average end user, it is unclear when permissions are given and what the app is actually capable of. Once the app is installed, the OS doesn't recheck with the user and goes on to use the permissions without prompting the user again. (TrendMicro 2012, 13)

A 2012 report published by Sophos showed that Google removed over 100 malicious apps throughout 2010, and that in December of 2011 malicious apps that cloned popular games were downloaded 10,000 times before being removed (Sophos 2012).

The permission-based method utilised by Android to determine an app's legitimacy has been shown to be insufficient at classifying malicious apps reliably. On the other hand, the review process used by Apple is more restrictive for developers, as each app is thoroughly analysed for security issues before being released to the public (although there have been reports of potentially malicious apps getting past Apple's reviewers in recent times – see Goodin 2011). More adventurous users may also feel restricted, and many turn to jail-breaking or rooting their device. This can pose a serious security threat to the mobile device user if the user is not aware of the full implications of doing so, as there is no guarantee that apps installed through unofficial sources are secure and legitimate. For example, a majority of the few instances of malware targeted at iOS devices reportedly affected only jail-broken devices (Felt et al. 2011).

We found that 16.4% of the devices in this survey were either jail-broken or rooted; with 90.2% of these jail-broken or rooted devices belonging to male participants. Younger participants were also more likely to jail-break/root their devices, with those aged 19–25 making up 53.6% of the group. Jail-breaking or rooting a phone does not necessarily mean that they will have a higher rate of infection, but such devices will be more exposed than devices that are not jail-broken or rooted. It was found that of the 41 participants who had reported jail-breaking or rooting their devices, 63.4% stored login credentials or credit card information on their devices.

Researching or reading a review of an app is usually the first step to ensuring the app is safe to install, and one would expect that issues commonly experienced by other users will be well documented on the Internet (unless the user is one of the first users to encounter the issue). Our survey suggested that a higher percentage of participants were more likely (66%) than unlikely (18%) to research or read a review. In total, 76.4% of males said that they would be likely to research or read a review compared to only 55.4% of females.

Slightly less than two-thirds of participants (64.4%) indicated that they did not install apps from an unknown app provider and that more males (41.3%) than females (28.5%) reportedly installed apps from an unknown app provider. It is pleasing to learn that 74.64% of males indicated that they researched or read reviews before they download an app (assuming that they understand and trust what they read – unfortunately, there does not appear to be any simple method for helping users to identify a more trustworthy source or to trust one app over another). Figure 6 shows the demographics of participants who would reportedly install apps from unknown app providers.

Malicious apps can be identified by the permissions requested when installed or run (although there have been instances of non-malicious apps requesting unnecessary permissions when installed or run) (Do, Martini, and Choo 2014); we found that only 16% of participants reportedly allowed apps permissions that appeared unnecessary on their smart mobile devices. Those aged 19–25 and 26–35 were the most likely to allow unnecessary permissions, with each age group making up 32.5% of the group (i.e. both age groups make up 65% of the group). The security and privacy implications of apps were aptly summarised by Chia et al. 'current forms of community ratings used in app[lication] markets today are not reliable indicators of privacy risks of an app[lication]', and the study found 'popular applications request more permissions [than required] as well as evidence of attempts to entice or mislead the user into granting sensitive permissions with free apps and mature content' (Chia, Yamamoto, and Asokan 2012, 311).

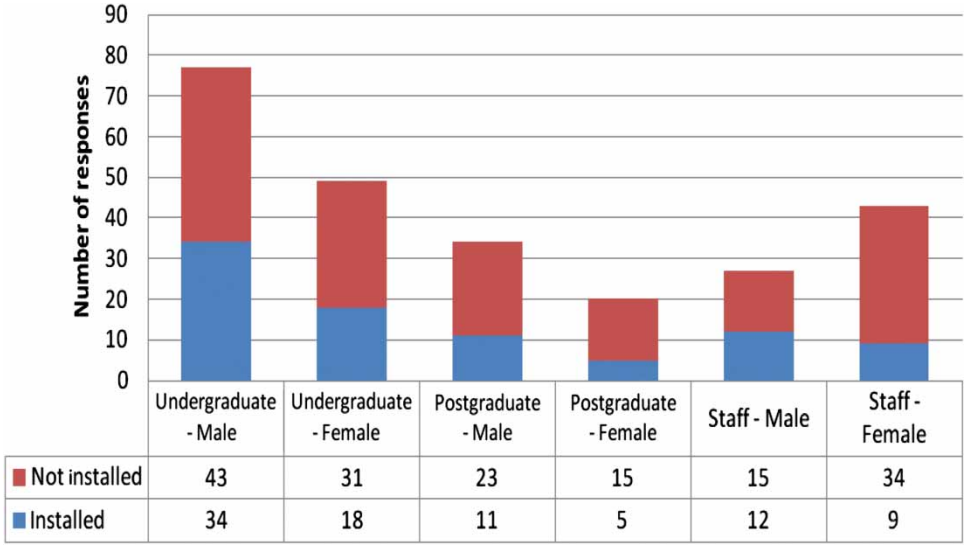

Figure 6. Do you install apps from unknown app providers?

Smart mobile device users are at a particular risk to malware due to the number of ways it can be spread onto their devices, and they need to carefully consider the links they click on, even on trusted websites (e.g. a link to a video clip on a friend's Facebook wall or private message). A 2012 report from AVG, for example, found an increasing number of attempts to spread malware through social networking mediums such as Facebook and Twitter, and particularly targeting Android devices (AVG 2012). Social networking is a popular attack vector for cyber criminals, where they are able to take advantage of social engineering techniques to trick unwitting users into clicking a link and installing malware onto their devices. For example in May 2012, malware analysts have reported that malware (detected as WORM_STECKCT.EVL) is spread via Facebook's private messages by distributing a shortened URL link. Once the malware is installed on the victim's device, the malware reportedly 'terminates services and processes related to antivirus (AV) software, effectively disabling AV software from detection or removal of the worm. WORM_STECKCT.EVL also connects to specific websites to send and receive information'. In addition, the malware is observed to download and execute another malware (detected as WORM_EBOOM.AC), which 'is capable of monitoring an affected user's browsing activity such as message posting, deleted posted messages and private messages sent on the following websites: Facebook, Myspace, Twitter, WordPress, and Meebo' (Pantanilla 2012).

In total, 12.3% of male participants and 27.7% of female participants indicated that they would be somewhat or very likely to download something from a link in an SMS, instant message (IM) or email message. A critical χ^2 value of 9.48 was calculated using an alpha of 0.05, resulting in a p-value of 0.01. This suggested a significant association between gender and the likelihood of downloading a potentially malicious app. Females appeared to be more trusting and likely to download content from a link in an SMS, IM or email message.

3.3. *Unauthorised access*

Unauthorised access of smart devices is a serious threat for any organisation whose employees store sensitive data and/or credentials on their smart mobile devices (Mani, Choo, and Mubarak 2014). It should by now be common knowledge that leaving a device unattended, especially if no locking mechanism is in place, exposes any personal and corporate data stored on the device. Even if data have been deleted from the device, it could still potentially be retrieved using open source and commercial forensic software (e.g. Micro Systemation XRY and CelleBrite UFED Kit). It is assuring to learn that the majority of participants indicated that they would be somewhat or very unlikely to leave their device unattended in a public setting such as a café or library (79.2%).

Of those who said that they would be more likely to leave a device unattended in a public setting, 33% in each of the Very Likely and Somewhat Likely categories reported having their device stolen from them or lost a device in the last financial year.

Of the 250 participants, 14.5% were aware of unauthorised access incidents involving their mobile devices, 66.8% were certain their device was not accessed without their knowledge and the remaining 18.8% were unsure. Of those who reported being aware that their device had been accessed without their permission, 63% did not use any form of locking mechanism.

Further analysis of the group that reported not locking their devices shows that 86% stored some form of personal information on the devices (password, login credentials and credit card information). Of those who answered that they were either somewhat or very likely to leave their device

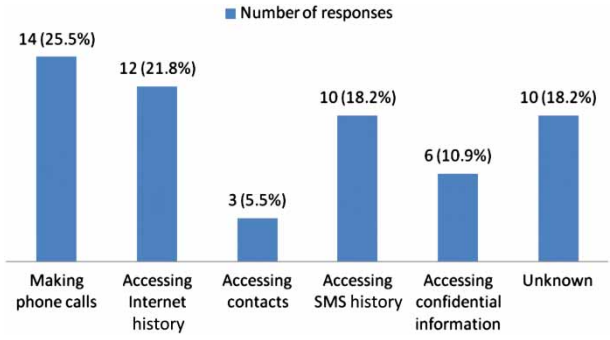

Figure 7. Consequences of unauthorised access to the devices.

unattended, 62% were undergraduate students, followed by 19% staff and 19% postgraduate students. Undergraduate students comprised 57% of the participants who reported that their devices were accessed without their authorisation and female participants (60%) appeared more likely to have their devices accessed without authorisation.

The top three known primary consequences of unauthorised access to the devices were making a phone call (Android), followed by accessing Internet and SMS history on the device (iOS devices) and accessing contacts and personal information (iOS devices) (see Figure 7).

3.4. Wi-Fi and Bluetooth security

Wi-Fi and Bluetooth functionalities are commonly found in smart mobile devices, although many users may be unaware of the potential risks associated with using these features in a public setting.

Participants were asked a series of questions to gauge their behaviour with connecting to unknown Wi-Fi and Bluetooth networks and how they would react to a request from an unknown source. About 48.4% of participants admitted leaving their Wi-Fi on at all times on their device (see Figure 8). This increases the risk of them connecting to a malicious network and potentially exposing their data to an attacker (e.g. man-in-the-middle attack if users unwittingly connect to rogue wireless access point).

Males tended to be more restrictive with their Wi-Fi; with 61.6% of males have their Wi-Fi turned off by default,

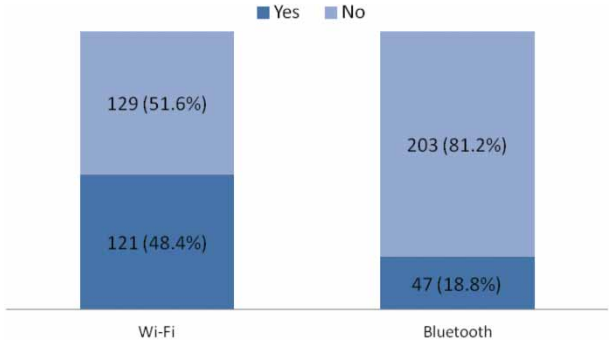

Figure 8. Do you leave your Wi-Fi or Bluetooth on at all times?

and only 38.4% keeping it on at all times. Females, on the other hand, appeared to be more trusting, with 60.7% leaving their Wi-Fi on at all times, and only 39.3% keeping it turned off.

Participants were asked if they would, when given a choice, connect to an unknown Wi-Fi hotspot. Only 16.4% said that they would, 37.2% would consider doing so depending on their situation, and the majority (46.4%) would choose not to.

A critical χ^2 value of 15.5 was calculated using an alpha of 0.05, resulting in a p-value of 0.03. This suggested a moderate association between the age of a participant and their decision to connect to unsecure and unknown Wi-Fi networks. For example, we observed that younger participants (18 and younger) were more likely to connect to an unknown Wi-Fi network, with 22% reporting they would connect to an unknown Wi-Fi network. Sixty-six per cent of the participants in the 36–50 age group reported they would not connect to an unknown network.

Of the 41 participants who responded they would connect to an unknown Wi-Fi network, 63.4% also performed online banking on their device. Females, particularly those in the 19–25 age group, comprised 76% of the group who perform online banking and would connect to an unknown Wi-Fi network.

Bluetooth is not as commonly used – only 18.8% keep their Bluetooth on at all times, as shown in Figure 8. Of the 47 participants who leave their Bluetooth turned on at all times, 23.4% reported that they had malware on their device within the last financial year. On the other hand, only 6.4% of those that kept their Bluetooth switched off at all times reported having malware on their device. This only takes into account the users who were aware of malware presence on their device, but it does highlight that devices that are always discoverable are at a greater risk of malware infection.

In order to infect a device via bluetooth, the user must accept the attackers' initial connection request and the device must be in visible mode. Users may blindly accept such requests without realising the risks. For example, of the participants who reported leaving their Bluetooth turned on at all times, 34% admitted that they would be very or somewhat likely to download content from a link in an unknown SMS and 25.5% admitted to allowing an app permission(s) that seem unnecessary.

As the number of Wi-Fi supported devices increases, wireless hotspots aimed at providing free wireless network connections are also springing up around every corner. Many mobile users may not be aware that not all hotspots have the same level of security, as well as the existence of rogue wireless access points (Beyah and Venkataraman 2011; Grubb 2010). As there is no way to guarantee who the owner of a hotspot is (e.g. attackers can easily 'mimic' a popular hotspot), participants were encouraged to restrict their use of unknown wireless connections upon completion of the survey.

3.5. Phishing

Smart mobile devices are a potential target for phishing scams. For example, the reduced screen size can be exploited by criminals to disguise the legitimacy of an email (e.g. using shortened URLs) and most smart devices will only display the first section of a website link.

Participants were asked a series of questions to gauge their perceived awareness of phishing-related threats and their behaviour towards situations that could lead to them becoming a victim of a phishing attack. This survey section is presented in two parts:

(1) participants were asked to rate the likelihood of them acting inappropriately in a situation that would expose themselves to a potential phishing attack
(2) they were then asked to rate their phishing awareness capabilities, before being presented with a series of example emails and asked to assess their legitimacy.

Figure 9 shows one such example presented to participants; and in total, there were three banking examples, three Facebook examples, one PayPal example, one eBay example, one Amazon example and one miscellaneous example.

Just over half of the participants (52%) indicated that they would be somewhat or very unlikely to open an email from an unknown contact, 69.6% of the participants stated that they would be somewhat or very unlikely to accept a friend's request (IM, Facebook, etc.) from an unknown source and 48.8% of participants would open an SMS from an unknown source. Phishing attacks are commonly associated with email messages, and SMS is another attack vector that is not widely understood by the average smart mobile device user. For example, Catiglione, Prisco, and Santis (2009) suggested that mobile users may be more trusting of a phishing message purporting to be from their bank sent via SMS than email.

Males were found to be slightly more security conscious with 57.1% of males indicating they would be somewhat or very unlikely to respond to unknown requests or correspondence respectively.

Thirty-four per cent of staff participants and 32% of undergraduate student participants indicated that they were somewhat or very likely to accept unknown correspondence, and postgraduate student participants appeared to be the most security conscious of the three groups – only 21% responding that they would be somewhat or very likely to accept unknown correspondence. Sixty-six per cent of participants in the 36–50 age group indicated that they would be somewhat or very unlikely to accept an unknown request or correspondence. Only 42% of participants in the 26–35 age group responded that they would be somewhat or very unlikely to accept the same unknown correspondence.

The results of the phishing questions, and the number of questions participants answered correctly are shown in Figure 10 and Tables 2 and 3 (mean = 6.62 and std. dev = 2.33). Fifty-four per cent of participants were able to answer seven or more questions correctly, and only a few (18.4%) answered less than five questions correctly and we are pleased to learn that all 250 participants were able to score at least one of the phishing questions correct.

Of the 138 male and 112 female participants, males rated themselves as being more likely than females at detecting a phishing scam; with 75% of male participants rating themselves as being somewhat or very likely to detect a phishing scam (compared to 49% of females rating themselves as somewhat or very likely to detect a phishing scam). The results show that males (mean = 7.10, std. dev. = 2.39) answered more questions correct on average than females (mean = 6.07, std. dev. = 2.13), and of the 135 participants who scored seven or more phishing questions correctly, 67.4% were male and only 32.6% were female. To assess whether gender has an impact on the ability to detect a phishing scam, a test was performed on the number of correct responses each gender managed to answer correctly. A critical χ^2 value of 9.48 was calculated using an alpha of

Figure 9. Example of a phishing email presented to participants.

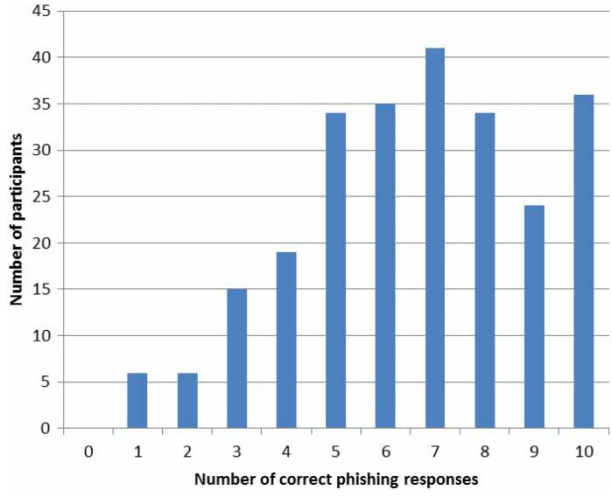

Figure 10. Results of the phishing questions.

Table 2. The responses to participants' perceived likelihood of detecting a phishing scam versus the number of correct responses to the 10 phishing questions.

No. correct phishing responses	Very likely	Somewhat likely	Neutral	Somewhat unlikely	Very unlikely	Total
9–10	29 (48.3%)	17 (28.3%)	6 (10%)	4 (6.7%)	4 (6.7%)	60
7–8	32 (42.7%)	22 (29.3%)	8 (10.7%)	9 (12%)	4 (5.3%)	75
5–6	15 (21.7%)	20 (29%)	21 (30.4%)	9 (13%)	4 (5.8%)	69
3–4	11 (32.4%)	6 (17.6%)	8 (23.5%)	7 (20.6%)	2 (5.9%)	34
0–2	0 (0%)	6 (50%)	4 (33.3%)	0 (0%)	2 (16.7%)	12
Total	87	71	47	29	16	250

Note: Due to rounding, row percentages may not total 100.

Table 3. Gender versus number of correct phishing responses.

Number of correct phishing responses	1–2	3–4	5–6	7–8	9–10	Total
Male	8	10	29	48	43	138
Female	4	24	40	27	17	112
Total	12	34	69	75	60	250

0.05, resulting in a p-value of 0.00009. This suggested a significant association between the gender of a participant and how well they performed in the phishing questions. In this context, males appeared to be better at detecting phishing scams.

Undergraduate students outperformed both postgraduates and staff, of the 135 participants who answered seven or more phishing questions correctly, 44.4% were undergraduate students, followed by postgraduate students (28.1%) and staff (27.5%).

Those aged 19–25 rated themselves as being the most likely to detect a phishing scam, comprising 44% of the 84 participants who reported they would be very likely to detect a phishing scam. Only 7% of those aged over 51 reported that they would be very likely to detect a phishing scam; and it appeared that they were right in their self-assessment, with 34.8% of those answering seven or more phishing questions correct were aged between 19 and 25, with only 5.9% being over the age of 51. However, a two-tailed chi-squared test of age versus performance shows no significant association between the two variables (χ^2 value $= 15.50$, p-value $= 0.13$).[1]

Participants appeared to be trusting of emails with clearly visible corporation logos. For example, two phishing emails that purportedly came from 'Bank' sources were plain text with a link to login to a fake website, and both had at least 70% of participants correctly guessed they were illegitimate. The other phishing emails that had some form of company logo (eBay or PayPal) or came from a trusted source yielded lower correct response rates, with less than 58% of participants correctly guessed that they were illegitimate. Our findings are consistent with several other studies, including that of Dhamija, Tygar, and Hearst (2006) who concluded that misconceptions about website features like images and text can influence a user's perception of the legitimacy of a website.

As shown in Table 2, participants may tend to overestimate their ability to detect a phishing scam. For example, only 100 of the 158 participants (63.3%) who indicated that they were very or somewhat likely to detect a phishing scam chose seven or more correct responses.

Slightly less than half of the 45 participants (46.7%) who indicated they were somewhat or very unlikely to detect a phishing scam chose seven or more correct responses. This may be due to this particular group of participants perceiving their lack of technical knowledge as a disadvantage, but they still possess the reasoning skills to be able to determine when they have received a malicious email.

Android participants were more likely to overestimate their ability at detecting a phishing scam, with 86.8% scoring fewer than eight correct responses while 57.9% of iPhone users scored fewer than eight correct responses.

Figure 11 shows the consequences of the 91 participants who acknowledged receiving a phishing email in the last financial year, only slightly more than half (52.7%) of participants experienced no consequence (these participants may not be able to identify the consequence), and the remainder had one or more of their personal accounts compromised.

Of the participants who had their social networking accounts compromised, 85% scored fewer than six correct responses. Seventy-eight per cent of participants who had either their email accounts or IM accounts compromised, scored fewer than six correct responses with 85.7% of those

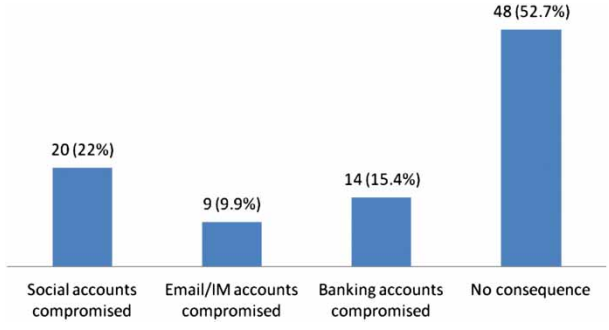

Figure 11. Consequences of receiving phishing emails.

who had their banking accounts compromised scored fewer than six correct responses. On the other hand, 50% of the participants who experienced no consequences scored more than seven correct responses. This suggests that participants who have their personal accounts compromised are likely to have less knowledge about phishing-based scams than participants who experienced no consequence as a result of receiving a phishing email.

4. Discussion and conclusion

4.1. Discussion

A typical crime prevention intervention is to create conditions unfavourable to crime. For example, the routine activity theory (RAT) is a theory about criminal events, but offender motivation is a crucial element. RAT proposes that crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen and Felson 1979). RAT draws on rational exploitation of 'opportunity' in the context of the regularity of human conduct to design prevention strategies, especially where terrestrial interventions are possible (Broadhurst and Choo 2011). The theory assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (Felson 1998; Yar 2005); and that victimisation risk is a function of how one (victim) patterns their behaviour and lifestyle. The interaction between smart mobile device users, cyber criminals (e.g. cyber criminals are financially motivated) and situational conditions (e.g. opportunities and weak guardianship) has great influence on the situation (e.g. How easy it is to design malware and phishing websites targeting smart mobile device users, and the risk of getting caught and prosecuted in a court of law?).

There are a number of ways that criminological theories such as RAT can be applied to reduce mobile security risk. Cyber crime prevention strategies using RAT, for example, target each of these areas – (1) increasing the effort required to offend; (2) increasing the risk of getting caught; and (3) reducing the rewards of offending.

Measures that users can undertake to protect the information stored on smart mobile devices:

- Enabling user authentication can reduce the rewards of offending (e.g. a password-protected device may be of little use to an opportunistic thief). In the survey, we found that a large number of users do not properly secure their devices. For example, over half of the participants reported not using any form of locking mechanisms, and the majority who reported using locking mechanisms used a 4-digit PIN, despite the latter being susceptible to brute force attacks (Bianchi, Oakley, and Kwon 2012).
- Adopting safe usage behaviours to increase the risk of getting caught (e.g. installing apps such as 'Find My iPhone' – http://www.apple.com/au/support/icloud/find-my-device/); and reduce the rewards of offending. For example:
  (i) Installing anti-malware tools and verifying the authenticity of downloaded apps. It was found that only a small percentage of participants reported having malware on their devices, and those that had jail-broken/rooted their devices tended to exhibit risky behaviour (e.g. downloading and installing apps from unknown app providers). We observed that females were more trusting and more likely than males to download content from a link in an SMS or email (p-value of 0.01).
  (ii) Installing remote wiping or locating apps: participants that were more likely to leave their devices unattended also showed more risky behaviour such as not locking their phones and storing personal information on the devices (e.g. using the 'Remember Me' feature), and that those who were more security conscious were less likely to have their device misplaced, stolen or accessed without their authorisation.

The findings from this survey also suggested that many end users are generally unaware of the risks that they may expose themselves to every day and that these users do not receive sufficient education regarding their smart devices' usage and security. The participants were generally unaware of the risks they subjected themselves to by leaving their Wi-Fi and Bluetooth turned on at all times, particularly those who were also likely to perform online banking and other activities that could expose personal information to an attacker. Younger participants responded that they would be the most likely to connect to an unsecure and/or unknown Wi-Fi network, in particular those in the 19–25 age group (p-value of 0.03). Social networking account, bank account and email account breaches were the top three recorded consequences as a result of phishing scams received by participants.

Although all of us need to take responsibility for protecting ourselves in the online space, a key message from the Australian Government House of Representatives Standing Committee on Communications inquiry in 2010 was that a more integrated, coordinated and concerted effort by government agencies, industry and community organisations is required to combat the cyber criminal activities that victimise individual end users and businesses, and can help to ensure that the most effective cyber crime prevention advice is provided to the community (e.g. smart mobile device users) (Australian Government House of Representatives Standing Committee on Communications 2010). One of the reviewers pointed out that ongoing training and education

> cannot be the sole solution or even one that can be very reliable at all times. When we teach someone to face a

> specific problem there is the danger that once the attacker knows that exploiting that problem is not working anymore, he finds new ways to do it, and the user is not likely to recognize the attack anymore. Maybe the educational part needs to be rethought in a way that the user must be thought how to 'fish' more than explaining how the 'specific fishes looks like' to recognise them.

The broad aim of the ongoing training and education programmes is to bring about behavioural change and increase user awareness.

Although there are various cyber crime educational initiatives in Australia, there has been limited evaluation of these educational initiatives. The evaluation and study of such educational initiatives is important (e.g. to develop a good understanding of what works, what does not work, and why), as a badly implemented educational initiative may not result in any of the hoped-for benefits eventuating (regardless how well-conceived the educational initiative may be). The post-survey feedback we received from the participants (e.g. interest in tips to identify fraudulent emails and scams and the educational materials provided at the conclusion of each survey – see Figure 12), for example, highlight the ongoing need for training and awareness initiatives, particularly initiatives focusing on mobile security and usage. In addition, we suggest that any educational materials developed for smart mobile device users need to be tailored specifically to the user group (e.g. Generation X, Generation Y, and baby boomers; and end users from diverse cultural and linguistic backgrounds) and end users with varying technical backgrounds.

Incubating and creating the market incentives for smart mobile device manufacturers to integrate security into their software, hardware and system development life cycle will lead to an improved level of security (Sobel and McGraw 2010), and increase the marginal cost of security violations. Consequently, the effort required to offend is increased and the marginal benefits of cyber crime reduced. Secure software (e.g. mobile operating systems[2] and firmware) and hardware[3] will also result in productivity gains for smart mobile device manufacturers as less time and resources will be spent on formulating and releasing patches (Choo 2011a).

4.2. *Limitation*

While the survey was only undertaken at one Australian University and the responses were small in number, by comparison to the number of smart mobile devices as a whole in Australia, the survey provides a good indication of the cyber threat landscape faced by users of smart mobile devices. For example, the majority of our participants are young and university educated, and likely to be more tech-savvy than the general public and, hence, may provide a better insight into cyber threat landscape faced by users of smart mobile devices.

4.3. *Future research*

There is an ongoing need to conduct more strategic research and evaluation that can provide policy and practice relevant evidence that would enable policy-makers and practitioners to design national regulatory measures and appropriate policy responses to address this new emerging cyber threat environment. Potential research projects that would help filling gaps in the knowledge base about mobile-related risks, and provide a vital regional perspective include:

- What is the nature of mobile-related risks, and how have mobile-related risks changed in the past few years?
- What are the current trends and emerging challenges that have an impact on smart mobile device users?
- How can we enhance the security of privacy on smart mobile devices?
- How can we put in place defences to protect even the unaware and/or non-educated smart mobile device users?

Future extensions of this survey include:

- A targeted approach to help develop the educational materials where small user groups (e.g. from different

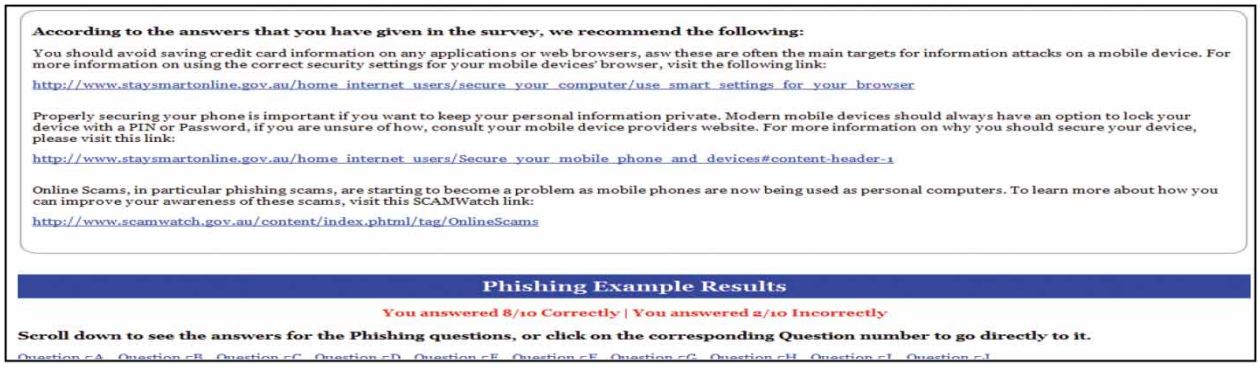

Figure 12. An example of the feedback page received at the end of the survey.

age groups – digital natives and digital migrants, different educational backgrounds, or cultural and ethnic backgrounds) are selected to participate in face-to-face interviews, and presented with the survey multiple times with educational materials specific to their results given after each round. The overall results could be used to show the effect that the materials have, and feedback from the participating user groups can be used to further refine the educational materials.

- Collaborating with like-minded researchers in higher educational institutions and other organisations in Australia and overseas[4] to conduct this survey on a wider scale including on a national scale, which would allow us to gauge change and monitor emerging mobile security-related trends. Analysing the collected data from multiple sources and countries will (1) provide statistically sound national and international data and a much broader international understanding of the current and emerging mobile security-related threats, and (2) allow us to ensure that any educational materials developed are based on international best practices.

Acknowledgements

The views and opinions expressed in this article are those of the authors alone and not the organisations with whom the authors are or have been associated or supported. This project has been approved by the UniSA's Human Research Ethics Committee. We would like to thank our colleagues including the participants for assisting and participating in this survey, and Ben Martini for his assistance in the earlier phases of the survey. We also like to thank Dr Changxu (Sean) Wu, the Associate Editor of this journal, and the three reviewers for their time, contributions, and positive response to this manuscript and the recognition of the significance and relevance of the topic. Despite their invaluable assistance, any errors remaining in this paper are solely attributed to the authors.

Funding

The corresponding author is partially supported by an internal grant.

Notes

1. As correctly pointed out by one of the reviewers, users generally pay more attention to detecting scams when they are aware that there may be a problem (in this context, whether the image they were shown was a phishing scam or not).
2. For example in July 2013, a security researcher 'discovered a vulnerability in Android's security model that allows a hacker to modify APK [Application Package File] code without breaking an app's cryptographic signature, to turn any legitimate app into a malicious Trojan, completely unnoticed by the app store, the phone, or the end user'; and it was estimated to affect nearly 900 million devices worldwide (Forristal 2013). A patch has been released by Google (2013).
3. For example in May 2012, it was reported that:

   > ZTE Corp, the world's No. 4 handset vendor and one of two Chinese companies under U.S. scrutiny over security concerns, said one of its mobile phone models sold in the United States contains a vulnerability that researchers say could allow others to control the device. (Sun 2012)

4. We have recently collected 250 responses and 221 responses from undergraduate and postgraduate students recruited through a university in India and Pakistan, respectively.

References

ACMA. 2012. "The Emerging Mobile Telecommunications Service Market in Australia." http://www.acma.gov.au/webwr/_assets/main/lib410148/CommsRep3_Emerging_mobile_tcomms_svce.PDF

Australian Government House of Representatives Standing Committee on Communications. 2010. *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. Canberra: Commonwealth of Australia.

AVG. 2012. *AVG Community Powered Threat Report*. http://aa-download.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf

Beyah, R., and A. Venkataraman. 2011. "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions." *IEEE Security & Privacy* 9 (5): 56–61.

Bianchi, A., I. Oakley, and D. Kwon. 2012. "Open Sesame: Design Guidelines for Invisible Passwords." *Computer* 45 (4): 58–65.

Broadhurst, R., and K.-K. R. Choo. 2011. "Cybercrime and On-line Safety in Cyberspace." In *Routledge International Handbook of Criminology*, edited by C. Smith, S. Zhang, and R. Barberet, 153–165. New York: Routledge.

Catiglione, A., R. Prisco, and A. Santis. 2009. "Do You Trust Your Phone?" 10th international conference on e-commerce and web technologies, Linz, Austria, LNCS 5692/2009, 50–61.

Chia, P. H., Y. Yamamoto, and N. Asokan. 2012. "Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals." International World Wide Web Conference Committee, Lyon, France, ACM, 2012, 311–320.

Choo, K.-K. R. 2011a. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers & Security* 30 (8): 719–731.

Choo, K.-K. R. 2011b. "Cyberthreat Landscape Faced by Financial and Insurance Industry." *Trends & Issues in Crime and Criminal Justice* 408: 1–6.

Choo, K.-K. R. 2013. "New Payment Methods: A Review of 2010–2012 FATF Mutual Evaluation Reports." *Computers & Security* 36: 12–26.

Choo, K.-K. R. 2014. "A Conceptual Interdisciplinary Plug-and-Play Cyber Security Framework." In *ICTs and the Millennium Development Goals – A United Nations Perspective*, edited by H. Kaur and X. Tao, 81–99. New York: Springer.

Cohen, L. E., and M. Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44 (4): 588–608.

Do, Q., B. Martini, and K.-K. R. Choo. 2014. "Enhancing User Privacy on Android Mobile Devices via Permissions Removal." 47th annual Hawaii international conference on system sciences (HICSS 2014), IEEE Computer Society Press, 6–9 January 2014, 5070–5079.

Dhamija, R., J. D. Tygar, and M. Hearst. 2006. "Why Phishing Works." SIGCHI conference on human factors in computing systems (CHI 2006), ACM, 581–590.

Felson, M. 1998. *Crime and Everyday Life*. New York: Pine Forge Press.

Felt, A. P., M. Finifter, E. Chin, S. Hanna, and D. Wagner. 2011. "A Survey of Mobile Malware in the Wild." 1st ACM workshop on security and privacy in smartphones and mobile devices, ACM, Chicago, IL, 3–14.

Forristal, J. 2013. "Uncovering Android Master Key That Makes 99% of Devices Vulnerable." Press Release 9 July. http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/

F-Secure. 2012. *Mobile Threat Report Q1 2012*. http://www.f-secure.com/weblog/archives/MobileThreatReport_Q1_2012.pdf

Goodin, D. 2011. "Apple Expels Serial Hacker for Publishing iPhone Exploit." *The Register* 8 November. http://www.theregister.co.uk/2011/11/08/apple_excommunicates_charlie_miller/

Google. 2013. Master Key Dual Fix. https://play.google.com/store/apps/details?id=tungstwenty.xposed.masterkeydualfix

Grubb, B. 2010. "Creator of 'Point-and-Click' Wi-Fi Hacking Tool Defends its Release." *Sydney Morning Herald* 5 November. http://www.smh.com.au/technology/security/creator-of-pointandclick-wifi-hacking-tool-defends-its-release-20101105-17gon.html

Guinchard, A. 2011. "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy." *Journal of Strategic Security* 4 (2): 75–96.

Hooper, C., B. Martini, and K.-K. R. Choo. 2013. "Cloud Computing and its Implications for Cybercrime Investigations in Australia." *Computer Law and Security Review* 29 (2): 152–163.

Juniper Networks. 2012. *2011 Mobile Threats Report*. http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

Mani, D., K.-K. R. Choo, and S. Mubarak. 2014. "Information Security in the South Australian Real Estate Industry: A Study of 40 Real Estate Organisations." *Information Management and Computer Security* 22 (1): 24–41.

Martini, B., and K.-K. R. Choo. 2013. "Cloud Storage Forensics: ownCloud as a Case Study." *Digital Investigation* 10 (4): 287–299.

McAfee. 2012. *McAfee Threats Report: First Quarter 2012*. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf

McAfee. 2013. *Mobile Security: McAfee Consumer Trends Report* (Trends in risky apps, mobile misbehavior, and spyware). http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf

Ohaya, C. 2006. "Managing Phishing Threats in An Organization." 3rd Annual Conference on Information Security Curriculum Development, ACM, 159–161.

Pantanilla, C. 2012. "Worm Spreads via Facebook Private Messages, Instant Messengers." http://blog.trendmicro.com/worm-spreads-via-facebook-private-messages-instant-messengers/

Quick, D., and K.-K. R. Choo. 2013a. "Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or Its Metadata?" *Digital Investigation* 10 (3): 266–277.

Quick, D., and K.-K. R. Choo. 2013b. "Digital Droplets: Microsoft SkyDrive Forensic Data Remnants." *Future Generation Computer Systems* 29 (6): 1378–1394.

Quick, D., and K.-K. R. Choo. 2013c. "Dropbox Analysis: Data Remnants on User Machines." *Digital Investigation* 10 (1): 3–18.

Sobel, A. E. K., and G. McGraw. 2010. "Interview: Software Security in the Real World." *IEEE Computer* 43 (9): 47–53.

Sophos. 2012. *Security Threat Report 2012*. http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Sun. 2012. "ZTE Score M Scores a Backdoor Vulnerability." Trend Micro 25 May. http://blog.trendmicro.com/trendlabs-security-intelligence/zte-score-m-scores-a-backdoor-vulnerability/

Symantec. 2012. *Internet Security Threat Report 2011 Trends*. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Tassone, C., C. Martini, K.-K. R. Choo, and S. Slay. 2013. "Mobile Device Forensics: A Snapshot." *Trends & Issues in Crime and Criminal Justice* 460: 1–6.

Total Defense. 2012. 2011 *Total Defense Threat Report*. http://totaldefense.com/news/threat-report-2011.aspx

TrendMicro. 2012. "Enterprise Readiness of Consumer Mobile Platforms." http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_enterprise_readiness_consumerization_mobile_platforms.pdf

US GAO (US Government Accountability Office). 2012. *Cybersecurity: Threats Impacting the Nation*. Washington, DC: US Government Accountability Office (US GAO).

Yar, M. 2005. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2 (4): 407–427.

Zhou, Y., and X. Jiang. 2012. "Dissecting Android Malware: Characterization and Evolution." 33rd IEEE Symposium on Security and Privacy, 95–109.