NSW GOVERNMENT Justice

Background paper: mobile phone crime

Hanna Mohamad, October 2011

Table of contents

Introduction **3**

Mobile phone ownership **3**

Accessibility 4

Theft of the handset **5**

Prevalence 5

How mobile theft occurs in NSW 5

Where and when mobile phone theft occurs 6

Why mobile phones are stolen 8

Theft of information **9**

Prevalence 9

Type of threats 9

Malware 9

Applications 10

Smishing 10

Contactless mobile phone payments and online banking 11

Offenders and technology 11

Security features on mobile phone devices **12**

Hardware 12

Software 12

Government solutions **13**

International Mobile Equipment Identity (IMEI) 13

Public awareness 13

Legislation 13

International mobile phone theft interventions **14**

United Kingdom 14

International Mobile Equipment Identity (IMEI) 14

Immobilise system 14

Education 15

Introduction

The mobile phone market in Australia continues to evolve and is becoming increasingly complex due to developments in mobile handset functionality. Their convenience and affordability coupled with evolving technology, has changed the way consumers use these devices from simply placing and answering calls, to capabilities of that of computers including Internet access and making bank transactions.

In the context of crime, theft of mobile phone devices is not a new area. This is a crime that has remained stable over the last three years and current research shows mobile phone handsets remain a 'hot' item for opportunistic thieves.[1] However, an area that hasn't previously received much attention is the notable shift in focus by cyber criminals to mobile phone devices to steal personal and other sensitive information, whether through theft of the device or 'hacking' into the phone while it is still in the owner's possession.

While mobile phone fraud is a relatively new area for Australia, we know that criminals are interested in stealing data wirelessly and given the current lack of attention directed at mobile phone security, theft of information from the handset has the potential to become an emerging and significant problem. It is on this basis that a Government response is required to examine this issue in greater detail and identify areas of intervention.

Mobile phone ownership

Ownership of mobile phone handsets in Australia has increased at a rapid rate. As of December 2000, there was estimated to be over 10 million network connections. Ten years later, the number of network connections has increased by 125 per cent and by June 2010, the total number of mobile telephone services in operation in Australia reached 22.5 million. Further it is estimated that 6.8 million, or 30 per cent, allowed Internet connectivity.[2]

Mobile phone ownership continues to rise with the Australian Communications and Media Authority (ACMA) showing 85 per cent of individuals in Australia owned mobile phones as of June 2010. Figure 1 shows the Australian population growth over the last 10 years in comparison to the number of active mobile phone services in Australia. It is noteworthy that since 2007 there are more mobile phone services than people in Australia, suggesting that a number of the population have more than one mobile phone in use.[3]

While there is no information available on the number of network connections in each State, over one-third of Australian residents reside in New South Wales[4] and therefore, it would be reasonable to assume that a large majority of mobile connections would be in this State.

---

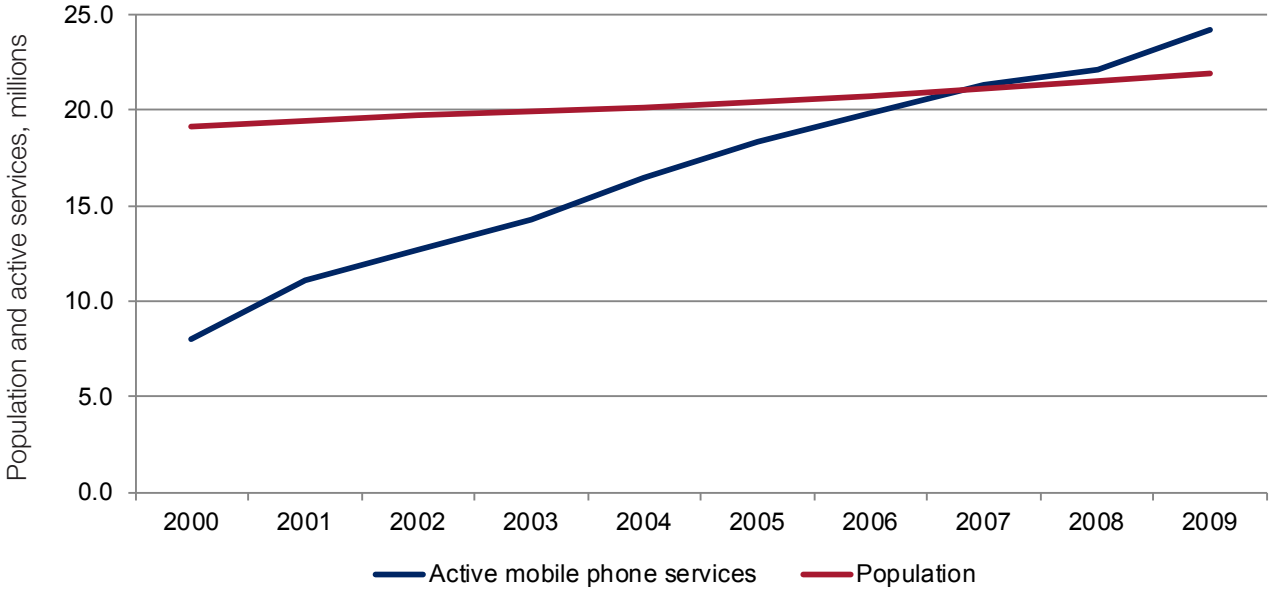
[1] Fitzgerald, J & Poynton, S. (2011). *The changing nature of objects stolen in household burglaries*, Issue Paper No 62, BOCSAR, Sydney.

[2] Australian Communications and Media Authority (ACMA) (2010). *2009–10 Communications report series: Report 2 – Take-up and use of voice services by Australian consumers*, Australian Communications and Media Authority, Sydney

[3] ibid

[4] Australian Bureau of Statistics (2010). *Australian Demographic Statistics, June 2010*, Australian Bureau of Statistics, Canberra.

Figure 1 – Population and active mobile phone services in Australia, 2000–2010



In addition, a recent survey[5] conducted by the ACMA examined the demographic characteristics of Australian consumers in relation to take-up and use of mobile phone services. The survey found:

- The 25–34 age group had the highest take-up of mobile phones (93 per cent). This was followed closely by the 35–44 age group (92 per cent) and 18–24 age group (88 per cent). Mobile phones are also now commonly provided to children aged between 14 and 17, with 77 per cent of children in this age bracket with a mobile phone.
- Location appears to not affect the take-up of mobile communications, with only a marginal difference between metropolitan and non-metropolitan respondents.
- There is little difference on the basis of gender.

Furthermore, in relation to ownership, by 2015, it is estimated that more than 60 per cent of mobiles in Australia will be smart phones. The term smart phone is generally used to refer to a high-end mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone. Some of the capabilities of a smart phone include web browsing, powerful email management, storage of information, a platform for many other digital applications known as 'apps', and software that run a complete mobile operating system (also known as mobile platform) such as Windows or Mac OS for a computer. All of these features offer the convenience of enabling mobile phone devices to be used in the same way as computers.

Accessibility

The ownership and availability of mobile phones has increased as the price of the handsets and plans have become more affordable. In Australia, there are three mobile network operators: Telstra, Optus and Vodafone Hutchison Australia (VHA operates the brands of

[5] Australian Communications Media Authority 2010, *2009–10 Communications report series: Report 2-Take-up and use of voice services by Australian consumers*, Australian Communications Media Authority, Sydney.

Vodafone and 3). Typically consumers purchase mobile phone devices either via a mobile plan or prepaid/outright. Mobile phone plans range from $19 per month to $129 per month over a 24-month contract, and often the customer receives the handset 'free' or at reduced cost. Phone handsets can also be purchased from as little as $29, however the majority of mobile phone devices retail for around $1,100 and can therefore be a valuable item to have stolen.

The next section discusses mobile phone crime in more detail, examining both theft of the handset and theft of information from the device.

Theft of the handset

Prevalence

In 2001 the Bureau of Crime Statistics and Research (BOCSAR) reported that the increase in mobile phone ownership had coincided with a dramatic increase in the number of incidents of mobile phone theft recorded each year in NSW. The highest increase was between 1999 and 2000, with the number of mobile phone thefts rising from 24,274 incidents to 39,891 incidents in 2000. The increases were evident immediately after the Christmas period, and were attributed to higher mobile phone sales during that time.[6]

Recent data from BOCSAR over the last 36 months (2008–2010) shows the number of incidents of mobile phone theft has remained relatively stable averaging 22,051 incidents per year.

It is important to note that available data on mobile phone theft only includes reported incidents. There is the possibility of under reporting of this crime, as it is likely consumers would only contact their phone provider when their phone is stolen and not report it to Police. Currently, we are not aware of any information sharing between mobile phone providers and law enforcement in response to this crime.

How mobile theft occurs in NSW

Analysis of the circumstances of mobile phone theft in NSW from 2008 to 2010 (shown in Table 1 below) reveals that:

- 'Other theft'[7] where the phone was not in the owner's possession at the time that it was stolen was recorded as the most common type of mobile phone theft (31% n = 20,540) followed by 'steal from person' as the second most common (18%, n = 11,643).
- A substantial number of mobile phone thefts continue to result from Break and Enter – Dwelling (17%, n = 11,347), although the overall volume of incidents has fallen.

[6] Briscoe, S. (2001). *The Problem of Mobile Phone Theft*, Crime and Justice Bulletin, Number 56. NSW Bureau of Crime Statistics and Research, Sydney.

[7] 'Other theft' is BOCSAR's category for NSW Police Force offences that include steal from marine vessel, steal vessel, other stealing *occurring somewhere other than a residential dwelling* (e.g. at temporary accommodation, business / commercial premises, in outdoor / public places, recreation premises).

- Steal from Motor Vehicle is the fourth highest offence type where mobile phones are stolen with a 17 per cent decrease since 2008,[8] in line with the overall reduction of this offence across New South Wales.
- There was a notable increase in the number of mobile phones being reported as stolen during a motor vehicle theft between 2009 and 2010, up by 518 per cent.

Table 1 Incidents where mobile phones were stolen, by crime type

Crime type	2008	2009	2010	% change 2008–2010	Total 2008–2010
Other theft	6,739	6,531	7,270	8	20,540
Steal from person	3,781	3,765	4,097	8	11,643
Break and enter – dwelling	3,933	3,756	3,658	-7	11,347
Steal from motor vehicle	3,616	3,121	3,016	-17	9,753
Steal from dwelling	1,575	1,634	1,773	13	4,982
Robbery without a weapon	1,372	1,099	981	-28	3,452
Break and enter – non-dwelling	590	431	430	-27	1,451
Steal from retail store	357	332	439	23	1,128
Robbery with a weapon (not a firearm)	416	322	295	-29	1,033
Fraud	96	104	88	-8	288
Motor vehicle theft	22	28	136	518	186
Receiving or handling stolen goods	63	44	40	-37	147
Robbery with a firearm	32	45	44	38	121
Assault	16	15	13	-19	44
Other offences	19	9	9	-53	37
Total	**22,627**	**21,236**	**22,289**	**-1**	**66,152**

The information in the table suggests that more mobile phones are stolen either directly from the individual or as a result of the device being left unattended. As mobile technology becomes more important to the lifestyles of users, consumers are likely to have their phone on their person and therefore the risk of leaving it unattended in a public place is greater, making it more accessible to an opportunistic thief.

Where and when mobile phone theft occurs

In relation to location of mobile phone thefts, Table 2 shows the Top 20 Local Government Areas (LGA) in NSW that had the highest incident of mobile phone theft per 100,000 population in the three years from 2008 to 2010. The information suggests:

- The top five LGAs recording the highest number of mobile phone thefts are the Sydney LGA,[9] followed by Blacktown, Newcastle, Parramatta and Wollongong. This is likely to be due to the relatively high use of mobile phones in each LGA's individual Central Business District.

[8] Between 1997 and 2000, the number of mobile phones stolen from motor vehicles accounted for the majority of incidents (38%).

[9] Sydney LGA often has a higher recorded crime rate, having a high 'visitor' population that can become victims of crime but are not reflected in the population rate.

- When compared with data from a decade ago, theft in 2010 occurred across a greater distance of NSW, whereas previously it was contained within the Sydney metropolitan area. This is reflective of data mentioned previously which indicates an increase in ownership of mobile phone devices regardless of location.

Table 2 NSW LGAs with the 20 highest rates of mobile phone theft, 2008–2010

Rank	LGA	Rate (per 100,000)
1	Sydney	18,996
2	Blacktown	4,196
3	Newcastle	3,814
4	Parramatta	2,942
5	Wollongong	2,565
6	Campbelltown	2,484
7	Liverpool	2,376
8	Waverley	2,289
9	Gosford	2,230
10	Randwick	2,210
11	Penrith	2,203
12	Wyong	2,085
13	Sutherland Shire	2,053
14	Fairfield	2,018
15	Bankstown	1,952
16	Lake Macquarie	1,565
17	Auburn	1,462
18	The Hills Shire	1,374
19	Canterbury	1,327
20	Holroyd	1,256

Currently, there is limited available information on when mobile phones are stolen. In a previous study, the Australian Mobile Telecommunications Association (AMTA) found that while mobile phones are most commonly stolen from vehicles (28 per cent), 20 per cent of devices are stolen in social venues such as restaurants, pubs and clubs. Further most phones were reported as lost or stolen on Monday, suggesting that most phones go missing over the weekend.[10] Further research is required in this area.

Similarly, there is limited information in regards to who commits mobile phone theft and the most commonly stolen phones. In 1996, Smith reported the most common thief to be a young, unemployed male whose primary motivation to steal mobile phones was profit.[11]

However, as mobile technology has evolved and handsets are increasingly used for storage of personal and financial information, they are no longer only attractive to an opportunistic thief interested in selling only the device for 'quick cash'. Mobile devices are valuable not

[10] Australian Mobile Telecommunications Association, *FAQs on mobile security*, Australian Mobile Telecommunications Association Viewed at: http://www.amta.org.au/pages/amta/FAQs.on.mobile.security
[11] Smith, R (1996). *Preventing Mobile Telephone Crime*, Australian Institute of Criminology: Canberra.

only because the hardware itself can be re-sold, but also due to the personal and sensitive information they may contain. Therefore potential offenders may now also include those individuals who are interested in stealing information from the handset, particularly as smart phones continue to penetrate the market.

We are currently not aware of any research that identifies which mobile phones are stolen more than others. However logic would dictate that that the most popular and valuable phones would be the most attractive.

Why mobile phones are stolen

Disposability

While the number of incidents of mobile phone theft may have declined over the last few years, the research suggests that the theft market for these devices is likely to remain fairly robust for two key reasons. First, many people change and upgrade their handset regularly, and markets with rapid turnover do not become 'saturated' as quickly as other products. Secondly, mobile phone technology is continually changing and handsets are becoming smaller while increasingly incorporating: MP3 players, video, Sat Nav, TV and other capabilities. This technology effectively keeps the price of the handset high.[12]

With such a robust theft market, the ease in which mobile phones can be disposed of makes them an attractive item to thieves. Stolen mobile phones are increasingly sold through second hand dealers or on online retail sites such as eBay and Gumtree to individual's wanting to buy a second hand phone. Currently the serial number of mobile devices does not need to be provided during the selling process, making it difficult to identify whether the handset has been stolen. Online retail stores do not support the secondary selling of stolen goods. Therefore to reduce the opportunity for thieves, one strategy would be to encourage sellers using online retail sites to list the serial number of the handset, enabling the item to be identified by the buyer and law enforcement.

Rebirthing

'Rebirthing' a mobile phone involves illegally modifying the phone's electronic serial number known as the IMEI number that unblocks the handset.[13] When a phone is reported lost or stolen, the phone service provider can bar the SIM card and block the IMEI number of the handset making the phone inoperable (IMEI handset blocking is discussed further in Section 5). Mobile phone thieves may then attempt to 'rebirth' the phone by unblocking it using software, which can modify the IMEI number, although this is becoming increasingly harder to do with newer devices.

Trafficking of mobile phones

We are currently not aware of this practice in Australia, however in the UK stolen phones are increasingly being trafficked to countries where unblocking is not illegal. Mobile handsets that are blocked in the UK can continue to be used overseas. The UK National Mobile Phone

[12] Mailley, J., Whitehead, S. & Farrell, G. (2006). 'Progress and Prospects in the Prevention of Mobile Phone Theft', *Justice of the Peace*, vol 170, p 404.

[13] ATMA. *Mobile Phone Industry Statement*, Australian Mobile Telecommunications Association. Available at http://www.amta.org.au/pages/amta/The.Mobile.Phone.Industry.Statement

Crime Unit (NMPCU) has uncovered cases of phones being stolen for export and according to the NMPCU, this has resulted in mobiles being used as a currency unto themselves, and are often being exchanged for drugs in a cashless transaction.[14] It would be valuable to find out whether this practice occurs in Australia.

Theft of information

As mobile phone handsets become more sophisticated, the issue of theft will become more important as handsets contain more and more sensitive information. If for example, the stolen phone can be resold not only for its value, but also for the information it contains, then the average value of the phone could increase significantly. In the next section, we examine in more detail mobile phone crime in the context of theft of information from the device.

Theft of information

Mobile devices have become the new personal computes, storing as much data as a PC but providing greater flexibility and portability. However, while smartphones now perform the same functions as a computer, one critical feature is missing – security. Rapid growth in the use of smart phones, with internet access along with the applications that allow users to bank, shop and social network, means that fraud risks (including theft of financial information and identity theft) which were previously associated with computers and laptops are becoming increasingly relevant to mobile handsets.

Prevalence

There is limited research in relation to the prevalence of mobile phone fraud however there appears to be a general understanding by technology experts and law enforcement agencies that there is a significant increase in threats towards these devices. For example, in April this year, Symantec released the findings of its Internet Security Threat report, which found 'attackers are exhibiting a notable shift in focus towards mobile devices',[15] and further cyber criminals are likely to develop even more threats targeting smart phones in the future.

Type of threats

While there are a variety of threats that can affect mobile devices, the following is a summary of the two most common; malware and smishing (short for SMS phishing). According to recent research, both threats are increasing in prevalence and sophistication.[16]

Malware

Malware is software that is designed to engage in malicious behaviour on a device and is currently regarded as the greatest threat to mobile phones.[17] Malware can commonly perform actions without a user's knowledge such as making changes to the user's phone bill,

---

[14] Anonymous (2007) 'Why do thieves still steal mobile phones?', BBC News, 30 October, Available at http://news.bbc.co.uk/2/hi/uk_news/7064192.stm

[15] Symantec (2011). *Internet Security Threat Report, Volume 16*, Symantec, Available at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_16

[16] Lookout Mobile Security. *Top 10 Mobile Banking Security Tips*, Lookout Mobile Security, Available at https://www.mylookout.com/mobile-banking-security

[17] Internet Fraud Watchdog. (2011). *Report on Mobile Phone Crime and Current Threats*. Internet Fraud Watchdog, Sydney.

sending unsolicited messages to the user's contact list, or giving an attacker remote control of the device. Malware can also be used to steal personal information from a mobile device. Currently much of the malware designed for mobile devices requires the user to download or install the software, but according to recent research, future mobile exploits will allow automatic malware installation.[18]

Mobile phones can be infected with malware through an open bluetooth connection, short messaging service (SMS), multimedia messaging service (MMS) and downloadable applications. According to the research there is a relationship between market share and mobile malware. Until recently, the Symbian platform, which is the operating system for Nokia smartphones, was the most popular platform for mobile malware. However as Google Android devices have increased in popularity, coupled with the rapid development and distribution of downloadable applications, this platform has also become a prime target.

Applications

Applications distributed through 'app stores' currently pose the greatest malware risk to all mobile operating systems and according to the experts, will continue to do so in the future.[19] While created as a means to distribute applications to mobile phone users, app stores provide an ideal transport mechanism for the delivery of malicious software to high volumes of mobile devices.[20]

Mobile operating system developers manage app stores. They include the Apple App Store, Android Market, Windows Marketplace for Mobile, Blackberry App World, or Nokia's Ovi Store; by known third- party organisations such as Amazon.com or by unknown third party companies. However the way apps are set up and their relative lack of safeguards makes them soft targets for hackers. Furthermore, the companies that maintain the app stores make no guarantees about the safety or quality of the apps. Users download apps and install them at their own risk.

For example, the Google Android platform has seen a 400 per cent increase in malware designed to steal user data since June 2010. This is due to Google's relaxed vetting process where anyone can anonymously create and distribute malicious applications. On the other hand, the Apple IOS platform has been largely resistant to attacks due to its more stringent vetting process. Each app author must be Apple approved and the company checks each application for malicious software prior to placing it in their app store.[21]

Smishing

Another common threat to mobile phone devices is SMiShing. The terms refers to a security attack in which the user is sent an SMS posing as a legitimate service that tricks them into divulging personal information or downloading a virus. For example, a text message may be sent claiming that the recipient's bank account had been blocked and then asks for confirmation of the account details so that a new card could be sent out.

---

[18] McAfee 2011, *McAfeeThreats Report: First Quarter 2011*, McAfee: Australia.

[19] Juniper Networks. (2011). *Malicious Mobile Threats Report 2010/2011*, Juniper Networks. Available at http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

[20] ibid

[21] Apple's security model for applications does not apply to 'jail-broken' phones. Jailbroken devices have been intentionally hacked by their owner's to allow them access to apps from sources other than the Apple app store.

Attackers often use email, texts and social networking sites to send links to phishing sites. Research indicates that as more people access sensitive accounts and services from their mobile devices, we can expect to see an increase in phishing attacks launched from malware on devices.[22]

Contactless mobile phone payments and online banking

Responding to mobile threats such as malware and smishing is increasingly becoming important as consumers begin to shift their banking online. By April 2010, 40 per cent of Australian mobile phone users accessed the Internet through their phone with almost half of these users conducting banking. However, with the implementation of banking apps by some of the major banks, it is expected that this number will continue to increase.[23]

An example of a recent mobile phone banking app developed by the Commonwealth Bank is '*Kaching*'. The app, which is currently only available to iPhone users, allows consumers to make payments to their friends using only their mobile number, email and Facebook, while it also allows payments to retailers through Mastercard PayPass contactless technology. Similarly, Google is currently field-testing *Google Wallet*, a mobile application for Android devices, which is advertised as 'Make Your Phone Your Wallet'.

The app will allow users to store virtual versions of their plastic cards on their handsets and allow for contactless payments at retail outlets.

With the obvious need to protect banking information on a mobile device, security measures are in place to reduce the opportunity for cyber criminals to steal data. In the case of Google Wallet for example, security measures such as PIN codes and encrypted payment card data have been implemented into the design. However, as previously discussed in the case of Google Android apps, cyber criminals have already commenced infecting mobile devices with malware, and experts believe that as more consumers shift towards mobile banking, so will the thieves.

Prevention efforts around mobile phone payments have already commenced in the United Kingdom. The UK Cards Association and mobile phone industry have together developed a preliminary list of best- practice guidelines for their respective industries. This was in response to Government and law enforcement concerns around a possible crime spike from the introduction of contactless payments on mobile phones. Given the technology is still relatively new to Australian consumers, it would seem that we are in a prime position to also develop industry guidelines around contactless payment using mobile phones.

Offenders and technology

As an emerging crime with limited information, we are currently not aware of who commits mobile phone fraud. In the US, researchers have demonstrated the reasonable ease to creating malicious software using off-the-shelf tools and a simple background in computer programming to infect mobile devices.[24] Further, over the past decade, cyber crime has

---

[22] Lookout Mobile Security. *Top 10 Mobile Banking Security Tips*, Lookout Mobile Security. Available at https://www.mylookout.com/mobile-banking-security

[23] Australian and New Zealand (ANZ), St George and Commonwealth Bank all have mobile banking apps.

[24] Mahoney W, R & Pokorny CA, 2009,'Do-It-Yourself Guide to Cell Phone Malware', *International Journal of Computer Science and Network Security*, vol.9 No.1.

changed from the cyber smart hacker into an organised trans-national crime committed for vast profit. A sophisticated underground economy provides the IT tools to commit these crimes and the market for stolen identities and financial information.[25] Further information in regard to cyber criminals can be found in the Plastic Card Fraud background paper.

Security features on mobile phone devices

With the increase in mobile phone fraud threats, handset developers and software companies consider a range of hardware and software strategies that will aid mobile phone users in keeping their phone and personal information safe.

Hardware

Mobile phones already have a security features built in that, if activated, require certain knowledge to be used.

- The SIM PIN code which locks the SIM card. There is often a default PIN code set by the service provider, which can be changed by the user. If the incorrect PIN unlock code is entered too many times, the SIM will become permanently disabled. Note however that this lock does not stop the handset being used with a new SIM card.
- The phone security code, which locks the handset itself. Again default codes are preset and can be changed by the user. If the incorrect PIN security code is entered too many times, the handset will lock up. The user must then contact the network provider to obtain a master reset code.

The effectiveness of security features such as PIN codes can be limited for two reasons. First, it requires the user to activate the security features on their mobile handset to be effective and currently we are not aware of how often this happens. Secondly, the security features of a phone can be unlocked by a number of third-party retailers who offer this service and do not require any legitimate paperwork.

Software

A number of software companies have developed anti-malware software for mobile phone devices to reduce the opportunity for theft of information from the device from malware and phishing scams. One example is *Norton Mobile Security*, developed to provide mobile users the same level of security that has become standard for laptops and computers. The product features anti-virus technology as well as firewall and antispam for SMS.

In addition, manufactures and software companies have developed phone-finder technology using GPS in the event a phone is lost or stolen. For example, Apple released *Find My iPhone*, a free service that allows iPhone users to remotely locate their lost or stolen mobile phone using the iPhone's GPS. Find My iPhone pinpoints the iPhone's current location using Google Maps and lets owners send and display a message on the iPhone even if it's locked, presumably to provide information on how to return the phone to the finder of the phone. In the event a phone is lost or stolen, it also allows users to either remotely set a password lock or wipe the contents of the phone. The service can also force the iPhone to play a sound for two minutes to get the attention of the owner in the event the device is lost.

[25] *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime: The Report of the Inquiry into Cyber Crime*, House of Representatives, Standing Committee on Communications, June 2010.

Currently, mobile phone software security is regarded as one of the most effective methods to protect information stored on mobile phone devices, and to also help locate lost or stolen devices. However there has been minimal uptake of software security by consumers, with a UK study showing only six per cent of users had installed an anti-virus program on their mobile phone (we are currently not aware of the uptake in Australia). While device-integrated security would be the most the most effective way to protect handsets, increasing consumer education about this issue may also prompt users to install additional security on their devices.

Government solutions

The Australian Government, Australian Mobile Telecommunications Association (AMTA), and State and Territory police services have implemented a range of initiatives under the 'Mind Your Mobile' campaign to reduce the incidence of loss or theft of mobile phones.

The 'Mind Your Mobile' campaign is a joint initiative of the industry and law enforcement agencies to reduce mobile phone theft. The campaign has three key elements.

International Mobile Equipment Identity (IMEI)

Industry-wide handset blocking (using the IMEI number) completed in March 2003, stops stolen phone handsets from being used on any network in Australia. Each mobile phone has an IMEI number which is a 15 digit number, which can be found underneath the battery of a GSM phone or by dialling *#06# on a GSM keypad. Blocking the IMEI number means that regardless of whether a new SIM card is placed in the blocked handset or not it will continue to be inoperable. Australia's GSM network providers – Optus, Telstra and Vodafone – agreed, in 2003, to send a list of lost, stolen or found mobile phones to each other every day so the identified mobile phones can be blocked or unblocked on all digital networks within 36 hours.[26]

In the first four years of the program, AMTA saw a 30 per cent reduction in the number of handsets blocked annually across Australia. In the past two years the number has stabilised at 125,000 blocks per year. Approximately 50,000 phones per year are unblocked at the request of the owner because they have been returned. The AMTA also provides an online service where second hand consumers or sellers can check if the phone has been reported lost or stolen and therefore been blocked from use by the network carriers.

Public awareness

A public awareness campaign via the website www.mindyourmobile.com to increase consumer awareness of the practical steps users can take to prevent theft such as keeping your phone on you when out, using PIN code security, backing up your personal information on a computer, and the importance of notifying your carrier to request an IMEI block.

Legislation

A partnership with the Federal Government to introduce legislation that made altering a mobile phone's IMEI number, or using a tampered phone, a criminal offence under the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004*. The penalty is up to two years.

[26] AMTA, *Mobile Phone Industry Statement*, Australian Mobile Telecommunications Association. Available at http://www.amta.org.au/pages/amta/The.Mobile.Phone.Industry.Statement

International mobile phone theft interventions

United Kingdom

The United Kingdom have been leading the way in combating mobile phone theft. In 2006 the Mobile Industry Crime Action Forum (MICAF), which included mobile network operators, UK retailers, and some handset manufacturers, developed the Mobile Phone Industry Crime Reduction Charter. The Charter documented the future commitment of the mobile phone industry to work in collaboration with law enforcement agencies and the Home Office. Some of their crime reduction strategies are discussed below.[27]

International Mobile Equipment Identity (IMEI)

The UK was the first country in the world to have all mobile phone carriers implementing IMEI blocking and sharing their blocked phone databases, followed by Australia. The MICAF charter agreed to a timeframe for blocking an IMEI number on all UK Networks once the handset had been reported to the Network. MICAF reported that within 24 hours a reported stolen mobile phone in the UK is blocked by its network provider for use on that network, and within 48 hours 90 per cent are blocked from every network in the country. Blocking, and other measures, is credited by MICAF for 20 per cent drop in mobile phone theft however even though it is a criminal offence phones can still be unblocked. Offenders can unblock a phone by changing the IMEI number using hardware and software, although this is a difficult process.

Immobilise system

Immobilise is the world's largest free register of possession ownership details which is used to help reduce crime and repatriate recovered personal property to its rightful owners. The register allows members of the public and businesses to register their valued possessions or company assets as well as to report lost or stolen property. All the registered details are viewable on the Police national property database and are then used by the police to trace owners of lost and stolen property.

The Immobilise system has been in operation in the United Kingdom for over eight years and was set up with the support of the Police, mobile phone industry and central government. Immobilise is used by over 22 million members of the public and businesses. As a direct result of Immobilise there are over 250 cases a week, in the UK, where property is returned or information collected that assists the Police in investigating criminal activity involving stolen goods.[28]

The Immobilise system is operated by an agency that also runs the police reporting systems. Funding for Immobilise is supplemented through on site advertising as well as revenue derived from sales of possession marking products that are available via the website and several retail outlets.

[27] Mobile Phone Industry Crime Reduction Charter, Mobile Industry Crime Action Form, July 2006.
[28] Immobilise National Property Register. Available at http://www.immobilise.com/about.html

Education

MICAF in the UK established a specialist-marketing group, to develop an agreed programme of activity to raise awareness of:

- mobile phone theft
- the industry's ability to block stolen phones
- the ability to register mobile phone ownership on the Immobilise database.

MICAF also focused on training and information to call centre and mobile phone retail sales floor staff about crime reduction.