Password Sharing: Implications for Security Design Based on Social Practice

Supriya Singh, Anuja Cabraal
Smart Internet Technology
Cooperative Research Centre
RMIT University
GPO Box 2476 V
Melbourne, VIC, 300, Australia
supriya.singh@rmit.edu.au
anuja.cabraal@rmit.edu.au

Catherine Demosthenous
Michele Furlong
GSA Information Consultants
PO Box 1141
Toowong, QLD, 4066, Australia
g.astbrink@gsa.com.au
mfurlong@iinet.net.au

ABSTRACT
Current systems for banking authentication require that customers not reveal their access codes, even to members of the family. A study of banking and security in Australia shows that the practice of sharing passwords does not conform to this requirement. For married and de facto couples, password sharing is seen as a practical way of managing money and a demonstration of trust. Sharing Personal Identification Numbers (PINs) is a common practice among remote indigenous communities in Australia. In areas with poor banking access, this is the only way to access cash. People with certain disabilities have to share passwords with carers, and PIN numbers with retail clerks. In this paper we present the findings of a qualitative user study of banking and money management. We suggest design criteria for banking security systems, based on observed social and cultural practices of password and PIN number sharing.

Author Keywords
Banking; security; Australia; UCD; sharing passwords, social and cultural centered design.

ACM Classification Keywords
K.4.2 Computers and society: Social issues; H.5.m Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Money is one of the most private aspects of life, but people talk with those within ‘their circle of care’ about their money. This ‘circle’ in Australia nearly always includes the partner [40]. Banks, however, tell consumers on their web sites not to disclose their access codes. As Westpac Banking Corporation says, “Internet Banking customers should not disclose their access codes to any third party including family, friends and institutions” [45]. If the access codes, passwords, user names and Personal Identification Numbers (PINs) are disclosed, the consumer is not protected. For example, under the Electronic Funds Transfer Code of Conduct (2002) [5], the account holder is liable for losses where “the user voluntarily discloses one or more of the codes to anyone, including a family member or friend” (paragraph 5.6(a), p.14).

Banks use what you know as the first order of authentication – hence user names and PINs. Banks buttress these arrangements by adding the second order of authentication, what you have, by the use of tokens. The third order of authentication, what you are, is potentially addressed by biometrics (the physical characteristics of the individual).

The traditional remedy for security problems is to raise ‘awareness’ of security issues and push for more consumer education [4]. We argue in this paper that, depending on the confidentiality of user names, passwords and PINs even within the family, as the first rung of security, goes against common social practice. We build on user-centered security perspectives to propose that security designers take into account the possibility of shared domestic use. Our research contribution is the reformulation of the design problem. Our empirical work demonstrates that shared use is common in different social and cultural contexts. We argue that security design that does not take this social and cultural context into account is inherently flawed.

In the next section we outline how we are building on the emerging field of user-centered security. Then, we show how we conducted the qualitative study from which we draw our summary and conclusions.

USER-CENTERED SECURITY
A user-centered approach to security places the user at the centre of security development. There has been an emphasis on aligning security and usability. There has also been a focus on the psychological dimensions of security.
Consequently, issues of ease of use and cognitive load have become part of the discussion of security mechanisms.

Our emphasis follows what has been termed ‘sociological security’ [18]. There has been some work on the group context in organizations [17, 31, 35] and ‘social transcluence’ [1, 2, 16]. There has also been the use of qualitative methods to discover the security problems in the context of everyday life [14, 18]. Gaw et al. [18] for instance studied “the social context behind users’ decisions about whether and when to encrypt email” (p. 591).

For the most part, the literature on user-centered security sees the user as an individual in an organizational context. We propose that the field needs to expand in three directions. First, the domestic context of individual and shared activities in the household has become important as the Internet becomes a channel for daily activities. Second, these activities and values need to be studied in the field, rather than the lab. The social and cultural meaning of activities would then become apparent. As Tognazzini [44] says, "Both students and professors need to do field studies of real people working in real environments" (p. 46). Third, the cultural meanings of activities also have to be taken into account. This is particularly true for online financial transactions as money is used, managed and owned in different ways in various cultures [39].

There are at present three strands in the literature on user-centered security: 1) the connection between usefulness and activity; 2) an emphasis on trust; and 3) the close connection between privacy and the control of personal information.

1) Usefulness and the Activity

People are not focused on security but on an activity [30, 33] with goals and therefore users’ main goals are at the centre of usability [22].

Aligning security and usability is a core aspect of user-centered security [11, 46]. As Tognazzini [44] says:

The goal of security is not to build systems that are theoretically secure, but to build ones that are actually secure.... It requires close examination not only of the technology, but also of the human beings that will use it (p. 31).

A focus on the psychological dimensions of security has emphasized ease of use [8]. The literature on passwords thus emphasizes cognitive load, that is, the need to keep the password easy to use but difficult to guess [12].

D’Hertefelt’s [13] research suggests that “The feeling of security experienced by a user of an interactive system is determined by the user’s feeling of control of the interactive system.” Based on qualitative research towards making the website of an European airline more usable, they came up with the unexpected finding that “people’s perception of security when doing on-line transactions depends on the simplicity of the site and on the availability of user support.”

It has been difficult for theoretically oriented security system developers to move from theoretical security to usable security. Schneier (2000) opens his book Secrets and lies: Digital security in a networked world with a mea culpa relating to his earlier text on applied cryptography [36]. He says he was wrong to think that mathematics alone could ensure digital security. He did not take into account users and their context [37]. He says security is a multi-layered process, rather than a product. Schneier realized in 1999 that “…the fundamental problems in security are no longer about technology; they’re about how to use the technology” (p. 398).

2) Trust and Security

The second strand in the user-centered security literature is to move from a focus on security to an emphasis on trust. Trust is a wider concept than security. Trust however is difficult to define. People speak of trust most clearly when they speak of a lack of trust. This is especially so in situations where there is a greater risk and where information is less easily available [42]. Issues of trust and the use of electronic money are increasingly being discussed [6, 21, 23-25, 42, 43].

It is important to disentangle the concepts of security and trust, because even “usable security” is not always a sufficient condition for trust. Friedman and Grudin emphasize the importance of human values for establishing and maintaining trust for the effectiveness of the information infrastructure [17]. They say:

The common good of our information infrastructure depends on designs through which users can establish and maintain trust and accountability. Without preserving such human values, users will be reluctant to embrace this infrastructure as a means for conducting their daily affairs -- commerce, communication, health, work, and education (p. 213).

Where the values of trust are not at the center of security systems in organizations, security mechanisms will be bypassed or subverted. Sharing information is essential for work in an organization and these preferences need to be taken into account [31]. Sasse and Flechais [35] say:

In most current cases, existing trust relationships in an organization facilitate the breaking of security policies and practices. In fact... adhering to existing security policies can undermine social relationships within a group of peers. The authors argue... that the organizational culture and the actual security should be
Seperating trust and security means distinguishing between issues of ‘hard trust,’ which involve authenticity, encryption, and security in transactions, and issues of ‘soft trust,’ which involve human psychology, brand loyalty, and user-friendliness... [9, p. 21]. Singh and Slegers (1997) [42] unpack issues of ‘soft trust’ in relation to electronic money. They conclude that the user has to feel he or she is in control of the information, that he or she has comfort in the use of the service or channel. The dimension of caring is particularly important as a ‘glue’ for trust in all cases, but particularly where the user does not have the expertise or ability to control the situation.

3) Privacy as the Control of Personal Information
Privacy and security are often seen as synonymous, particularly when privacy is interpreted legally and technically as keeping intruders out of a person’s business. However user centered studies of privacy have emphasized that privacy rests in the control of the sharing of personal information and presenting our version of ourselves [3, 32, 40]. Tognazzini [44] states that “Privacy considerations should be separate and distinct from security... You can build highly secure systems that enhance, rather than reduce privacy” (p. 41). Furthermore, Karat et al. [22] say .... it is becoming increasingly clear that really making our systems secure and enabling appropriate attention to privacy issues will require more than just a technology focus (p. 1).

Issues of privacy in the banking context focus strongly on the risk of losing money via the fraudulent use of the credit card and/or information related to Internet banking. As banks hold detailed personal information about a person’s financial status, there is the additional worry that a leaking of this information could affect a person’s representation of self and also lead to ‘spam’. However, privacy should also lead to an increasing emphasis on personalization and user control over personal information [41].

THE STUDY
We conducted a qualitative study of how people deal with money and banking in the context of their relationships. The sharing of passwords emerged within the broader study of the way people manage money and do their banking in their everyday lives. (We did not begin by asking people whether they shared passwords and it is doubtful such a direct approach would have yielded rich data).

This research is part of a wider project focusing on Security, Trust, Identity and Privacy in the Smart Internet Technology Cooperative Research Centre (SITCRC). The Centre involves the federal government, a state government, industry, small and medium enterprises and universities across Australia.

Our qualitative study, conducted between April 2005 and July 2006, covered 108 people in Australia (Melbourne, rural Victoria and Brisbane). We conducted 84 open-ended interviews, two ‘yarning circles’ (these are like group interviews) with six indigenous people in Brisbane and three focus groups with 18 people with disabilities.

We paid particular attention to the 45 married and 11 de facto couples in our interviews to understand how money is managed between the partners. We also sought to include the indigenous population and people with disabilities, groups traditionally under-represented in the Human Computer Interaction (HCI) and security literature.

We chose a qualitative approach to understand how people deal with issues of security and privacy in personal banking across life stages. We also wanted to go beyond attitudes to behavior. The interviews were transcribed. We used N6, a computer program to assist with qualitative analysis. This meant we first broadly coded the data, then organized the data into matrices to check emerging themes in a transparent manner. It was a ‘grounded’ study in that there was a fit between data and emerging theory, rather than a testing of hypotheses [19].

We also used the N6 computer program for qualitative research to identify negative cases to ensure rigor. We believe that the transparency of analysis is particularly important because we are addressing technologists and industry who were more familiar with quantitative work and metrics. As Morse and Richards [28] say:

The key to rigorous qualitative inquiry is the researcher’s ability … of being constantly aware and constantly asking analytic questions of data, which, in turn, constantly address the questions asked. Qualitative inquiry constantly challenges assumptions, constantly challenges the obvious, reveals the hidden and the overt, the implicit and the taken for granted, and shows these in a new light (p. 170).

The challenging of assumptions was particularly important on two fronts. First, we were challenging the assumptions that money and banking only dealt with economic issues. And second, towards the end of data collection and in the process of analysis, we began to question banking industry and technical assumptions about security.

Sample
The participants were accessed through personal and professional networks. We attempted to cover some of the major socio-economic divisions to understand the diversity of the Australian population. The aim was to understand the issues across these multiple demographics, rather than to generalize. Our sample had:
• 45 men and 63 women. The high number of women was partially explained because more women were managing money particularly in the lower income households;

• Four participants were aged between 18-24; 24 aged 25-34; 28 aged 35-44; 21 aged 45-54; 18 aged 55-64; and 13 aged 65 or over. The 18-24 age group was under-represented as few of them were yet in de facto or marital relationships;

• We had a range of annual household income levels: 25 had an income below $25,000 (all dollar values are in Australian dollars); 25 between $25,000-$49,999; 20 between $50,000-$74,999; ten between $75,000-$100,000; and 21 had over $100,000 a year. Seven participants did not want to disclose their household income.

• 37 participants had a Certificate or lower educational qualification, 64 had a BA or higher degree, four had other qualifications and three did not say. Of those who had a BA or higher degree, at least 11 were in IT.

• We had 70 Australians with an Anglo-Celtic background, 17 with other European heritage; 11 indigenous people (eight Australians of Aboriginal background, and three Australians from the Torres Strait Islands); six associated with Asia; and four associated with Africa and the Middle East.

MARRIED AND DE FACTO COUPLES
In this section we focus on the sharing of Internet and phone banking passwords within the context of married and de facto (cohabiting or common law) relationships in the domestic context.

Sharing Internet banking passwords
Our study shows that when one person in a couple relationship manages the money (pays the bills, and monitors Internet banking) it is not unusual for that person to manage the joint accounts as well as all the individual accounts, including the accounts of the partner. This sharing happens because of trust; not because of a lack of awareness and education.

The form of the account (joint or individual) remains important symbolically in terms of meaning. Sometimes the account symbolizes the ownership of money, but in some cases the different kinds of accounts earmark and separate money according to the source or anticipated use of the funds [39, 47]. But, in Internet banking where passwords are shared, the form of the account no longer defines the boundaries of access to money, or access to information about money. Given a shared password, an individual account operates like a joint account.

In our sample of 84 interviewees, we have 45 persons in married relationships, 11 were de facto; 27 were single, and we do not have information on one. We do not have detailed information on the money management practices of participants of the yarning circles and focus groups. Hence in this section we consider 29 of the 45 married persons and eight of the 11 de facto persons who do Internet banking (37 in total). We do not have specific account information for four of these persons. Of the remaining 33:

• There were 11 cases of joint accounts only (including residual individual accounts with minimal amounts of money) – that is the money was shared;

• Nine persons in couple relationships had individual accounts only that were individually managed. There were no joint accounts;

• In five cases the couple had a joint account and one of the partners also had an individual account. However the partner with the individual account managed all the joint and individual money;

• There were seven cases where the couple had joint and both partners also had individual accounts;

• One person had no account. Her salary went into her husband’s account.

• The issue of sharing passwords arises only when a person is managing the other person’s individual accounts. In our study there were eight such couples. Four couples shared passwords, and four did not. We give their brief stories below.

The common theme among the four who share passwords is that the sharing of passwords is just another example of trust in the partner. Erin (all names are pseudonyms), an administration assistant, 25-34, with an annual household income between $75,000 and $100,000, says:

As far as the bank is concerned they say that no-one else should have your password and that sort of thing but (my husband) trusts me as his wife to have that information and do the transactions that need to be done. We could be breaching security as far (as) the banks are concerned but as a married couple it’s a trust thing. But I wouldn’t go giving it to anyone else.

Tina, 25-34, is married and a marketing professional, with an annual household income of over $100,000. She migrated from the United Kingdom a few years ago, and as a non-resident, found it was complicated to open her own account. So she kept on using her husband’s account.

Her salary goes into her husband’s account, and she earns more than he does. She uses his access card for his account, and she is the one who does the Internet banking. She is also the partner who spends more of the money. Tina says it is a matter of commitment. She says “we’ve been together for seven years now and, you know, I really see him as the
person I’m going to grow old with”. She is going to grow old with him, so what is the issue?

Benjamin, 34, a farmer, is married, with a six month old daughter. Benjamin and his wife have a joint account, and each of them also has an individual account. All bills associated with their house are paid by Benjamin from his account and his wife usually pays for things for their baby. The joint account has their savings. Each of them knows the other’s log-ins. Sometimes his wife logs in as him to pay for the bills. “Now that she is at home (on maternity leave) it is easier for her to do this” Benjamin says. He had also logged in as her a few times to conduct some transactions.

Ellen, 40, is an academic, working part time. She has been in the same de facto relationship for 18 years. They own a home and have two children and a household annual income of over $100,000. Ellen manages all the money, joint and individual. From the main joint account she pays the mortgage, bills, household and children’s expenditure. They transfer an equal amount of money each month to their separate accounts. They have separate credit cards, which are now being paid off from their joint account. At one point she transferred some of her partner’s credit to her credit card as the interest rate was lower. So the distinction between personal and joint is becoming porous. She set up the accounts and linked the card accounts. She says her husband “doesn’t know what the numbers are and he can’t remember” them.

Though some couples share passwords, this sharing does not happen in all cases. There were another four people in our study who had a mix of joint and individual accounts, but each partner managed his or her own individual accounts. In two cases, it was because the wife used her account for household shopping or personal expenditure, whereas the husband managed the more substantial joint account. In two other couples it was because the partner wanted to keep his money separate:

Celia, 45-54, with a household income of more than $100,000 has a blended family. Celia knows her husband has an individual account, but does not know the specific details of the account. Celia thinks the separateness of her husband’s individual account is linked to the separation of money for the child Celia and he share together. This way it doesn’t go towards Celia’s children from a previous marriage.

Faroukh, 45-54, an IT professional, does not usually share information about his individual account with his wife. He keeps it separate in part because he sends money from this account to his mother overseas, as part of his filial obligations.

Sharing Phone Banking Passwords
Couples also share phone banking passwords for their joint credit cards. Bank practice, however, stipulates that the primary account holder alone has the rights to change contact details.

Kevin, 45-54, with an annual household income of more than $100,000 says ‘it’s a pain’ “primarily when one or the other has set up the account or done something and we need to change and we’re not the original signatory, or we’re not.”

Gillian, 35-44, a PhD student in IT, with a household income between $75,000 and $99,999 said she and her husband found themselves in the awkward situation where the bank would not accept her changing the contact details for the credit card for both herself and her husband. She is the one who has the online log-on for the credit card. This is so that they can minimize the number of passwords they have. She says she emailed and asked

…to change our address, our postal and home address because we had moved. They changed mine but they wouldn’t change his, even though I’m a secondary card holder. They said it had to be the primary card holder even though he doesn’t have a log-on. So we had to physically ring the bank and change it, which was really not as secure as it could have been.

This meant that her husband had to ring the bank to give Gillian permission to change the credit card details. She tried to find out if she could change the details in the future and “the bank said ‘No. Every time you want to make any changes, he has to ring and authorize you to talk to me again’. How ridiculous!”

Gillian says,

All we had to do was tell his name, his date of birth, his mother’s maiden name and the account number….If you knew the person you could quite possibly know the mother’s maiden name. ….To me that is not as secure as being able to send an encrypted email through a banking system. There is no point fighting them. They don’t listen.

In this section we have shown that married and de facto couples share Internet and phone banking passwords because they trust their partner and see all their money as joint, irrespective of the form of the account. They have also chosen to have one person manage all the money in the relationship.

AUSTRALIAN INDIGENOUS COMMUNITIES
The qualitative study of banking gave us the opportunity to study the sharing of ATM (Automated Teller Machine) and EFTPOS (Electronic Funds Transfer at Point Of Sale) passwords in the Aboriginal and Torres Strait Islander communities.
cultural practices and the spatial and temporal dimensions of island life.

**Security and Privacy in Remote Aboriginal and Torres Strait Islander Communities**

In remote Aboriginal and Torres Strait Islander communities, especially in the Torres Strait Islands, security and privacy are often compromised due to the lack of banking facilities. Banks are not easily accessible, and the process of obtaining services such as replacing a passbook or getting a keycard involves significant travel costs and time. The sharing of PINs and keycards (for EFTPOS) is a norm that is taken for granted, especially among family members and household clusters. This sharing is not seen as a breach of privacy or security by those in the community, who view it as a matter of survival, especially in areas where banking services are inadequate. The sharing of keycards and PINs is often spontaneous and undertaken to assist family members and friends, especially in situations where they are tied to a particular store or need access to cash. For instance, if the grandparents need to go to a bank, they have to be accompanied by a family member, as the bank staff in Cairns (north of Brisbane) where they do not know the languages of the Islands. However, when family members accompany the older people, bank staff ask them to wait outside, as it is breaching their privacy and security guidelines. So often the grandparents come away without completing their banking.

On Sanna’s island, the keycard used for EFTPOS is the only immediate way of getting cash. Sanna says the older people do not know how to use EFTPOS. So when they have to pre-pay their electricity and water (prepayment is the norm), they use the norm of shared money. The old person will give the card and a piece of paper with the PIN number written on it. And they tell you, ‘Take out $50 for electricity and buy me [an electricity] card’. They tell you, ‘this much for something else, take out this much for groceries’. And then you write it all down and they tell you, ‘OK, so how much is that I need all together?’ So you’ve got to add it all up and tell them, ‘Old Lady that will be $150 or that will be $200’. And they’ll say, ‘OK and get out an extra $50 for me for this or an extra $50 for you for something’.

Sanna says, “You don’t remember [the PIN]. You just use it and give it back to them”.

In this section we have shown how sharing of keycards and PINs is a matter of survival in an area ill-served by banking. This sharing is not seen by those in the community as questionable; it is a matter of survival, and it also is in tandem with a norm of shared money.

**PEOPLE WITH DISABILITIES**

Telephone and Internet banking have increased the independence of many people with disabilities. This is one reason people with disabilities use Internet banking even if they have low income.

We conducted three focus groups with people with disabilities. One group had seven persons with physical disabilities and two able-bodied spouses; another group comprised two people with hearing impairments; and a third group comprised seven persons with vision impairments.
Thirteen of the 18 participants used Internet banking. Of these, twelve had an annual household income of under $50,000. In the rest of our sample, low income meant an unlikely use of Internet banking. Accessibility problems continue with banking in the branches and with the use of banking technologies like the ATMs, EFTPOS, phone and Internet banking. These accessibility problems continue despite the Australian Bankers’ Association (ABA) introducing voluntary industry standards for accessibility in accordance with the Disability Discrimination Act [10, 29].

There are two themes that emerge from our focus groups. The first is that issues of security and identity are at times more important in the physical domain than the digital. Secondly, the lack of accessible banking services necessitates the sharing of passwords and PINs with partners or family members. This sharing also happens at times with carers/support workers or shop assistants in order for transactions to be completed.

Jason 45-54 with a household income of under $25,000 has a physical disability. He says that Internet banking empowers the person with a disability. It gives control where historically the bank used to have the power. Once it is set up it works. The main problem is getting the account in the first place. I don’t have a driver’s license. An 18 plus card isn’t adequate… it’s expensive to get a passport.

This difficulty with establishing physical identity so that one could go on to Internet banking is a common problem in the group. Driving certificates were not possible for many with disabilities. The extract of a birth certificate has to be certified by a Justice of the Peace to be acceptable. Heide, 55-64 had to get her original birth certificate sent from Ireland.

Banking fraud of the ‘old fashioned’ kind still exists. Glen, 55–64, with an Advanced Diploma, and a physical disability, told the researcher after the focus group that he managed his mother’s accounts under an enduring power of attorney. Eight or nine years ago he went to his local branch to check the money in his mother’s three passbook accounts. He suspected one had $75,000. He came back a few months later and there was nothing like $75,000 in it. He went to bank manager and ultimately a staff member was convicted of fraud. He thinks the staff member picked on him because he was in a wheelchair.

The second theme is that inaccessible banking services leave little choice but to have others help with personal banking. Fiona who has a physical disability, aged 35–44, with a Masters’ degree and a household income of $50,000–$74,000, says she withdraws money via EFTPOS, so that the cashier can help with the swiping of the card. She says when I go to do EFTPOS I tell the shop assistant my PIN… I do that on a random basis. Not at the same time every week. Some shop assistants say they can’t do that and I say they have to because I can’t do it.

Grant, 75 is deaf. He depends on tellers to help him. He says:

Before I go to a bank I write a list explaining I am deaf and what I want. The woman then reads it, looks at me and reads it again and gives me the thumbs up. And she does not shout. I say, ‘don’t shout, I’m deaf’. And when I go to the bank another day, I try to go to the same teller who knows me.

Where this kind of help is not available, help has to be sought from parents or other carers. Jamie, 35–44, visually impaired, does not want to seek his parents’ help with his passbook. He says, “My parents can see what my finances are in terms of that account. I’d rather not have to do that. Not a big deal but I’d rather not share the information”. So he is planning to give up his passbook and move into electronic banking.

**SUMMARY AND DESIGN IMPLICATIONS**

In this section we summarize the findings from our qualitative study and discuss the design implications.

**Findings from the qualitative study**

Our study of banking and security practice among three populations shows it is common to share user names, PINs and passwords:

- In married and de facto relationships this sharing is an expression of trust rather than a lack of awareness of the need to keep access codes confidential;
- For remote indigenous populations, sharing is a key to survival and is the only feasible way of getting cash. Banking services are sparse or non-existent far from major mainstream population centers; and
- Many people with disabilities often need the help of others with their banking, both in terms of face-to-face interactions (with retail clerks and bank tellers), and to use machines that rely on physical and sensory abilities such as ATMs and EFTPOS devices. For many people with disabilities, sharing of access codes is the only way to obtain most goods and services.

Our findings reveal usage patterns from Australia that have wide applicability. Sharing of passwords, where studied, is equally common in other populations. Dhamija and Perrig [12] interviewed 30 people to test the comparative usability of recognition-based and recall-based authentication. They did not say where this population was located, though it is likely to be in the United States. They found that in recall based authentication systems:
...people viewed the ability to share passwords with others as a feature. Almost all participants shared their bank PIN with family or friends and several users shared account passwords with others because this was a convenient way to collaborate, share information or transfer files (no page numbers).

The sharing of passwords is now emerging as an issue for estate planning. A CNET.news.com piece [27] says

“As more and more people move their lives, address books, calendars, financial information, online, they are taking a risk that some information formerly filed away in folders and desks might never be recovered (no page numbers).

Some of the proposed solutions were to include a key password in estate planning, or to have it on a USB drive in a safety deposit box. But as one of the 34 people who commented on the article said, “What you need is to have a person in your life that you trust enough, so that (s)he can know your password. Then there’s no problem.”

Sharing of passwords is even more likely to be common in developing nations, where technologies such as email, and the mobile phone are routinely shared.

**Design implications for banking security systems**

The implications from our findings and the results of related research lead us to believe that security systems need a re-evaluation in terms of password and user name sharing. Though current authentication practices for banking shield providers from risk, the practices go against observed everyday use. This gap between authentication systems and social practice leads to a weakening of overall security because:

- Customers in married and de facto relationships are not able to personalize their security practices to fit the way they conduct their money management activities;
- Banks have not provided usable ways of accessing cash and services in remote areas, and
- Lack of accessibility means that people with disabilities have to share confidential information in order to bank and make purchases.

Thus, security awareness programs targeted to the consumer, which do not take into account social practice, are bound to fail to meet their aims. Unlike Dhamija and Perrig [12] who argued for recognition based software so that people cannot share passwords, we propose that security design should take into account social and cultural practice and enable the sharing of passwords. The design should minimize the risks, while allowing customers to personalize the degree and limits of sharing.

We propose the following principles for design that have implications for the way banking security systems are structured. These principles are purposefully broad. They are intended for people in the banking industry and security designers who are in a position to develop and implement the application solutions.

The overarching approach is that design should build on people’s social and cultural practices. The design has to go beyond the individual user to seeing a person in the context of his or her social relationships and cultural meanings. This leads to five principles:

1. Security systems should be flexible in allowing for delegation so that more than one person can access account information, when all persons involved agree.
2. Security design should involve personalization so that the customer has choices about sharing information to varying extents with different people. This personalization will allow customer control over his or her personal information, and increase customer trust.
3. Security design should take into account the need to access banking services in remote areas.
4. The design of security needs to encourage accessible services for people with disabilities.
5. In designing security systems to meet social contexts of use, the continuum between physical and digital security needs to be addressed.

The sociological approach to the study of media and communication encourages thinking about the way people experience security in the physical and digital worlds [14, 15, 20, 26].

Accepting the need to consider the sharing of passwords in security design will mean a change in the metaphors of security and ways of studying users. At present, the military metaphors of defence and attack underlie security development. But as our paper shows, in domestic contexts, not sharing a password to a bank account can signal a lack of trust. An emphasis on the controlled sharing of information would mean we would be able to build secure systems that enhance trust, privacy and personalization.

The sociological underpinnings of security design have to be built on empirical studies in the everyday social and cultural contexts of the user. Empirical sociological studies may become even more important when we go beyond the cultural boundaries of Australia and the developed countries, to India and China. Given infrastructure and affordability issues, the assumption of the individual user in front of a personal computer is even more questionable. It is the publicly shared Internet kiosk or the mobile phone which will underpin Internet transactions in many communities. Values of trust and shared use should become a necessary central consideration in security design.
Our conclusion overall is that we need to extend the user centered security approaches and the emerging work on security in the organizational context. We need to go beyond the individual user in front of his or her individual computer or users in the organizational context of the workplace, to shared use in the domestic context. Security design needs to take into account the importance of social and cultural practice. Without such an approach, the gap between social practice and security design can lead to a lessening of the security of digital banking systems.

ACKNOWLEDGMENTS
We acknowledge the support of the Smart Internet Technology Cooperative Research Centre in making this research possible (www.smartinternet.com.au). We would also like to thank Jenine Beekhuyzen, Margaret Jackson, Chris Law, Jan Browne, Lesa Beel and Doug Lorman for their help with the project.

REFERENCES


38. Senior, K., Perkins, D. and Bern, J. Variation in material wellbeing in a welfare based economy, South East Arnhem Land Collaborative Research Project, University of Wollongong, Wollongong, 2002.


