Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions

Nicola Davinson[a] & Elizabeth Sillence[b]

[a] Psychology Department, University of Sunderland, Sunderland, SR6 0DD, UK
[b] PACT Lab, Department of Psychology, Faculty of Health and Life Sciences, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK

Author for correspondence
Nicola Davinson
Psychology Department, University of Sunderland, Sunderland, SR6 0DD, UK
Telephone + 44 191 515 2618
Fax + 44 191 515 2781
Email nicola.davinson@sunderland.ac.uk

Abstract

Fraudulent transactions occurring via the Internet or Automatic Teller Machines (ATMs) present a considerable problem for financial institutions and consumers alike. Whilst a number of technological improvements have helped reduce the likelihood of security breaches, users themselves have an integral role to play in reducing technology mediated fraud. This paper focuses on the role of the user, specifically capturing information about their perceptions and behaviour when using technology to complete financial transactions. Semi-structured interviews with twenty-nine participants were conducted to increase knowledge and understanding in this domain. The findings are guided by the components of the Health Belief Model (HBM) which is used as a framework for exploring critical issues associated with behavioural change. Results indicate that users typically felt safe and secure whilst conducting financial transactions online and at the ATM. The users' perceived level of threat was low mainly because they thought it unlikely that they would be a victim of fraud and because of a reduced sense of responsibility for any negative outcomes. Whilst users were aware at a superficial level of what fraudulent activities take place they were less sure about behaviours designed to counteract fraud and their potential efficacy. Furthermore, security concerns among ATM users were not as high as concerns among Internet users with Internet users appearing to take more individual responsibility for their more personal technologies in more private spaces. The paper concludes with some practical implications based around the HBM suggesting user focused ways forward for encouraging secure behaviour.

Keywords: Security perceptions, behaviour change, Internet, ATM, technology mediated communication, Health Belief Model

1. Introduction

Millions of financial transactions are conducted every day through technology as users interact with the Internet and Automated Teller Machines (ATMs). The convenience and efficiency these technologies provide is countered by the novel and unique methods available to defraud the user through the very same technology.

Until recently attention has focussed on technological improvements and interventions as a way of countering fraud and reducing the likelihood of security breaches. This however, has led to a situation in which technology constantly has to react to the changing nature of fraudulent activity. The introduction of Chip and PIN or EMV cards has succeeded in reducing fraud via lost and stolen cards but at the same time has led to an increase in card-not-present fraud(UK Cards Association, 2011). In response, the banking industry has introduced additional technological countermeasures including 3-D secure commonly known by its brand names Verified by Visa and MastercardSecurecode, however this technology is also not without issues (see Murdoch & Anderson, 2010 for a discussion).Other potential technologies for fraud reduction include biometric authentication and improved Internet protection software. However, there remains a degree of uncertainty surrounding the motivation for technology related countermeasures with some researchers suggesting that the banking industry's aim to shift liability onto its consumers is the key driver of these advancements (Bohm et al, 2000; Murdoch et al, 2010). Despite this there is some agreement that users themselves are an important and often neglected factor in improving security behaviour where financial transactions are concerned. Users have previously been labelled the "weakest link in the security chain," Schneier (2000) highlighting the importance of taking user issues into consideration. Similarly, Sasse et al (2001) discuss transforming the 'weakest link' in the security chain in a process where designers and security professionals move away from simply blaming users for insecure behaviours and move towards identifying these behaviours and designing effective systems accordingly. Consequently there is a growing move towards a more user-centred approach to reducing fraud which has seen, inter alia, the introduction of ATM best practice guidelines and warnings, online visual security cues as well as research into the cognitive, social and cultural issues associated with different user populations in relation to financial transactions (De Angeli et al., 2004; Liu et al, 2007).

Given the prevalence of fraudulent activity, relatively little is known about users' security awareness or the security behaviours they employ when they use technology to complete financial transactions, this is particularly apparent in relation to ATM use. In addition there is no clear way of mapping this information onto actual security issues so that practical suggestions for improving secure behaviour can be made. In this paper then we propose using the Health Belief Model (HBM) (Rosenstock, 1974) as a way of understanding users' attitudes and behaviour in this context. This will extend our current limited knowledge of Internet based security behaviours and for the first time provide a way of mapping ATM users' knowledge and perceptions onto a behaviour change model. Understanding the factors associated with secure behaviour use in relation to the Internet and ATMs allows a clearer picture of users' understanding of their role in fraud and security and allows us to generate a

number of practical implications based on the behaviour change literature. The rest of the paper is organised as follows. Firstly we present an overview of the nature and scale of the fraud problem with respect to the two technologies. We highlight the fact relatively little is currently known about users' perceptions, and present an overview of the banks' position with regard to fraud and liability. We document the existing user centred approaches to fraud, highlighting issues of authentication and usability. Secondly we present our empirical work based on interviews designed to elicit detailed information about the users' perspectives and practices in relation to ATM and Internet use. Finally we discuss the implications of these results in relation to the HBM and make a number of practical suggestions for improving practices in relation to the literature on behaviour change.

1.1 Background

Both ATMs and the Internet offer the user convenience, flexibility and a sense of control when carrying out financial transactions. ATMs allow users to withdraw cash, and perform a variety of other transactions, at a range of locations both during and outside normal bank opening hours(Payments Council, 2010).Likewise, the Internet allows users to bank or shop 24 hours a day from the convenience of their own home. As vehicles for financial transactions, however, ATMs and the Internet are both susceptible to misuse and abuse. Despite their similarities in terms of access and convenience the two differ in a number of distinct ways including longevity and familiarity, location of use and the threat types to which they are vulnerable. This section introduces the technologies in relation to secure behaviour. It also examines the relevant types of fraud and their prevalence rates, usage statistics and the threat in relation to banking industry policy.

Over the last forty years users have become familiar with the functional design of the ATM as well as its operating procedures. ATMs are predominantly used to complete financial transactions, with the Payments Council indicating 85% of all cash acquired by individuals occurred via an ATM in 2009 (Payments Council, 2010). Importantly, any transaction conducted at an ATM requires the user to insert his/her card and enter the correct PIN, and it is the disclosure of such information that has the potential to incur fraudulent activity.

ATM security can be broadly considered in three categories which consist of physical attacks, ATM fraud, and software and network attacks (GRGBanking, 2011). Early ATM security was concerned with preventing physical attacks on the actual machines. ATMs were broken into and attempts were made to steal entire machines, or they were sealed with silicon and broken open using explosives. These types of attacks are now countered with dye markers or smoke canisters which deny the thief the money inside the machine by rendering the cash unusable if opened by force (Curran & King, 2008). Security of ATMs has now moved on to consider threat via technology, which is much more subtle and increasingly difficult to detect as opposed to its physical counterpart. Software and network attacks have occurred more recently, with the first known malware attack on an ATM in 2008 (TrustwaveSpiderlabs, 2009). Such attacks focus on the ATM network and its bespoke applications rather than attacking the ATM user, and as such are beyond the scope of this paper. More traditional

ATM fraud is targeted at user behaviour, with criminals employing a number of different methods in order to obtain cash, or more typically obtain card and/or PIN details fraudulently from an ATM user. GRGBanking (2011) outline the common types of ATM fraud which are described below:

1. Card-trapping – A device is placed on the card reader that traps the card. When the user leaves the ATM the criminal will remove the device and obtain the card. Even if the user attempts to 'Cancel' the transaction, the criminal can still obtain the card and use it in conjunction with another type of attack, such as PIN capture or card-not-present fraud.

2. Skimming – Typically, illegal devices are attached to the card-reader that enables the criminal to record the data from the magnetic stripe. The user's PIN is recorded either by shoulder surfing, by using a hidden camera, or keypad logger. They then reproduce the card and use it to withdraw cash from the user's account. To note, skimming was reported as the top global threat for ATMs in 2012 (ATMIA, 2012).

3. PIN capture – This technique is typically used in conjunction with another technique such as card-trapping or skimming. It can be achieved by shoulder surfing which involves the criminal observing the user input their PIN and subsequently acquiring their card, which can include distraction and pick pocketing. Hidden cameras can also be attached to machine or surrounding area which observes PIN entry or keypad loggers can be attached to the keypad of the ATM which records the entry of the PIN.

4. Cardholder-Not-Present (CNP) – CNP fraud typically occurs when a card is fraudulently obtained and then used over the telephone or Internet where a PIN is not required.

In terms of prevalence, the European Central Bank (ECB; 2012) report fraud statistics for all European countries in the single euro payments area (SEPA) which includes all EU member states as well as Switzerland, Iceland, Liechtenstein and Norway. In 2010 card fraud totalled €1.26 billion, which represents 0.04% of the value all card transactions and 16% of this fraud occurs at an ATM. On average this amounts to €1.73 lost for every card that is issued, which is greater than the average transaction value. ECB (2012) also report fraud figures in relation to transaction volume, which indicates 1.2% of all cards issued were affected by fraud and represents 0.018% of transactions in 2010, with 31% of this occurring via ATM. Further to this, ECB (2012) report a comparison of fraud volumes with fraud values which reveals that ATM fraud involves larger losses per transaction than any other transaction channel (e.g., POS or CNP).

The UKCA (2012) states the total losses due to plastic card fraud in the UK for 2011 to be £341 million, which is a dramatic decrease of 52% from 2008 where losses peaked at £609.9 million. Fraud losses in relation to total turnover have also fallen considerably since 2008 and now represent 0.061% in 2011. More recently fraudulent attacks have targeted outlets

where the card is not required to complete the transaction, with a considerable 65% of losses accounted for by card-not-present fraud, in contrast to counterfeit fraud which now only accounts for 11% of all losses.

A survey by CPP (January 2011) indicated that 13 million people in the UK have now fallen victim to card fraud with one-third of them not being aware of the attack until being informed by their bank. Seven per cent of people in the survey also reported suffering from card fraud in the last 12 months down from 10% in the previous year. The same survey also indicates a number of geographical hotspots for fraudulent attacks, with Brighton, London and Manchester topping the list in the UK. Overall, the UK has a greater proportion of card fraud victims than most other major countries, with only China having a greater proportion (ACI Worldwide, February, 2011).

To put these figures into perspective 30 million people use ATMs every month in the UK (PayPoint, 2013) and in January 2013 239 million transactions were made via the LINK ATM network (Link, 2013). Given the high levels of ATM usage worldwide it is perhaps not that surprising that people report being relatively unconcerned about ATM security.A2006 survey suggested that 19% of ATM users indicated they were not concerned about security when using an ATM and 68% would continue to use ATMs as they normally would despite being aware of the possibility of fraud (NCR, 2006). However, a more recent survey suggests bank card fraud is the number one security concern among respondents, closely followed by identity theft (Unisys Security Index, 2011). This increased concern may be related to a shift in liability as the banking industry attempts to move responsibility for fraud and security onto consumers (see Murdoch, 2013). If the bank can show that a customer has been 'grossly negligent' (a term the bank is free to define themselves) then the full liability shifts to the consumer. Gross negligence may range from failing to take all available steps to keep the card and the PIN safe at all times; to a more recent edict that customers must have different PINs for separate cards (Lewis, 2012). As banks continue to shift liability onto consumers it becomes increasingly timely to investigate users understanding of security, threat and responsibility in respect to their financial transactions.

Defrauding the user *online* takes a number of different forms with some being more amenable to secure user intervention than others. Whilst malware and spyware infiltrate the user's system collecting the user's data relatively unobtrusively to some extent these attacks happen behind the scenes/in the background and require less active user involvement at the point of attack. By comparison phishing attacks play on user's involvement with websites often relying on their familiarity with a particular website in order to spoof it, thus the importance of the user in relation to secure behaviour is paramount in this kind of attack. Relatively less is known about secure user behaviour in relation to phishing attacks, which some research focusing on phishing toolbars (Zhang et al., 2007) however; again this allows the user to pass responsibility to a technology-based countermeasure. It is already known that users will ignore warnings given to them by such toolbars (Wu et al., 2006) and therefore the actual user behaviour remains central to the issue of fraud prevention.

Phishing attacks typically occur with emails and websites that fraudulently mimic legitimate organisations in attempt to harvest personal and financial information from the user. In the past 10 years phishing methods have become much more prevalent and sophisticated and Abad (2005) indicates that phishing attacks are rarely committed by a single individual but usually by a number of people who specialize in different techniques. The UK Cards Association (2011) report total losses associated with online banking fraud of £46.7m in 2010, a decrease of 22% since 2009. Online banking fraud typically arises from scams including spyware and phishing attacks. The Anti-Phishing Working Group (APWG) reports on phishing activity trends, and the December 2010 report indicates financial services are targets for 55.1% of all phishing attacks, with payment services accounting for a further 24.9%. Further to this, the Internet accounts for 59% of all CNP-based fraud and a 2010 international survey suggests 10% of people polled had been victims of online scams, 9% taken in by phishing and 7% subject to online credit card fraud (Norton, 2010). In the UK the number of people reporting having had their credit card details stolen online has increased threefold during the period 2003-2009, from less than one percent to over three percent, and in the year 2009 20% of survey respondents reported having been asked to provide their banking details to non-banking websites (Blank& Dutton, 2011).

Again, to put this in context, over half the UK population now bank online (UKCA, November 2012) and many report in surveys feeling confident about doing so. It is also reported that 836 million card payments were made online in 2011, which represents £63 billion spent via plastic cards in this domain (UKCA, 2011). When trying to understand users attitudes and behaviour with respect to security practices researchers have attempted to describe the kinds of mental models that users hold about different computer security risks. Wash (2010) suggests that users hold inaccurate mental models or folk models of computer security. These mental models may differ from security experts' mental models so that experts may think of password loss as resulting from more malicious activities whilst non experts perceive password loss as closer to the risk of a naive or innocent loss of a key (Camp, 2009). Wash (2010) also suggests that many users attempt to avoid security decisions altogether choosing to pass the responsibility for security to some external entity. This could mean shifting the responsibility onto a technological entity such as a firewall or virus protection software, a social entity i.e. another person or IT technician, or another institution such as the bank.

Nevertheless, the literature on e-commerce suggests that security concerns are the most common factor affecting adoption of online banking (Booz et al, 1997; Daniel, 1999; O'Connell, 1996; Sathye, 1999). Security concerns remain important for existing users of online banking services. The Gartner Group (Litan, 2005) found 28% of online banking users indicated their banking online was influenced by online attacks, with 4% of users no longer paying bills online and 1% refusing to use online banking again. Similarly, the adoption of online shopping appears to be predominantly affected by issues of security and privacy of information with such concerns playing a major role in the consumer's willingness to purchase goods online (Culnan, 1999; Federal Trade Commission (FTC) 1998b, 2000).

Despite frequent references to the importance of security concerns, these concerns do not always translate into actual behaviour and may not be sufficient to inhibit technology mediated financial transactions. We know, for example, that users will put their concerns aside if the benefits of using the Internet are made pertinent (Spiekermann et al, 2001). This can lead to insecure behaviour which leaves the user open to fraudulent attacks. There have been a number of studies investigating the dichotomy between attitudes and behaviour towards security online (Acquisti, 2004; Acquisti & Grossklags, 2003; Shostack, 2003). A number of explanations have emerged, including a lack of information about the problems and countermeasures, and low privacy sensitivities. Any future research needs to consider the factors which can contribute to the adoption of secure behaviour which are more carefully matched to the security concerns that are expressed.

Considering the two technologies side by side there are some notable differences with respect to fraudulent activity. Firstly, the location of the technology itself means that for ATM users, predominantly accessing banking services in public spaces, the issue of safety is more tangible with users on their guard against observation,- shoulder surfing and even physical attack (Goucher, 2008; Keizer, 2005).In contrast, the Internet is typically accessed from a private or, at least, personal space on a personal computer within a domestic environment, thus affording the user more time to carefully consider their transactions. Being in one's own home may however confer a false sense of security allowing the user to feel unduly 'safe' and potentially act in a less than secure manner online. Finally, the timing or sense of immediacy surrounding the threat varies between the two technologies.ATM fraud can occur regardless of whether or not the victim completes the transaction. The victim's details can be illegally harvested as soon as they have entered their card and PIN. Whilst Internet fraud can also occur with minimal user interaction (e.g., malware or spyware attacked) it is also possible for a fraudulent attack to only be rendered successful once the user has completed the online transaction and disclosed login details and/or financial information (e.g., in the case of phishing attacks).This means that in some instances, there are potentially more opportunities for the Internet user to spot fraudulent signs and behave in a vigilant, proactive manner with regard to security as the transaction progresses. In contrast, the ATM user often has to act retrospectively in response to fraud.

1.2 The problem of security from a user perspective

As previously discussed approaching the problem of security from a purely technological standpoint misses the importance of the user in the security chain. Technology designed without thought to the user's cognitive, social and cultural understandings is likely to fail in its objectives and increase the likelihood of users acting insecurely. The growing recognition of the importance of taking a user perspective on security can be seen within a number of areas of ATM research. These include the design of navigation menus (Curran & King, 2008), improved usability and user experience (Camilli et al, 2011), user's perceived physical privacy (Little, 2003; Little et al, 2005), and authentication mechanisms (e.g., De Luca et al., 2010; Renaud & De Angeli, 2004). The issue of authentication has received considerable attention in recent years. ATMs use a combination of token-based and knowledge-based

authentication, with a plastic card required to satisfy token-based authentication and personal identification via PIN to satisfy knowledge-based authentication. Knowledge-based authentication has come under scrutiny due to the cognitive load imposed upon users to remember and recall any number of PINs and passwords which can be easily forgotten (Renaud & De Angeli, 2004). This leads users to manage their PINs and passwords negligently (Proctor et al., 2002), typically using simple words or biographical information, or using the same password for multiple accounts (Ives et al., 2004). Furthermore, Cheswick and Bellovin (1994) suggest weak passwords are the most common cause of security breaches. This may be due to lack of awareness relating to good practice for secure PIN and passwords, alternatively it may be due to the usability-security trade-off that often exists and has been investigated in the literature (Chiasson et al, 2007; Sasse et al, 2001; Yan et al, 2004). Alternatives to PINs and passwords have been proposed as a way of increasing the security of the ATM authentication process. These have centred on biometric measures as a technological solution to the authentication of individuals (Coventry, 2005). Biometric measures include fingerprinting and iris, retina and voice recognition. In user studies participants favoured iris verification over PIN believing it would be more secure, more reliable and faster (Coventry et al, 2003), although concerns over privacy persist (Coventry, 2005).

Improving authentication techniques may assist genuine users to gain legitimate access to the ATM whilst improved designs in terms of accessibility and privacy may encourage use and satisfaction. These steps alone, however, fall short of protecting users against security threats in the form of skimming and any subsequent card not present fraud. Understanding more about users' perceptions of the security risks surrounding ATM use and their subsequent behaviour (secure or otherwise) is a first step towards designing for improved secure behaviour. There are a number of strategies a user can employ to help reduce the threat of fraud when using an ATM, such as protecting PIN entry and checking the exterior of the ATM before use, as suggested by a number of 'best practice' guidelines (e.g., LINK; Safecard; Financial Fraud Action UK).

User centred issues are also apparent when considering the problem of Internet related security. Hu and Dinev (2005) indicate evidence to suggest that people avoid using protective, anti-spyware software due to issues surrounding its perceived ease of use and perceived control. There are a number of best practice guidelines for financial transactions online, such as ensuring the PC is protected using anti-virus and firewall software, and assessing the credibility of websites using visual indicators such as the padlock security icon and web address (e.g., Financial Fraud Action UK; getsafeonline.org). Similarly, security toolbars have been developed (e.g., SpoofGuard toolbar; Chou, et al., 2004) that aim to identify phishing websites. However it is noted that users can still be fooled by attacks when they implement the security toolbars and even ignore the warnings such toolbars provide (Wu, et al., 2006). More recently Murdoch & Anderson, (2010) have noted that technological solutions to card-not-present fraud such as 3Dsecure actually undermine the users own security practices and training by forcing them to enter sensitive details on a third party site. This further highlights the importance of considering user behaviour as a primary

concern, whether it be for the purpose of understanding how we can motivate users to adopt protective technologies (Dinev et al, 2009) or for the purpose of understanding how we can motivate users to behave more securely without relying so heavily on technological countermeasures, such as Chip and PIN or protective software technologies.

From a bank perspective there are inevitable costs associated with insecure user behaviour. However, Myers (2007) explains that the costs of phishing are not simply the direct losses associated with the crime, but also the indirect and opportunity costs that are incurred. Indirect costs are those which do not arise from stolen money or goods but are incurred from dealing with the problem, such as call centre costs and customer service. For example one of the top 20 banks in the U.S. is reported to have fielded 90,000 phone calls per hour for five hours following a phishing incident in February 2004 (Krebsbach, 2004). These indirect costs are not only associated with staffing time and costs but also branding. The Anti Phishing Working Group (APWG) estimates that $100,000 to $150,000 is lost in brand devaluation per attack. Another cost to banking organisations manifests in lack of trust or apprehension of adoption a user may exhibit following a fraudulent attack. The Gartner Group (Litan, 2005) survey indicates online banking user interaction is affected by known fraudulent attacks.

It is possible that some of these costs can be offset by the benefits obtained by widespread use of technology for banking transactions, which provides a self service driven system that does not have to be staffed at a physical outlet and can be more profitable for the banking industry (Christoslav et al., 2003). It is also possible that such costs can also be reduced by the shift of liability onto the consumer that will reduce direct costs of fraud (Murdoch et al., 2010), but are unlikely to reduce the indirect costs noted. Therefore, it is not surprising that financial institutions have invested in technological countermeasures that can help to reduce fraud or shift liability in order to reduce their own costs.

In summary, despite the development of technological solutions to the problem of Internet and ATM fraud, the amount of money lost to these activities is still substantial, with considerable numbers of people still becoming victims of ATM/card and online financial fraud. The real threat of fraud and its mechanisms vary between the two technologies, as does the way in which people engage with the technologies in terms of location and the sense of public and private use. The ultimate aim is to explore users' attitudes towards secure behaviour and understand factors which might support or discourage users from engaging in secure practices across the two technologies. Drawing on the behaviour change literature within health psychology, the HBM provides us with a framework for exploring these factors with a view to supporting secure behaviour.

1.3 Using the health belief model as a way of understanding users' financial security behaviour

The HBM is a psychological model that attempts to explain and predict health behaviours. The original model (Rosenstock, 1974) was based on four constructs: perceived susceptibility, perceived severity, perceived benefits, and perceived barriers. These concepts

were proposed as accounting for people's "readiness to act." In more recent versions of the model the concept, cues to action, has been added with the notion that cues would activate that readiness and stimulate overt behaviour. Another recent addition to the HBM is the concept of perceived control which is a measure of level of self-efficacy, or one's confidence in the ability to successfully perform an action. Although devised to examine behaviour change within a health setting (see for example, alcohol use [Minugh et al, 1998; Von et al, 2004], smoking [Von et al, 2004], drug use [Bonar & Rosenberg, 2011; Welch, 2000], exercise [James et al, 2012; Wouters et al, 2009] and medical screening behaviours [Austin et al, 2002; Yarbrough & Braden, 2008]),the model is flexible enough to usefully explore different domains and table 1 demonstrates how the HBM can be considered within a financial security context.

In recent years researchers from a wide variety of domains have been adopting and modifying behaviour change models rooted in health psychology such as protection motivation theory (PMT) (Rogers, 1975), implementation intentions (Gollwitzer 1999) and the HBM (Rosenstock, 1974)as a way of explaining and predicting behaviour in their respective areas. These include energy (Bell et al, in prep) and computer based security within workplaces (Ng et al, 2009) and Internet security (Davinson & Sillence, 2010). More specifically, Ng et al (2009) use the framework of the HBM to design a measure of secure user behaviour in a workplace setting and find perceived susceptibility, perceived benefits, and self-efficacy to be significant determinants of user behaviour in relation to email attachments. In addition, Davinson and Sillence (2010) consider the role of perceived susceptibility when developing interventions to promote secure behaviour in relation to phishing attacks.

Although the HBM has been used previously in relation to phishing (see for example Davinson & Sillence, 2010) this paper extends its application by firstly considering Internet use in broader everyday terms and secondly by considering its suitability in the context of ATM use. To our knowledge this is the first paper of its kind to focus on ATM user security perceptions in relation to this model of behaviour change. The review above indicates a number of differences between ATMs and the Internet in relation to security behaviour and a further aim of this study is to examine whether or not the HBM allows these differences to be categorised in relation to potential behaviour change strategies.

TABLE 1 ABOUT HERE

Overall aims and approach

The broad aim of the study is to contribute to our understanding of users' awareness of, and behaviour towards, financial security. More specifically, the study aims to evaluate an appropriate framework, based on the HBM constructs, for addressing the issue of technology-mediated fraud from a user perspective. The study also aims to determine whether this framework is appropriate to investigate user behaviour for both ATM and Internet technologies. It is expected that an understanding of these issues will identify the key areas for improvement and inform behaviour change strategies. To this end a series of semi-structured interviews were carried out with ATM and Internet users. The aim is to unpack the

issues associated with secure behaviour in both domains through an analysis that is driven by the factors of the HBM.

2. Method

Interview design and procedure

The semi-structured interviews focussed on how the user interacts with technology to complete financial transactions as well as user knowledge of security issues and associated risks. Questions included: What are you concerned about when using technology to complete your financial transactions? How do you alleviate any concerns you have? How do you think you will be affected if you became a victim of fraud? What measures do you think can be taken to prevent fraud?

Prompts and questions were used throughout the interview but participants were able to develop their own topics of conversation as appropriate. Participants were made aware that although there were a number of topics of interest to cover, it was perfectly acceptable to deviate from these questions and discuss anything else they felt was relevant. The interview was recorded using a digital mini disc player and the typical duration was between 30-45 minutes.

Participants

Twenty nine interviews were conducted, with fourteen females (mean age 51.9 years) and fifteen males (mean age 50.1 years) agreeing to take part. All participants were recruited from the Northumbria University, Psychology and Communication Technologies (PaCT) lab database. The PaCT lab database contains contact information for a range of potential participants from the general population, and is therefore not restricted to a University population sample. Letters were sent to 100 members of the database outlining the nature of the study and the inclusion criteria. All participants were required to have used ATMs and the Internet to complete financial transactions within the last six months. All participants lived in the North East of England, two participants were students, six were retired, and the remaining 21were in full or part time employment. All participants were compensated for their time and paid £10. In addition to the inclusion criteria, one participant also reported using telephone banking. Most participants used the ATM for cash transactions only and convenience was the most important factor in determining where to use an ATM. In terms of Internet use purchasing online was more common than online banking.

3. Findings and discussion

The data were managed using ATLAS.ti qualitative software and the analysis began with a thorough reading and re-reading of the transcripts. The coding process was guided by the main factors of the HBM although these codes were not used exclusively and the prevalence and importance of codes were still taken into account. Themes relating to the six main factors of the HBM were initially coded from the interviews: perceived susceptibility, perceived severity, perceived costs, perceived benefits, perceived control and cues to action.

Perceived susceptibility

Two main themes emerged in relation to perceived susceptibility; Perception of fraud prevalence and Personal susceptibility. Overall participants were aware that fraudulent activity takes place, and how it might happen and whilst not consistent on the prevalence rates they were all inclined to believe they were not particularly personally susceptible to fraudulent attacks.

Perception of fraud prevalence

In general, participants commented on how prevalent they believed fraudulent attacks to be, which in turn, may impact how susceptible they believe they are. Comments in relation to prevalence were quite mixed, with some users considering prevalence to be high:

"I know that it's on the increase, I've seen it on the news that it is one of the biggest causes and that's why the chip and PIN was supposed to have come about"

Whereas others were unsure or thought that fraud prevalence was low:

"I don't know, I really couldn't say how prevalent that was. I don't think it can be that much because people would be making a huge effort to stop it wouldn't they."

More specifically, two main types of risk emerged that participants were aware they could be susceptible to; these were risks associated with physical safety and risks associated with technology security.

Participants identified a risk to their physical safety when using an ATM in particular. This type of risk included their cash or card being stolen via physical attack, and also PIN vulnerability via shoulder surfing. Most commonly users referred to isolation and lack of privacy as being the catalyst for such risks. Comments relating to isolation indicate some users considered it risky to use an ATM at night, in quiet areas with low footfall, enclosed rather than open locations or in unfamiliar areas. For example:

"I wouldn't use an ATM late at night, in an unfamiliar area, and if I saw anyone around me that made me uncomfortable."

However, there appears to be a fine line between too few and too many people present when using an ATM. A few users said they would feel uncomfortable using an ATM if the environment felt too busy for example in a crowded high street. The aspect of privacy was also discussed in terms of entering PINs when purchasing goods from a retail outlet, for instance:

"I still think, I mean you're always in a queue usually aren't you, and you can't tell me there isn't somebody can look"

The term technology security is used to describe risks to personal finances or personal identity via technology, such as fraudulent attacks arising from ATM or Internet use. Comments regarding knowledge of risks to technology security occurred more than twice as frequently as comments regarding physical safety. However these comments did refer to both ATM and Internet use. Risks in relation to identity are commented upon much less than direct financial risks and most commonly refer to Internet use. Users appear to be aware of the risk towards their identity in the form of phishing emails or purchasing goods from dishonest websites, for example:

"I've, where I work we've had people use the Internet and answered spam emails in error and basically handed their details over."

Risks to finances via the Internet are generally noted as being due to illegitimate websites and completing purchases on websites that are not secure. Financial risks via the ATM are recognised as being due to ATM tampering e.g. the use of skimming devices and false fascias, for example:

"People who actually put a false front on the machines and therefore they read the card number and they can also record your PIN number so therefore they can go and use it."

Personal susceptibility

Although participants identified types of fraudulent activity, and had a general sense of prevalence rates, this did not necessarily translate into a sense of personal susceptibility. In most cases participants reported they believed it was *possible* they could become a victim of fraud, but that they did not really feel that it was likely to happen to them:

"Not as concerned as I should be. I think that's probably fair to say. One day I'm going to get badly burned but I have this feeling 'oh it's not going to happen to me'."

However, a number of other factors also appear to have an impact upon personal susceptibility. These include familiarity, trust, and personal experience. Firstly, it appears that users will feel more susceptible when they are unfamiliar with the situation or the technology. Users were much more confident when using the ATM than the Internet and some even went as far as to say it was more likely they could become a victim of fraud via Internet use:

"Internet more so because I'm just not sure about it. ATM machines I'm not too, I'm alright with it, but more Internet shopping I would maybe think twice."

Likewise the perception of susceptibility is also affected by the amount of trust the user has in the particular transaction or technology. Many users noted that they only purchased products on the Internet from reliable and well known brands, for instance:

"I don't think I'm particularly concerned, apart from as I say I would only use it in what I felt to be a reliable, with a reliable company or a sort of relatively secure situation."

Users commented that when purchasing online, particularly via eBay, they will try to use PayPal as much as possible because they consider it to be more secure. This leads to an interesting situation as being security conscious should encourage people to only use trusted or familiar sites paradoxically it may also provide users with a false sense of security. Phishing attacks commonly target well known, established and trusted brands including eBay and PayPal to use as the vehicle for their criminal activity. Therefore users that consider trust in a brand to be a suitable benchmark for risk on the Internet may in fact increase their chance of becoming victims themselves.

Additionally, drawing on personal experience and past 'habitual' behaviour also plays a role in personal susceptibility, with a reduced sense of susceptibility for participants who have not previously experienced any fraudulent activity:

"I've never had any problems with the cash machine or over the internet so I feel quite secure when I'm using them."

"As I've said I've used ATMs ever since they came out and I've never had any problems with ATMs."

Perceived severity

Participants did not see the consequences of fraudulent activity as being severe. Fraud was seen as less serious than many other events, partly due to the amounts of money involved, and partly because of the lack of perceived responsibility for dealing with the consequences i.e. someone/something else will be responsible/deal with the consequences.

Participants mentioned the seriousness of fraud in relation to PINs and passwords, Internet purchases and ATM withdrawals. In terms of PIN/password behaviour a minority of participants believed that keeping their internet based passwords secure was less important than keeping their PINS safe. The immediate consequences of PIN exposure were contrasted with the more opaque consequences of harvested passwords. Whilst PINs typically have financial significance, and passwords are more diverse in nature, it may be that owning multiple passwords, in a sense, might dilute the perceived severity of someone fraudulently having access to just *one* of your passwords. Furthermore, in terms of both Internet and ATM use some users felt the consequence of fraud was low because they did not perceive they had a substantial amount to lose:

"And on the other hand, heck I don't have enough money in my bank account that anybody is going to make a million pounds off me, so it's not that much of a problem."

There are also a number of participants who show an overt disregard for the threat of fraud and choose not to implement secure behaviours despite indicating they are aware that they should:

"Even though when you're using eBay and Amazon it says 'make sure that the address is', you never take the time to look at that, you'd have to be a right anorak to be looking for that."

Again this could be explained by a lack of perceived responsibility. Those that believed fraud was not their own individual responsibility considered the consequences of fraudulent attacks to be less serious. A number of participants, for example, indicated the bank would take responsibility and reimburse any financial costs incurred due to fraud:

"I would definitely blame the bank if it, I mean if I hadn't told someone my pin number or something and I was losing money. I think the banks would honour that as well."

Perceived costs

Participants saw a number of costs or barriers to changing their behaviour and acting in a more secure manner. These included convenience, time, memory load, and use of services. In terms of convenience, ATM users indicated they would continue with their regular habits and behaviours because it was more convenient than considering security implications, particularly in relation to location of ATM use:

"If I'm in the town I'll use any one like that I come to first, it doesn't have to particularly be any kind of branch."

In a similar vein, participants indicated they want their transactions to be as quick and efficient as possible, and often see additional security behaviours as an unacceptable extra time cost:

"Again, since I'm not that concerned about it, it doesn't make the slightest bit of difference to me. If it makes the little old lady who's in the queue in front of me and she can get out of there quicker, then sure."

Memory concerns were raised mainly in relation to PIN and password use. Participants often considered the security guidelines surrounding PINs and passwords to be restrictive in terms of memory costs, which often results in negligent behaviours:

"I know that I don't do that, but you should. It's just too hard to remember them all without writing them do and then it's no good."

Finally, participants appeared to value the services delivered by technology such as ATMs and the Internet and due to this were reluctant to restrict their current behaviour practices, which could also lead to a cost of adopting secure behaviour:

"Plus I save money by shopping around and seeing what deals are available."

Perceived benefits

In contrast to the perceived costs of behaving securely, participants rarely touched on the possible benefits of adopting secure behaviour. A very small number of participants referred

to peace of mind in knowing they had taken preventative or protective actions, such as choosing ATM locations more carefully, or confidence in security software and insurance policies.

Cues to action

Participants considered both long-term and short-term cues to action. Over the longer term participants discussed the use of information as a way of raising awareness about fraudulent activity in terms of both susceptibility and severity. This was usually achieved via information leaflets in relation to online banking, or media reports of ATM attacks, for example:

"Well because of the recent publicity on the ATMs I'm conscious of looking to see if the machine is what it should be. So newspapers and radio has alerted me to that, so I've taken that on board."

Short-term cues are those which occur before or during the interaction itself. A number of participants reported being aware of these cues, for example, looking for security icons on websites, or shielding PIN entry at the ATM. However, some cues were also reported as being ineffective, particularly in relation to the exterior of the ATM:

"I'm sure some of them have a little sticker saying 'if you notice anything suspicious about this cash machine' and I thought well if it had a sort of extra slot with the word swag on it and a little cartoon of burglar bill then you might know what it was your were looking for. But if it just looks like a cash machine and you just put your card in the slot to get some money out, what am I supposed to look for?"

In some cases participants did not appear to pay attention to cues, such as warnings stickers, because that was not a part of their habitual behaviour.

More disconcerting still were a few comments indicating a lack of motivation to understand cues:

"Well that's the only one I know but because I haven't really wanted to pursue it that much I haven't looked into it anymore."

Perceived control

The extent to which participants had confidence in their ability to take appropriate action can be broken down into three facets: Awareness of the behaviours to control fraud; implementation of the behaviours and; perceived efficacy of the behaviours to control fraud. In other words do users know what to do, do they do it and do they think it will work?

Awareness of behaviours to control fraud

Participants are aware of both prevention and containment actions. The term prevention is used to describe actions a user can take before or during the transaction which can help to prevent fraud. Whereas, the term containment is used to describe actions a user can take to

protect themselves from the consequences of fraud, and can occur both before the transaction and sometime after, but these actions do not necessarily prevent the actual fraud from occurring.

Users were aware of some preventative measures that can be taken when using the ATM and the Internet, and also noted preventative PIN behaviour. In terms of the ATM, users were aware that PIN shielding, checking the exterior for signs of tampering, and being aware of surroundings, are all measures that can help prevent fraud, with PIN shielding the most frequently mentioned measure. In terms of Internet use participants were aware they should have security software, they should only visit secure sites and to a lesser degree that they should not respond to phishing emails. Users most frequently commented that the padlock icon indicates they are using a secure site:

"Yes, at the top it's got the h whatever it has, but it has to have an s by it. And then you've got to have that little padlock in the bottom."

Often, however, participants' descriptions of what they considered to be a 'secure site' was confused and vague, suggesting only a surface level understanding of this concept.

Comments relating to knowledge of containment measures occurred far less frequently than knowledge of prevention measures. Containment knowledge included awareness of checking bank statements and insurance policies that can protect against the consequences of a fraudulent attack, for example:

"I know that everything I do, because I do quite a lot of transactions through the Internet or by automatic banking and at least I know what I'm doing is safe now because I have this policy in place."

Implementation of control behaviours

Knowing what to do does not automatically mean that users will go ahead and implement the behaviours to control fraud. Some participants, however, did note implementing a number of control behaviours. In terms of preventative actions, ATM users typically reported shielding their PIN, checking for a safe location, and checking that the ATM has not been tampered with. For example:

"I always cover because what I find is people stand very close to you when you put your PIN number in. The post office they stand right behind you. So I always stand in front and put my hand across when I do the PIN."

Although most of the comments concerning prevention relate to ATM use a minority of participants reported preventative actions when using the Internet. These included ensuring they use a computer that has appropriate security software, not responding to phishing emails, looking for security icons and only purchasing from trusted sites. However, as noted in terms

of trust and perceived susceptibility, reliance on security icons and 'trusted' sites is not always a successful prevention strategy.

Almost all participants said they relied upon security software and packages installed on their personal computers. Most participants expressed that they would not use the Internet, particularly for financial transactions unless they were sure security software was in place:

"Again, my own system, I've got my own security software, I've got my own password, I'm perfectly happy with it and I'm the only one that uses it, so again that says yes to me. Using a common terminal, again, would just make me too uncomfortable I think."

Participants also noted generally being more cautious as a way of preventing or controlling fraud. Typically this consists of using the technology in a manner or in a location that leaves the user feeling comfortable. In terms of ATM use this often meant using an ATM in an area deemed to be safe.

Typically participants were cautious about how and where they used the Internet. Some participants were happy to purchase online, but were not happy to bank online, which indicates a higher perception of risk associated with banking.

"Well because as I say I limit my use of it and I don't use it in what I suspect is the most dangerous side and that is the banking side."

Containment action was commented upon less frequently than prevention and consists of insurance and verification. Containment is often implemented retrospectively such as checking bank statements, or is something that is put in place and requires no further direct action such insurance policies. Insurance does not prevent the user from becoming a victim of fraud but does ensure that they are protected from the detrimental consequences. A small number of participants noted that they had an insurance policy to cover them against fraudulent activity which enables them to feel more at ease. Whereas, verification behaviour consist of steps taken to determine whether or not a fraudulent attack has occurred. This includes keeping receipts and checking statements carefully:

"But I always check my bank statements and I've never had a problem, and if somebody did use it for something else you'd knobble them pretty quickly wouldn't you."

The choice of relying on preventative or containment behaviours can reflect whether a participant chooses to be proactive or reactive in relation to fraudulent attacks. The choice to be proactive or reactive will also be influenced by the type of risks and range of control behaviours known to the participant.

Perceived efficacy of control behaviours

Believing that carrying out the behaviours will actually control fraud is also important and perhaps goes some way to explaining why some users may not choose to act despite their

awareness of behaviours to control fraud. In particular, there is a reported sense of fatalism which indicates a lack of belief that control behaviours will control fraud:

"And we're never going to get rid of all fraud because there's always people who are trying to find ways around it."

At a more specific level participants felt that the behaviours they knew were unlikely to be successful if implemented. A number of users, for example, said they were aware of the importance of checking the exterior of the ATM before use but were not confident that the action would be successful in terms of controlling fraud:

"No I wouldn't. Even though I've heard it on the news and they say watch out if something looks odd, but I don't think I would know if something, I don't think I would know."

Summary

In reality, the actual threat of fraud is relatively high. Prevalence rates are increasing in some contexts and if it does happen the consequences can also be highly detrimental. This study, however, shows that the perceived threat of fraud (i.e. perceived personal susceptibility and perceived severity) is low, despite the demonstration of some understanding of prevalence and likelihood of an attack in general. Typically, people do not think it will happen to them and believe that it will not be their responsibility even if it does occur. At a somewhat superficial level people are aware of behaviours they could use to control fraud or at least render it less likely but are reluctant to implement them because they appear time consuming and fairly impotent. This ultimately leads to the perceived costs of secure behaviour adoption outweighing the perceived benefits, and can result in negligent behaviour.

3.1 ATM and Internet technology comparisons

A number of similarities and differences in terms of the two technologies are evident in the HBM analysis (table 2). Firstly the awareness of susceptibility within the perceived susceptibility factor appears to be very similar across both ATM and Internet technology. However, there were certain susceptibilities that were more relevant to ATM use, such as the potential for physical attacks.

TABLE 2 ABOUT HERE

Additionally both ATM and Internet technology use were affected by familiarity, trust, and personal experience; however some contrasting outcomes were apparent. Users appeared to be more familiar and therefore more comfortable with ATM technology compared to Internet technology which reduced their perception of susceptibility. Trust appeared to be mainly an issue for Internet use with greater trust reducing perceptions of susceptibility.

On the whole perceived severity was considered in a similar way for both ATM and Internet technology. In both cases the severity of consequences was considered to be quite low. It

appears users consider risks associated with both technologies to be acceptable and that the consequences of fraud are not specifically their responsibility. There were a number of differences around the issue of perceived control. Users, for example, were more aware of what they should be doing to control their security behaviour online compared to the ATM. In terms of actually carrying out these behaviours, preventative controls were more common when using an ATM and containment controls more common when using the Internet. This distinction, however, may reflect the forms of control behaviour available for the two technologies rather than a conscious decision to use one form over the other. Importantly, users felt that the control behaviours for both technologies would be unlikely to control fraud successfully. Perceived costs and perceived benefits were considered in a similar way for both ATM and Internet technology, with some minor differences in relation to convenience, which appeared to be a greater cost for ATM use, however, again this may reflect the context of use in the sense that transactions take place in a public space and are time limited. Cues to action were considered for both ATM and Internet technology in a similar way in relation to long-term cues, short term cues were however often considered to be ineffective for ATM use.

4. Discussion

The application of the HBM has proved useful in guiding our understanding of the factors affecting users' perceptions of being safe and secure whilst carrying out technology mediated financial transactions. It has extended our knowledge in relation to a broader range of Internet tasks and for the first time has guided our understanding of the factors affecting security behaviour in an ATM context. The findings paint a picture of users who do not feel under threat when using technology. The participants in this study did not feel personally susceptible to fraud and believed the consequences if it did occur to be insubstantial. Whilst users show some awareness of the kinds of techniques employed by criminals their knowledge is fairly high level. In terms of secure behaviours and practices users were aware of what they could or should do to prevent some kinds of fraud from occurring but where unconvinced that taking action would actually control the threat of fraud. A number of differences emerged between ATM and Internet use. These differences serve to highlight some of the fundamental issues surrounding user security and the difficulties in terms of changing behaviour.

Users reported a greater sense of familiarity with ATMs and subsequently were more trusting of the technology in comparison to the less familiar Internet. Participants tried to use their 'regular' ATMs. They felt comfortable doing so and their interactions had become fairly habitual. These habitual practices, however, can stand in the way of users adopting 'new' secure behaviours. Past behaviour and habit are relevant factors in the study of attitudes, intentions, and future behaviours (Ouellette & Wood, 1998; Sutton, 1994). A meta-analysis investigating the impact of habit on intentions and future behaviour indicates the relationship between past behaviour and intention was stronger when the behaviour was habitual and the relationship between attitudes and intention was weaker when the behaviour was habitual (Ouellette and Wood, 1998). Therefore habit may be affecting the security behaviour of

users who behave in a set, repeated manner particularly in light of Azjen's (2002) proposition that infrequent actions can also be affected by habit, such that actually not performing the behaviour becomes habitual. Thus, habit is not simply a product of frequency of past behaviour but a construct in its own right (Verplanken, 2006; Verplanken & Orbell, 2003) and also appears to be important in this domain.

Without habitual behaviours to rely upon, other heuristics appear to come into play when users are accessing the Internet. Relying upon certain trust seals and markers (e.g. Jensen et al, 2005) for example underlies a number of misconceptions that users hold about their value in relation to security. Flinn and Lumsden (2005) found that users believed that the trust mark present on some websites was responsible for the site's security. In practice, however, this marker does not indicate that the site itself is trustworthy; it simply indicates the information in the privacy policy is adhered to, and imposes a requirement for a minimum amount of information to be included in the policy. Other 'trust marks' that users appear to rely on are icons that denote the type of payment that is accepted, such as VISA and Mastercard logos (Jensen et al, 2005). Again this kind of information often relied upon by users to make decisions about whether or not to interact with this site is unreliable in that sense and can also be easily spoofed by a fraudulent source.

In terms of personal susceptibility many participants simply did not believe that a fraudulent attack would happen to them. This form of unrealistic optimism (Weinstein, 1987) has been noted in relation to other IT hazards (Sjoberg & Fromm, 2001). The longer the lack of fraud persists the less likely users are to believe that anything bad will happen to them. The sense of complacency surrounding ATM use in particular may stem from the relative longevity of use and in the case of most of our participants fraud free use. Interestingly, those participants with some experience of direct or indirect fraudulent activity showed a heightened awareness of security issues.

There was a general sense amongst the participants that in the unlikely event of them becoming a victim of fraud then it would be the bank's responsibility to deal with the consequences. Whilst not all participants were confident the bank would accept responsibility, there was a feeling that the fraud itself would not result in any financial loss for them, as some other entity existed which would reimburse them. This is consistent with previous research which suggests users appear to regard security as the responsibility and concern of the bank (Weir et al., 2009). Dourish et al (2004) note that users frequently delegate security to particular organizations or financial institutions, which are expected to take appropriate security measures. Therefore, this lack of responsibility could lead users to feel less concerned about the financial implications, and result in different or lower perceptions of severity. Furthermore, their perception of susceptibility and severity appears to be affected by their perception of responsibility, with most delegating responsibility to technology or an external institution, which is also consistent with Wash (2010) who suggested that users avoid taking responsibility for security decisions.

In terms of unauthorised transactions on UK issued credit cards the Lending Code (2011) states that unless the customer has acted fraudulently or with gross negligence then they will

only be liable for a maximum of £50 before they give notification of loss. If the card is out of their possession and if the customer still has their card then they will not have to pay anything. However as previously noted individual banks are free to set their own terms and conditions concerning what constitutes 'reasonable care' and are thus beginning to shift liability onto the consumer. Despite this, it is still typical for the bank, in most cases, to cover any losses through fraud. Whilst in the longer term people may not be financially hindered the participants in this study failed to mention any of the other costs associated with becoming a victim of this kind of fraud. Cancelling debit or cash cards, for example, can leave users temporarily without access to funds and there is the inconvenience of reporting an incident and providing any relevant documentation. There is also the inconvenience and frustration of waiting for any fraudulent activity on the account to be reversed or refunded. A stolen card can leave users feeling afraid and violated and in situations in which the user still retains the card there is the uncertainty associated with trying to pinpoint the specific time during which the card details were fraudulently obtained. Many of the participants were able to report a number of behaviours that could potentially control fraud and listed actions they 'should be doing' in order to improve their security in relation to financial transactions. Whilst participants' high level knowledge does not appear to be the problem a close inspection indicates that for many they are unsure as to what the behaviour actually does and how it works. This reduced users' sense of control over the behaviours and left them wondering whether or not implementing the behaviour would have any effect at all on fraud.

This is consistent with previous research as Flinn and Lumsden (2005) point out two main interpretations of a 'secure web site' which include the site itself as being secure and trustworthy, and the more technically accurate interpretation that it is the connection or method of transporting data that is secure (e.g., via the use of SSL technology). Therefore, if the user does not distinguish between storage and transport, there are clear implications for the user's understanding of which sites are trustworthy or not, as they may perceive a secure site to be a trustworthy site. Although it is true that SSL protocols do provide server authentication, it can only go as far as determining the communication is only with the intended recipient, and not as far as determining the trustworthiness of the intended recipient. Similarly, Friedman et al (2002) found differing interpretations of the term website security. Therefore, although participants in the current study appeared to be aware of certain practices, they may not fully understand what the behaviours actually achieve.

Internet based research also indicates that users can feel a sense of futility in terms of their security actions. With threats constantly changing and evolving, vigilance was seen as more important than security per se (Dourish et al., 2004). Moreover, if participants are not convinced their behaviours will reduce the threat of fraud they are unlikely to act, with previous research indicating the importance of self-efficacy in this domain. Woon et al (2005), for example, found self-efficacy to be a significant predictor of using the security features on wireless networks in the home. More recently, Rhee et al (2009) found that users with higher self-efficacy in relation to information security reported using more security software and features. Higher information security self-efficacy also related to more reports of security care behaviour in general in relation to computer/Internet use, and greater

intention to continue with such security efforts. It also appears that past experience impacts self-efficacy, such that previous success is likely to increase self-efficacy and previous failure is likely to decrease self-efficacy (Compeau & Higgins, 1995). Therefore, if participants feel their previous attempts at behaving securely have not been effective they are likely to have a lower self-efficacy in relation to adopting secure behaviour in the future.

The findings highlight that users perceive there to be a number of costs associated with behaving securely. In relation to ATM use these costs were predominantly related to time and convenience. The costs of behaving securely online were seen as more restrictive with participants reporting difficulties with remembering different PINS and passwords. The usability-security trade off for PIN and password use is already well documented (e.g., Chiasson et al, 2007; Sasse et al, 2001; Yan et al, 2004). Passwords and PINs are the most typically implemented knowledge-based authentication type. It is often recommended that passwords and PINs be complex and difficult for anyone else to guess. They should be changed periodically and never be used for more than one access point. However, much of the literature suggests users do not manage their PINs and passwords effectively and securely, and studies have found that users typically use simple passwords that can be easily guessed (Proctor et al., 2002; Ives et al., 2004).Users can also feel that increased security acts as a barrier to work activities, increasing the time it takes to complete tasks (Dourish et al., 2004). People place more value on usability and convenience than security, and only when the perceived threat increases will they accept more complicated processes for security (Weir et al, 2009).

For those using the Internet to conduct financial transactions it is key to remember that their goals can to some extent be frustrated by the adoption of more secure behaviour online. A user may be unable to buy a certain product online if they decide to only purchase goods from trusted sites. Whilst users appeared relatively well educated about security behaviours, they might feel less inclined to implement those behaviours if in doing so they were thus unable to achieve their goals. For example, people may be able to accurately list the steps they should take to identify a trustworthy site, but are prepared to disregard the list completely if the very thing they desire is only available on an untrustworthy site (Dudek, personal communication). For banks themselves there are obviously costs associated with users behaving insecurely. But any losses the industry endures through fraudulent activity are offset by the savings they make through the use of automated, technology driven transactions in terms of self service provision and online banking. In addition to the goal driven pressures the customer places upon themselves they are also then faced with pressure from the banks to use the technology.

FIGURE 1 ABOUT HERE

The HBM has proved a useful tool for mapping users' knowledge and attitudes concerning security behaviour onto useful theoretical constructs. For completeness Figure 1 reflects a modified HBM model which takes into account the external and internal pressures of the domain more clearly and it is anticipated will be used in future work in this area. The model thus provides a basis for the generation of practical suggestions towards encouraging secure

behaviour. Outlined in Table 3, the practical implications based on our findings are underpinned by a number of behaviour change techniques (see Abraham & Michie 2008).

TABLE 3 ABOUT HERE

Implications

The shifting nature of the problem, the relative complexity of some of the fraud types and technologies involved, coupled with numerous individual as well as cultural differences, make the issue of encouraging secure behaviour far from straightforward. There are a number of implications, however, which emerge from this study and are discussed below.

It is worth noting that whilst users were typically well informed about the security risks and about different security measures available they were less clear about the detail of the threats and exactly how security actions countered these risks. Card not present fraud often leaves a very frail link between the users insecure behaviour and the fraudulent outcome, making it difficult for the user to know which specific behaviour was the problem and therefore which piece of knowledge might have been helpful in preventing the fraud. Whilst it is apparent that simply educating users is not the answer to this problem, spending more time thinking about the kinds of information users receive may have an effect, in that it might allow them to refine their mental models to think about how and why they are taking the action they are. It may also prove useful for designing training materials that transform users' passive knowledge into more active behaviours, thus encouraging the modelling or demonstrating of behaviour as a behaviour change technique (Abraham & Michie, 2008) (see for example Sheng et al., 2007 on phishing websites). Given that the number and variety of fraudulent attacks increases, it remains important that people are kept up to date so that they have the most recent and relevant knowledge to refer to in combination with other behavioural interventions. This information could be imparted at key communication points with users, for example, on holding screens on ATMs, leaflets included in promotional material from the bank and during online banking transactions. It is important to note that raising awareness may have undesirable consequences in terms of leaving some users feeling fearful. Increasing the perception of the threat is important in terms of behaviour change but overly frightened users may choose to cease using the technology altogether rather than modify their behaviours appropriately. The use of fear appeals leading to adaptive and/or maladaptive responses is considered extensively in the health domain as a means of behaviour change (e.g., Witte & Allen, 2000). Findings from that body of literature suggest that successful campaigns to raise awareness, yet not impede action through fear, will need to consider the impact of individual characteristics, such as self-esteem and importantly the perceived efficacy of the proposed action.

The findings of this study have a number of implications for design. Increasing the salience of prompts and warnings would improve cues to action and increase perceived control. Users were unsure of the cues that indicated when the behaviour should be carried out, or they were not convinced that their actions could control the threat of fraud. Thus, it is not surprising that users value convenience and resort to habitual behaviours instead of more secure behaviours, and it is important that future design takes into account the user experience that drives

technology-mediated transactions. Indeed preliminary data collected in the lab suggests that differences in timing and positioning of warning messages on ATM screens do not have an adverse effect on user satisfaction with ATM use (Davinson & Sillence, n.d.) and so may be a promising research avenue in terms of encouraging behaviour change. In the current study, saliency of the cues was most problematic for ATM use, and therefore ATM design could consider how cues to act can be optimised to be prominent and timely within the task flow of using ATMs. ATM technology use in particular appears to suffer from users' habitual behaviours. It is therefore important to recognise the value of appropriate prompts and cues (Abraham & Michie, 2008). These could include recognition of a warning as part of the transaction process that highlights the benefits of undertaking secure behaviour, rather than simply proceeding with less secure habitual behaviours. A similar course of action can be taken with Internet technology, whereby users can be encouraged to overcome the costs of secure behaviour adoption and provided with a clear focus on the positive benefits of practicing secure behaviour. Saliency was less of an issue for Internet use and therefore the focus of Internet cues to action should be on a more accurate interpretation of what the icons and symbols really represent. Misunderstandings were apparent in the discussions and could lead users to believe they were acting securely when, in fact, they were not. Jensen et al (2005) indicate the importance of creating highly visible and easily understandable trust markers that will lead the user to rely on the correct cues, rather than missing the legitimate cues and relying on superficial and/or inappropriate information. Focusing on clear and accurate interpretations may help reduce the perceived costs associated with secure behaviour allowing people to recognise that it need not be overly time consuming. Likewise reinforcing the benefits of behaving securely could focus on both the practical issues associated with avoiding time and financial costs as well as the enhancement of intrinsic factors such as a sense of competence surrounding security management and a feeling of contributing to the wider aim of reducing fraud overall. Again this requires some consistency in terms of the technology countermeasures in place. The simple yet effective heuristics we encourage users to enact online are in some instances undermined by the very countermeasures designed to protect them (see Murdoch & Anderson, 2010).

The consequences of not behaving securely are still regarded as minimal, and with the shifting liability issue still to gain widespread visibility, increasing perceptions of susceptibility appear to be one of the most promising avenues for investigation. We know from the persuasion literature that both the source and the message are important in terms of increasing persuasive content (Chaiken, 1980).Thinking about the message itself, the salience to the user could be increased through message tailoring in terms of location, demographics and individual differences, such as orientation to threat or information processing style. Location tailoring may be more appropriate for ATMs and could be achieved by providing users with data relating to fraudulent attacks and losses in the local area. Tailoring the information to match individual differences has proven useful in the health domain with Kreuter et al., (2000) demonstrating that tailoring a message to the individual does attract more attention. Other studies have used tailored messages to elicit the adoption of more desirable behaviours (Williams-Piehota et al., 2003; Williams-Piehota et al., 2004a; Williams-Piehota et al., 2004b). It may be possible to personalise the susceptibility

information for ATM and Internet users. Personalisation could be achieved via questionnaire measure that could alert the user to negligent behaviours they carry out and direct them to more secure behaviour practices, in line with providing instruction and prompting specific goal setting (Abraham & Michie, 2008).

Work in the health domain has also successfully demonstrated the power of narrative versus statistical material in the presentation of risk information (Green & Brinn, 2003). In the security domain as well, many people use stories from friends and family about security incidents to shape their subsequent thinking and behaviour about security (Radar et al, 2012). A number of studies have recently pointed to the changing nature of expertise with the health domain, moving away from a designated medical expert towards patients own experiential information. Patients retelling their own stories have the potential to improve knowledge, recall, and outcomes (see Ziebland & Wyke, 2012 for an overview). Presenting security information in the form of personal experiences or narratives might help increase the salience of the risk message and increase users' sense of susceptibility. Furthermore improving the degree of similarity between the user and the source of the narrative is likely to strengthen user engagement with the material (Briggs et al, 2013;Wang, et al., 2008; Winterbottom, et al., 2012;de Wit, Das, & Vet, 2008)making it easier to recall and more influential in terms of any subsequent decision making around risk and security. In addition to this, and to tackle the issue of perceived severity, provision of information regarding responsibility and consequences can be re-iterated to both ATM and Internet users, alongside information that alerts the user to whether others approve or disapprove of current behaviour practices (Abraham &Michie, 2008).

Behaviour change models are only just starting to be applied to a security context. It is not yet known which, if any, interventions will prove successful in promoting secure user behaviour, but risk perception and susceptibility in particular appears to be a promising avenue for further investigation. Further research in this domain is clearly necessary, despite the promising decrease in fraudulent activity both via ATM and Internet technology fraud is still occurring in these domains, and it is typically user error that introduces the threat of fraud. Therefore, highlighting barriers to secure behaviour adoption, using a framework such as the HBM, and developing interventions to overcome such barriers will ultimately aid the promotion of secure behaviour and help to decrease fraudulent attacks further.

Limitations

The inclusion criteria for this study meant that all the participants used ATMs and the Internet for online banking. A more fine grained analysis of technology use may have revealed differences between the users in terms of their security knowledge and behaviours. Likewise, any future work utilising a larger sample size may be able to focus on an analysis by age and gender. Although it should be noted that no substantive demographic differences were noted in the current study.

Conclusion

Although users show some awareness of fraud and security issues they perceive the threat to themselves from using the Internet or an ATM to be low. Familiarity and high trust levels play an important role in this (mis)perception and whilst users talk about being safe and secure they typically fail to implement the behaviours necessary to stay that way. Whilst this awareness-implementation gap is present for both ATM and Internet transactions, subtle differences between the two mediated environments exist. The relative novelty of the Internet coupled with its use within a private space seems to confer on users a slightly heightened perception of the risk coupled with an increased sense of personal responsibility for pro-actively trying to keep fraud at bay. Practical suggestions for promoting secure behaviour derived from the HBM factors have been devised for both ATM and Internet users and increasing the salience of the risk message has been highlighted as a promising avenue for further research. In conclusion the HBM appears to be a useful tool for guiding further research and promoting the adoption of secure behaviour in relation to technology-mediated transactions.

Acknowledgements

The authors would like to acknowledge the support of NCR Corporation throughout this project.

References

Abad, C. (2005). The economy of phishing: A survey of the operations of the phishing market. *First Monday,* 10 (9).

Abraham, C., & Michie, S. (2008). A taxonomy of behavior change techniques used in interventions. *Health psychology*, *27*(3), 379.

ACI Worldwide (2011, February 9). A third of Britons have been hit by card fraud - but scams declining. Retrieved October 2011 from http://www.aciworldwide.com/en/News-and-events/ACI-in-the-news/110209-A-third-of-Britons-have-been-hit-by-card-fraud-but-scams-declining.aspx

Acquisti, A. (2004). Privacy and security of personal information. Economic incentives and technological solutions. In J. Camp and R. Lewis (Eds.), *The Economics of Information Security*, Kluwer Academic Publishers.

Acquisti, A., and Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security (WEIS '03).*

Ajzen, I. (2002). Residual effects of past on later behavior: Habituation and reasoned action perspectives. *Personality and Social Psychology Review, 6,*107-122.

Anti-Phishing Working Group, Phishing Activity Trends Report 2nd Half 2010, available at http://www.antiphishing.org/reports/apwg_report_h2_2010.pdf

ATMIA (2012). ATM fraud report. Retrieved from: https://www.atmia.com/clientuploads/ATM%20Security%20Forum/ATMIA's%20ATM%20Fraud%20Report%202012%20%20PUBLISHED.pdf

Austin, L. T., Ahmad, F., McNally, M. J., & Stewart, D. E. (2002). Breast and cervical cancer screening in Hispanic women: a literature review using the health belief model. *Women's health issues: official publication of the Jacobs Institute of Women's Health*, *12*(3), 122.

Bell, B., Toth, N. & Little, L. (in prep). Planning to save the planet: Using an online intervention based on implementation intentions to increase teen energy saving behaviour.

Blank, G. and Dutton, W.H. (2011) Age and trust in the Internet: The centrality of experience and attitudes toward technology in Britain. *Social Science Computer Review*, February 2011.

Bohm,N., Brown,I., & Gladman, B. (2000). Electronic commerce: Who carriesthe risk of fraud? The Journal of Information, Law and Technology, (3). Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/

Bonar, E. E., & Rosenberg, H. (2011). Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies. *Addictive Behaviors*, *36*(11), 1038-1044.

Booz, Allen & Hamilton, (1997*). Internet banking: a global study of potential*. New York, NY: Booz, Allen & Hamilton Inc.

Briggs, P., Hardy, C., Sillence, E. & Harris, P.R. (2013). An Engagement Framework for Understanding the Communication Needs of Different Health Groups. CHI workshop on Patient-Clinician Communication: The Roadmap for Human-Computer Interaction. Paris, France 28th April, 2013.

Camilli, M., Dibitonto, M., Vona, A., Medaglia, C.M., &Di Nocera, F (2011). User-centered design approach for interactive kiosks: evaluation and redesign of an automatic teller machine. *Proceedings of the 9th ACM SIGCHI Italian Chapter International Conference on Computer-Human Interaction: Facing Complexity*, 13-16 September, Alghero, Italy.

Camp, J.L. (2009). Experimental evaluation of expert and non-expert computer users' mental models of security risks. *Workshop on Security and Human Behaviour (SHB 2009)*, June 11-12.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of personality and social psychology*, *39*(5), 752.

Cheswick, W.R. and Bellovin, S.M. (1994). *Firewalls and Internet Security*, Addison-Wesley.

Chiasson, S., Biddle, R., and van Oorschot, P.C. (2007). A second look at the usability of click-based graphical passwords. In *Proceedings ACM Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, USA, July.

Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., and Mitchell, J.C. (2004). Client-side defense against web-based identity theft. In *Proceedings of The 11th Annual Network and Distributed System Security Symposium (NDSS) 2004*. San Diego, CA, USA.

Christolav E. A., Marianne A.H. and Jeanne M. H. (2003). US Consumer's and electronic banking 1995- 2003. Board Division of Consumers and Community Affairs. Los Angeles

Compeau, D.R., and Higgins, C.A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, 19, (2), 189-211.

Coventry, L. (2005). Usable Biometrics. In L Cranor& S Garfinkel (Eds). Usability and Security: Designing secure systems that people can use. O Reilly Media Inc., Sebastopol, CA.

Coventry, L., De Angeli, A., and Johnson, G. (2003). Usability and biometric verification at the ATM interface. Proceedings of CHI 2003 Conference, Fort Lauderdale, Florida, 153-160. ACM Press.

CPP (January 2011). Card fraud affected a quarter of adults. Available at http://blog.cpp.co.uk/index.php/news/card-fraud-affected-a-quarter-of-adults

Culnan, M. J. (1999). *Georgetown Internet privacy policy study: Privacy online in 1999: A report to the Federal Trade Commission*. Washington DC: Georgetown University.

Curran, K. & King, D. (2008). Investigating the Human Computer Interaction Problems with Automated Teller Machine (ATM) Navigation Menus. *Computer and Information Science,* 1 (2), 34-51.

Daniel, E. (1999). Provision of Electronic Banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, 17(2), 72–82.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26 (6), 1739-1747.

Davinson, N., & Sillence, E. (n.d.). *Warning messages on ATM screens: Exploring the impact of timing and positioning on user satisfaction.* Unpublished manuscript, Pact Lab, Northumbria University, UK.

De Angeli, A., Athavankar, U.A., Joshi, A., Coventry, L. &Johnson, G.I. (2004). Introducing ATM's in India: A contextual enquiry. Interacting with Computers special issue: Global human-computer systems, 16(1) 29-44.

De Wit, J.B., Das, E. &Vet, R. (2008). What works best: objective statistics or a personal testimonial? An assessment of the persuasive effects of different types of message evidence on risk perception. *Health Psychology*, 27(1)110-5.

Dinev, T., Goo, J., Hu, Q., and Nam, K. (2009) User behavior towards protective technologies -The role of national cultural differences. *Information Systems Journal*, 19, 391-412.

Dourish, P., Grinter, R.E., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8, 391-401.

European Central Bank (2012). Report on card fraud. Retrieved from: www.ecb.int/pub/pdf/other/cardfraudreport201207en.pdf

Federal Trade Commission (2000). Privacy Online: Fair Information Practices In the Electronic Marketplace. Available at http://www.ftc.gov/os/2000/05/testimonyprivacy.htm

Federal Trade Commission. (1998b). FTC report on consumers' online privacy. FTC Press Release, (June 4), FTC File N. 954-4807.

Financial Fraud Action UK. Using your card at a cash machine. Retrieved from: http://www.financialfraudaction.org.uk/Consumer-using-your-card-at-a-cash-machine.asp

Financial Fraud Action UK. Card smart online. Retrieved from: http://www.financialfraudaction.org.uk/Consumer-be-card-smart-online.asp

Flinn, S., and Lumsden, J. (2005). User perceptions of privacy and security on the web. *Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST 2005).* St. Andrews, New Brunswick, Canada. October 12-14, 2005.

Friedman, B., Hurley, D., Howe, D.C., Felton, E., &Nissenbaum, H. (2002). Users' conceptions of web security: A comparative study. In *Proceedings of CHI 2002 Conference on Human Factors in Computing Systems*, 746-747.

Getsafeonline.org. Protecting yourself. Available at: https://www.getsafeonline.org/protecting-yourself/

GRGBanking (2011). Best practice for ATM security. Retrieved from: http://www.grgbanking.com/en/exh/images/Best%20Practice%20for%20ATM%20Security%20-GRGBanking.pdf

Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist, 54*, 493-503.

Goucher, W., (2008). Enabling secure behaviour. *Computer Fraud & Security*, 12–14.

Greene, K., & Brinn, L. S. (2003). Messages influencing college women's tanning bed use: statistical versus narrative evidence format and a self-assessment to increase perceived susceptibility. *Journal of Health Communication*, 8, 443–461.

Hu, Q. and Dinev, T. (2005). Is spyware an internet nuisance or public menace? *Communications of the ACM*, 48, 8, 61-66.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

James, D., Pobee, J. W., Brown, L., & Joshi, G. (2012). Using the Health Belief Model to Develop Culturally Appropriate Weight-Management Materials for African-American Women. *Journal of the Academy of Nutrition and Dietetics, 112*(5), 664-670.

Jensen, C., Potts, C., &Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63, 203-227.

Keizer, G. (2005, January 26) Shoulder Surfing, Sniffing Worse Than "Evil Twin" Access Points. Retrieved October 2011 from http://www.informationweek.com/news/57704059

Krebsbach, K. (2004). Goin' phishin. *Bank Technology News*, April.

Kreuter, M., Farrell, D., Olevitich, L., & Brennan, L. (2000). *Tailoring health messages.* Mahwah, NJ: Lawrence Eribaum.

Lewis, P., (2012). Where do customers stand if they break banks' PIN rules? Communication on BBC, retrieved from: http://www.bbc.co.uk/news/business-20336555.

LINK (2013). Statistics. Retrieved from: http://www.link.co.uk/AboutLINK/Statistics/Pages/Statistics.aspx

LINK Cardholder Security. Retrieved from: http://www.link.co.uk/Cardholders/security/Pages/CardholderSecurity.aspx

Litan, A. (2005). Increased phishing and online attacks cause dip in consumer confidence. *Gartner Group*, (G00129146).

Little, L. (2003). Attitudes towards technology use in public zones: the influence of external factors on ATM use. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*. Ft. Lauderdale, Florida, USA, April 5-10.

Little, L., Briggs, P., & Coventry, L. (2005). Public space systems: Designing for privacy? *International Journal of Human-Computer Studies* 63, 254-268.

Liu, Z, Coventry, L, Johnson, G, Zhang, H and Chen, J. The people's machine: Automatic Teller Machines in China. User Experience, 6, 2, 18-22. 2007.

Minugh, P. A., Rice, C, & Young, L. (1998). Gender, health beliefs, health behaviours, and alcohol consumption. *The American Journal of Drug and Alcohol Abuse, 24(3),* 483-497.

Murdoch, S.J. (2013). UK bank fraud up by 11% in 2012, but how much do customers lose? Retrieved from: http://www.lightbluetouchpaper.org/2013/03/13/uk-bank-fraud-up/

Murdoch, S., & Anderson, R. (2010). Verified by visa and mastercard securecode: or, how not to design authentication. *Financial Cryptography and Data Security*, 336-342

Murdoch, S.J., Drimer, S., Anderson, R.J., & Bond, M. (2010) Chip and PIN is Broken. IEEE Symposium on Security and Privacy.

Myers, S. (2007). Introduction to phishing. In Jakobsson, M., and Myers, S. (Eds.) *Phishing and Countermeasures*. New Jersey: John Wiley and Sons.

NCR, (2006). ID theft and ATM fraud, NCR Webinar Series. Available at http://www.hacfe.gr/events/Papers/NCR-ATM_Fraud_WP06.pdf

Ng, B., Kankanhalli A. and Xu Y. (2009) Studying users' computer security behavior: a health belief perspective, *Decision Support Systems*, 46, 4, 815-825.

Norton (2010). Cybercrime report. Retrieved October 2011 from http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_UK-HumanImpact-A4_Aug4.pdf

O'Connell, B. (1996). Australian banking on the Internet - fact or fiction? *The Australian Banker*, December, 212-214.

Ouellette, J. A., and Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin*, 124, 54-74.

PayPoint (2013) Key facts. Retrieved March 2013 from http://www.paypoint.co.uk/retailers/atm)

Payments Council (2010). The way we pay. Available at http://www.paymentscouncil.org.uk/files/payments_council/the_way_we_pay_2010_final.pdf

Proctor, R. W., Lien, M. C., Vu, K. P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods*, *34*(2), 163-169.

Rader, E., Wash, R., & Brooks, B. (2012, July). Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 6). ACM.

Renaud, K., De Angeli, A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers* 16 (6), 1017-1041.

Rhee, H-S., Kim, C., and Young, U.R. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security*, 28, 816-826.

Rogers, R.W. (1975) A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114.

Rosenstock, I M. (1974). The health belief model and preventive health behavior. *Health Education Monographs*, 2, 354-386.

Safecard. Be safe at the ATM. Retrieved from: http://www.safecard.ie/cardholders/be-safe-at-the-atm/

Sasse, M.A., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link' – A human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19 (3), 122-131.

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, 17 (7), 324-334.

Schneier, B. (2000). *Secrets and Lies*. John Wiley and Sons: New York, NY.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., and Nunge, E. (2007). Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, July 18-20, Pittsburgh, Pennsylvania.

Shostack, A. (2003). Paying for privacy: Consumers and infrastructures. In *2nd Annual Workshop on Economics and Information Security (WEIS '03)*.

Sjöberg, L., & Fromm, J. (2001). Information technology risks as seen by the public. *Risk Analysis*, *21*, 427-442.

Spiekermann, S., Grossklags, J., and Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, Tampa, Florida, USA, October 14-17.

Sutton, S. (1994). The past predicts the future: Interpreting behaviour-behaviour relationships in social psychological models of health behaviour. In D. R. Rutter & L. Quine (Eds.), *Social psychology and health: European perspectives (*pp. 71-88). Aldershot, UK: Avebury.

The Lending Code (2011). Retrieved from: http://www.bba.org.uk/downloads/bba/The_Lending_Code.pdf

The UK Cards Association, (2011) Fraud the Facts 2011. Available athttp://www.financialfraudaction.org.uk/Publications

The UK Cards Association (2012). Fraud the Facts 2012. Available at www.theukcardsassociation.org.uk/wm.../Fraud_The_Facts_2012.pdf

The UK Cards Association (November, 2012). Summary of key statistics for Q4 2012. Retrieved from: http://www.theukcardsassociation.org.uk/wm_documents/2012%20Q4%20Statistical%20Release%20-%20Final%20%282%29.pdf

Trustwaves Spiderslabs (2009) ATM technical security review. Retrieved from: https://www.trustwave.com/downloads/Trustwave_SpiderLabs_ATMTechReview.pdf

Unisys Security Index, (February, 2011). UK public security worries reach four-year peak, according to Unisys Security Index. Retrieved October 2011 from http://www.unisys.com/unisys/countrysite/news/index.jsp?cid=300008&id=2600068

Verplanken, B. (2006). Beyond frequency: Habit as a mental construct. *British Journal of Social Psychology*, 45, 639-656.

Verplanken, B., and Orbell, S. (2003). Reflections on past behaviour: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33, 1313–1330.

Von, A. D, Ebert, S., Ngamvitroj, A., Park, N., & Kang, D. H. (2004). Predictors of health behaviours in college students. *Journal of Advanced Nursing, 48(5),* 463-474.

Wang, Z., Walther, J. B., Pingree, S., & Hawkins, R. P. (2008). Health information, credibility, homophily, and influence via the Internet: Web sites versus discussion groups. *Health communication*, *23*(4), 358-368.

Wash, R. (2010). Folk models of home computer security. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, Redmond, WA USA

Weinstein, N.D. (1987). Unrealistic optimism and illness susceptibility: Conclusions from a community wide sample. *Journal of Behavioural Medicine*, (10) 481-500.

Weir, C.S., Douglas, G., Carruthers, M., and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens.

Welch, K. J. (2000). Correlates of alcohol and/or drug use among HIV-infected individuals. *AIDS Patient Care and STDs, 14(6),* 317-323.

Williams-Piehota, P., Cox, A., Silvera, S.N., Mowad, L., Garcia, S., Katukak, N., and Salovey, P. (2004a). Casting health messages in terms of responsibility for dietary change: Increasing fruit and vegetable consumption. *Journal of Nutrition Education and Behavior, 36*, 114-120.

Williams-Piehota, P., Schneider, T.R., Pizarro, J., Mowad, L., &Salovey, P. (2003). Matching health messages to information processing styles: Need for cognition and mammography utilization. *Health Communication, 15*, 375-392.

Williams-Piehota, P., Schneider, T.R., Pizarro, J., Mowad, L., and Salovey, P. (2004b). Matching health messages to locus of control beliefs for promoting mammography utilization. *Psychology and Health*, 19, 407-423.

Winterbottom, A. E., Bekker, H. L., Conner, M., & Mooney, A. F. (2012). Patient stories about their dialysis experience biases others' choices regardless of doctor's advice: an experimental study. *Nephrology Dialysis Transplantation*, *27*(1), 325-331.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27 (5), 591-615.

Woon, I. M. Y., Tan, G. W., and Low, R. T. (2005). A Protection Motivation Theory approach to home wireless security. *In Proceedings of the Twenty-Sixth International Conference on Information Systems*, 11-14 December, Las Vegas, Nevada, USA.

Wouters, E.J., Nunen., A.M., Vingerhoets.,A.J, & Geenen, R. (2009). Setting overweight adults in motion: the role of health beliefs. *Obesity Facts*. 2, 362–9.

Wu, M., Miller, R. C., and Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Montréal, Québec, Canada, April 22 – 27.

Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy*, 2 (5).

Yarbrough, S. S., & Braden, C. J. (2008). Utility of health belief model as a guide for explaining or predicting breast cancer screening behaviours. *Journal of advanced nursing*, *33*(5), 677-688.

Zhang, Y., Hong, J.I., and Cranor, L.F. (2007) Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web (WWW) 2007*, New York, NY, USA.

Ziebland, S., & Wyke, S. (2012). Health and Illness in a Connected World: How Might Sharing Experiences on the Internet Affect People's Health?. *Milbank Quarterly*, *90*(2), 219-249.