Security Design Based on Social and Cultural Practice: Sharing of Passwords

Supriya Singh[1], Anuja Cabraal[1], Catherine Demosthenous[2], Gunela Astbrink[3], and Michele Furlong[4]

[1] Smart Internet Technology Cooperative Research Centre/RMIT University, GPO Box 2476V, Melbourne 3001, Australia
{Supriya.singh,anuja.cabraal}@rmit.edu.au
[2] Smart Internet Technology Cooperative Research Centre
[3] Smart Internet Technology Cooperative Research Centre/GSA Information Consultants, GSA Information Consultants
PO Box 1141, Toowong, QLD, 4066, Australia
g.astbrink@gsa.com.au
[4] Smart Internet Technology Cooperative Research Centre/GSA Information Consultants, GSA Information Consultants, PO Box 1141,Toowong, QLD, 4066, Australia
mfurlong@iinet.net.au

Abstract. We draw on a qualitative study of 108 people to examine the routine sharing of passwords for online banking among married and de facto couples, Aboriginal users and people with disability in Australia. The sharing of passwords goes against current banking authentication systems and consumer protection laws that require customers not to reveal their access codes to anybody, including family members. The everyday violation of these security requirements results from the lack of fit between security design and social and cultural practice, rather than a lack of security awareness. We argue for the need to go beyond individualistic user-centered design, so that social and cross-cultural practices are at the centre of the design of technologies. The need for a social and culturally centered approach to design is even more important when dealing with different notions of privacy across cultures and a culture of shared use in public and private spaces.

Keywords: Banking; security; Australia; sharing passwords, social and cultural centered design, privacy across cultures.

1 Introduction

Banking security design assumes an individual keeps his or her access codes confidential while conducting Internet transactions using a personal computer. In this paper we argue that these assumptions are against common social and cultural practices. There are multiple situations where the individual shares access codes particularly with members of the family. Internet transactions are also not always conducted on a personal computer, whether at home or in the work place. Hence we

N. Aykin (Ed.): Usability and Internationalization, Part II, HCII 2007, LNCS 4560, pp. 476–485, 2007.

are arguing that for the "effective use" of technologies, design and policy should be built on social and cultural practice.

Banks use what you know – usernames, Personal Identification Numbers (PINs) and passwords - as the first order of authentication. At times, this first order of security can be complemented by what you have (such as tokens) and who you are (biometrics). Australian banks like Westpac Banking Corporation tell consumers on their web sites not to disclose their access codes to "any third party including family, friends and institutions" [39]. If the access codes are disclosed, the consumer is not protected under the Electronic Funds Transfer Code of Conduct (2002) [5]. The Code states that 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). Breaches of this confidentiality are primarily dealt with through consumer education leading to increased security awareness [3].

There is an equally strong presumption that Internet transactions will not be conducted in cyber cafes or on other publicly shared computers. Westpac drawing on material from the Australian Bankers' Association actively discourages consumers from using publicly accessed computers. Westpac says "It is important to use only a trusted and secure computer to access your Internet banking account. Using publicly shared computers, such as those at Internet cafes, is strongly discouraged"[39]. The State Bank of India has a similar warning on its site, despite the fact that for most Indians, Internet is accessed primarily via publicly shared computers. The State Bank of India while welcoming users to use Internet banking warns "However, as a matter of precaution and safety, he should avoid using PCs with public access"[35].

In Section 2 we draw on a qualitative study of 108 people in Australia to show that passwords are routinely shared in some situations by different user groups. In section 3 we draw attention to public and shared access to the Internet in India and different cultural notions of privacy. In the concluding section we build on perspectives of user centered security to propose a social and culturally centered approach to design so that security design is based on social and cultural practice.

2 The Study

We[1] conducted a qualitative study of how people deal with money and banking in the context of their relationships. This research is part of a wider project focusing on Security, Trust, Identity and Privacy in the Smart Internet Technology Cooperative Research Centre. Our qualitative study conducted between April 2005 and July 2006, covered 108 people in Melbourne, rural Victoria and Brisbane in Australia. We attempted to cover the diversity of the Australian population to understand the issues rather than to generalize. We conducted 84 open-ended interviews, two 'yarning' circles (these are more like group interviews) with six Indigenous people in Brisbane and three focus groups with 18 people with disabilities. The interviews, focus groups and yarning circles were transcribed. We used the N6 computer program for qualitative research to analyze the data and identify negative cases to ensure rigor. This meant we first broadly coded the data, then organized the data into matrices to check emerging themes in a

[1] We are grateful to Jan Browne, Jenine Beekhuyzen, Gabriele Hermansson, Margaret Jackson, Lesa Beel and Doug Lorman who also helped conduct the qualitative study.

transparent manner. It was a ‘grounded’ study in that there was a fit between data and emerging theory, rather than a testing of hypotheses [15].

2.1 Sample

The participants were accessed through personal and professional networks. The aim was to understand the issues across the major socio-economic groups in Australia, 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.

2.2 Sharing Passwords

In our study, three groups of people shared banking passwords, in different social contexts. Married and de facto (cohabiting) couples who shared passwords to their individual accounts, saw it as a matter of trust and convenience. Indigenous people in remote areas shared passwords and cards to access EFTPOS and withdraw money from ATMs, because of a lack of banking services. People with disabilities had to share passwords because they needed help in order to complete a banking transaction.

Our qualitative study shows that when one person in a couple relationship manages the money, that is 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. The form of the account, whether it be joint or individual, remains important in terms of meaning. This is because different kinds of accounts earmark and separate money according to ownership and source of the funds [32, 43]. In the case of Internet banking where passwords are shared however, the form of the account no longer defines the boundaries of access to money, or information about money.

In our study we had eight couples with joint accounts where both partners also had individual accounts. In four of these cases, one partner managed all the accounts, including their partner's individual account. With the other four couples each person managed his or her own individual account.

Where the couple's joint and individual money was managed by one of the partners (4 of 8), this was possible because the spouse had given him/her the password. As Erin (all names are pseudonyms), an administration assistant, 25-34, with an annual household income between $75,000 and $100,000, said,

> 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.

The sparse literature on Indigenous banking in remote areas shows that key cards and access codes are often shared [7, 26, 31]. In our study, Sanna, a Torres Strait Islander now living in Brisbane, 45-54, with a BA and earning more than $50,000 a year, talked of banking on her island. She described how the bank was only on one of the 17 inhabited islands. A plane trip and a one night stay were required to get to that island. She said "When one person goes into Thursday Island they [do] everybody's business and shopping". This means they take others' keycards with the PINs. "You have to" said Sanna, "It's a matter of survival".

Telephone and Internet banking have increased the independence of many people with disabilities. However, 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.

Fiona who has a physical disability, aged 35-44, with a Masters' degree and a household income of $50,000-$74,000, said she withdraws money via EFTPOS, so that the cashier can help with the swiping of the card. She said, "When I go to do EFTPOS I tell the shop assistant my PIN… Some shop assistants say they can't do that and I say they have to because I can't do it."

Sharing of passwords, where studied, is equally common in other populations. Dhamija and Perrig [10] interviewed 30 people (most likely in the United States) to test the comparative usability of recognition-based and recall-based authentication. They found that:

> …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).

In this section we have presented qualitative data that reveals that the sharing of passwords for banking is found among couples, in remote Indigenous communities and with people with disabilities. There is evidence from other literature where people see the possibility of sharing passwords as a useful feature of design.

3 Public Access to the Internet

In this section we examine the second underlying assumption of banking security design and policy—that every household will have its own Personal Computer or other personal access device. The Australian pattern follows that of Internet access in developed countries. Sixty-seven per cent of Australian households in 2004-05 accessed the Internet from home [4]. In the same period however, seven percent of the Australian population aged over 18 years accessed the Internet from the public library, and 12 per cent from other sites (excluding home, work, educational institution, neighbours, and friends).

In countries like India, as Sadagopan reminds us "While PC stands for Personal Computer elsewhere, in India it represents a Public computer" [27]. This public access can be provided by commercial Internet access points where customers pay a fee for service (at times called cybercafés), or the free Internet access points for development, in libraries or other institutional places targeting a specific audience. There are also rural kiosks that are run by commercial entities such as ITC's e-chaupal, government initiatives such as e-Seva, and entrepreneurial projects run by NGOs such as those by the M. S Swaminathan Foundation. Others are run by individuals.

Concentrating only on the urban commercial cybercafés [16], Haseloff said, "…as much as one-third of the middle class is dependent on cybercafes as their only access point " (no page number). Estimates of the number of cyber cafés and Internet kiosks in urban and rural areas range from 105,000 to 200,000 cyber cafés in India in 2005 (accounting for 60% of net users) [19, 25].

3.1 Internet Banking and E-Commerce at Indian Cybercafés

Internet cafes and kiosks are important in India, not only for incidental communication and searching, but for Internet banking and the estimated $US 498 million e-commerce industry in 2006-2007 [19]. This is one of the main findings of surveys by industry associations Internet and Mobile Association of India and Internet & Online Association [20].

The Internet and Online Association's urban online survey of 3,099 Internet users in April 2005 [20] showed that more than a quarter (28 %) of these respondents accessed the Internet from the cyber café. This was not the dominant mode of access for e-commerce, as 65 per cent accessed e-commerce sites from the office, and 52 per cent from the home.

The Internet and Mobile Association of India (IAMAI) also conducted an online survey of 882 persons who regularly visited e-commerce sites from cyber cafés. Of these, 47 per cent (417 persons) had shopped online more than once. Of these 417 persons, 58 per cent did online banking. This sub-sample as with the IAOI survey had an over representation of males (87%), 18-35 years of age (84%) and those with graduate and postgraduate degrees (80%).

The survey findings are in conflict with bank advice that customers avoid banking using public computers. The need is to ensure that publicly accessed computers are secure and seen as secure by customers. As Sadagopan [27] notes, security "is indeed a serious problem & cannot be taken lightly".

The level of fraud in Internet banking in India is unclear. It is also unclear what protections the Indian consumer has in case he or she loses money from his or her Internet banking account accessed from a cyber café. However, the bank's warning against the use of Internet cafes for Internet banking reflects the greater potential for such fraud from public kiosks.

3.2 Shared Use of Mobile Phones in Developing Countries

Mobile phones are emerging as an important way of accessing the Internet. As the Internet and Online Association's urban online survey [20] shows, seven percent of their sample in India access the Internet from the mobile phone. Toyama et al. [36] noted it is possible

> …that the most compelling scenarios will be hybrid experiences, where a shared-access kiosk provides a full Internet experience occasionally, and pre-paid mobile phones provide a shallow experience continuously. Neither mobile providers nor computing firms have emerged with such a solution thus far (p. 9).

The security problems posed by mobile phone access to the Internet are those of mobile applications everywhere. But unlike Japan, the United States, Europe and Australia, in India and other developing countries, individually owned mobile phones are often shared [6, 12, 24, 37, 38]. As noted in the Information Economy Report (2005) [37]

> …in developing countries a single mobile phone is frequently shared by several people, particularly in poor, rural communities, and people at all income levels are able to access mobile services either through owning a phone or using someone else's (p. 12).

The leasing of mobile phones in the villages of Bangladesh by Grameen Bank is based on shared use [6]. A 2004 study of rural municipalities in the Philippines found that 15 per cent of the cell phones were family owned but 62 per cent allowed others in the household to receive and respond to messages [24].

The sharing of mobile phones is common in Africa [38]. In Rwanda as Donner notes [12]:

> …in Africa, as elsewhere in the developing world, handsets often pull double-duty, used by multiple family members, shared among friends (perhaps by swapping SIM cards in and out), or perhaps by a whole set of users in a village or neighborhood. Across the region, many people make their living by selling individual calls on handsets. These micro-entrepreneurs play an important function in extending connectivity to people who can not afford their own handset, or who might only require an occasional call (p. 2).

3.3 Cross-Cultural Attitudes to Privacy

With an increasing global flow of money and information, it has become critical to study privacy attitudes and behaviours for different activities, social contexts and technologies, in a cross cultural framework. In our approach to privacy, we draw on user centered studies that have emphasized that privacy rests in the control of the sharing of personal information and presenting our version of ourselves [2, 8, 23, 34]. Cross cultural research is also important because the right to be left alone is seen as less important than connectedness to family and community in some activity contexts, in some countries. This argument draws on broader theories of the cultural differences between countries [18]. The move towards indigenous psychologies also emphasizes the relatedness of individuals over individual autonomy [17].

Some cross cultural research is happening in the context of the use of media. As Livingstone [22] says, in a global world, it is difficult not to do cross cultural research. Much of the comparative research, particularly with mobile phones and other new media, is happening within the Western developed countries, or across diverse groups within the same country. There is also the beginning of cross cultural research in the use of media in developing countries. Research on privacy laws across borders is also becoming more important. However, the cross cultural research on privacy, where it exists, still has to be more clearly linked to design and policy.

The sharing of mobile phones and the comfort with public telephones and cybercafés in India is part of broader boundaries of the privacy of personal information. Some of the most distinctive cultural differences related to privacy lie in the boundaries of domestic money [25]. Among middle income Anglo-Celtic married couples, money and information about money is often shared by the couple, but not always between the parents and children. Money also flows in one direction, between parents and children, and at times between grandparents and children. However in many other cultures, money and information about money also flows from children to parents. Using money as a medium of family relationships has been central to the $US167 billion in migrant remittances flowing back to developed countries in 2005 [41].

Even within Western countries, there are cultural differences about the privacy of money. In Australia, among Aboriginal groups, money is shared within an extended family, kinship group or household cluster. [28, 31]. Similar differences are also found for Islander and Maori families in New Zealand [14].

Greater research on the privacy of money needs to be done in developing countries. In what contexts is it appropriate to ask about money earned, money spent? What are the culturally appropriate ways of not answering these questions?

Personal information too is shared in different ways across cultures. Genevieve Bell, Director of the User Experience Group, Intel, in her keynote address at OZCHI 06 noted it was not unusual for Indian families to have a single email address. It is a common practice in India and Korea for educational institutions to post students' full names and grades on public notice boards or newspapers [21, 40].

There has been little discussion of the impact of these cross cultural differences in the privacy of personal information, particularly money, on design and policy. Kumaraguru (2005) drawing on a sample of 407 persons in companies and universities found that people in the high-tech workforce may not be "sufficiently aware of privacy issues in general, and more specifically, privacy issues related to technologies".

4 Conclusion: Social and Cultural Centered Design

Our study of banking in Australia showed that banking access codes were shared in some contexts by married and de facto couples, Indigenous people in remote communities and people with disabilities. The literature on public access and shared devices in India and other developing countries revealed that public access and shared devices are one of the main ways of accessing the Internet.

The security implications of these social and cultural practices have yet to be considered by designers, bankers and policy makers. The usual industry and policy reaction to access codes not remaining confidential is to propose further education of customers, or more stringent laws. Our study showed that people with a high education were also sharing access codes. The sharing was in response to a customer need, whether it be trust in the couple relationship, lack of banking services or accessibility.

We argue that social and cultural practices need to be placed at the center of design. To do this we need to extend the perspectives of user centered design (UCD) in three directions. The UCD approach places the user at the centre of security design, aligning usability and security [1, 9, 11, 13, 29, 30, 33, 42]. First, we need to expand from the individual alone or the individual in an organisation to the domestic context of individual and shared activities in the household. Second, these activities and values need to be studied in the field. Third, the cultural meanings of online financial transactions have to be taken into account. This is particularly important as money is used, managed and owned in different ways in various cultures [32].

These approaches will help link design, policy and practice. They will also bridge the household experience with national and international approaches. It is only with such connections, that the Internet can deliver its potential for individual and community empowerment across cultures.

References

1. Ackerman, M.S.: The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. In: Carroll, J.M. (ed.) Human-Computer Interaction in the New Millennium, pp. 303–324. ACM Press, New York (2002)
2. Agre, P.: Introduction. In: Agre, P., Rotenberg, M. (eds.) Technology and Privacy: The New Landscape, pp. 1–28. The MIT Press, Cambridge, Mass (1998)
3. Australian Bankers' Association Inc. Stay safe online: ABA supports the e-security awareness week, Australian Bankers' Association Inc. (2006)
4. Australian Bureau of Statistics. Household Use of Information Technology, Australia, 2004-05, Australian Bureau of Statistics, Canberra (2005) Cat No. 8146.8140
5. Australian Securities and Investment Commission. Electronic Funds Transfer Code of Conduct: As revised by the Australian Securities & Investments Commission's EFT Working Group, Australian Securities and Investment Commission, Sydney (2002)
6. Bayes, A., Braun, J.v., Akhter, R.: Village Pay Phones and Poverty Reduction: Insights from a Grameen Bank Initiative in Bangladesh, ZEF Bonn, Zentrum für Entwicklungsforschung, Center for Development Research, Universität Bonn, Bonn (1999)

7. Birdsall, C.: All in the family. In: Keen, I. (ed.) Being Black: Aboriginal cultures in 'settled' Australia, Aboriginal Studies Press for the Australian Institute of Aboriginal Studies, Canberra, 137–158 (1994)
8. Castro, M., Singh, S.: Rigour at a trotting pace: A story from the user-centred design of smart internet technologies. In: QualIT, Brisbane (2004)
9. Cranor, L.F., Garfinkel, S.: Preface. In: Cranor, L.F., Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems that People Can Use, O'Reilly, Sebastopol, CA, ix-xviii (2005)
10. Dhamija, R., Perrig, A., Déjà, V.: A User Study Using Images for Authentication. In: Proceedings of the 9th USENIX Security Symposium Denver, Colorado, USA, 2000, The USENIX Association, No page numbers (2000)
11. D'Hertefelt, S.: Trust and the perception of security (2000)
12. Donner, J.: User-led innovations in mobile use in sub-Saharan Africa Receiver Newsletter#14 (2005)
13. Erickson, T., Kellogg, W.A.: Social translucence: Designing systems that support social processes. In: Carroll, J.M. (ed.) Human-Computer Interaction in the New Millennium, pp. 325–345. ACM Press, New York (2002)
14. Fleming, R., Taiapa, J., Pasikale, A., Easting, S.K.: The Common Purse. Auckland University Press, Auckland (1997)
15. Glaser, B.G., Strauss, A.L.: The discovery of grounded theory: Strategies for qualitative research. Aldine, Chicago (1967)
16. Haseloff, A.M.: Cybercafes and their Potential as Community Development Tools in India, The Journal of Community Informatics (2005)
17. Ho, D.Y.F.: Indigenous Psychologies: Asian Perspectives. Journal of Cross-Cultural Psychology 29, 88–103 (1998)
18. Hofstede, G.: Cultures and Organizations: Software of the Mind. McGraw-Hill, New York (1997)
19. Internet and Mobile Association of India. Cybercafé Users Ecommerce Activities, Internet and Mobile Association of India (2005)
20. Internet and Online Association. IOAI Survey: Ecommerce Security 2005, Internet and Online Association (2005)
21. Kumaraguru, P.: Internet Privacy in India Hot Topics, Carleton University (2005)
22. Livingstone, S.: On the Challenges of Cross-National Comparative Media Research. European Journal of Communication 18(4), 477–500 (2003)
23. Palen, L., Dourish, P.: Unpacking privacy for a networked world. In: Proceedings of the conference on Human factors in computing systems, Ft. Lauderdale, Florida, USA, pp. 129–136. ACM Press, New York (2003)
24. Pertierra, R.: Mobile Phones, Identity and Discursive Intimacy. Human Technology 1(1), 23–44 (2005)
25. Ranjan, A.: Milestones in India's Internet Journey (2005)
26. Renouf, G.: Bookup - some consumer problems. A report for ASIC (2002)
27. Sadagopan, S.: Why I feel e-commerce will fly in India?, IIITB, Bangalore, n.d.
28. Sansom, B.: A grammar of exchange. In: Being Black: Aboriginal cultures in 'settled' Australia, Aboriginal Studies Press for the Australian Institute of Aboriginal Studies, Canberra, pp. 159–177 (1988)
29. Sasse, M.A., Flechais, I.: Usable security: Why do we need it? How do we get it? In: Cranor, L.F., Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems that People Can Use, O'Reilly, Sebastopol, CA, pp. 13–30 (2005)

30. Schneier, B.: Secrets and lies: Digital security in a networked world. John Wiley & Sons, New York (2000)
31. Senior, K., Perkins, D., Bern, J.: Variation in material wellbeing in a welfare based economy. In: South East Arnhem Land Collaborative Research Project, University of Wollongong, Wollongong (2002)
32. Singh, S.: Marriage money: the social shaping of money in marriage and banking. Allen & Unwin, St. Leonards, NSW (1997)
33. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., Furlong, M.: Password Sharing: Implications for Security Design Based on Social Practice. In: Computer Human Interaction, San Jose, ACM, San Jose, New York (2007)
34. Singh, S., Zic, J., Satchell, C., Bartolo, K.C., Snare, J., Fabre, J.: A Reflection on Translation Issues in User-Centred Design. In: 7th International Conference on Work with Computing Systems, WWCS 2004 (Kuala Lumpur, 2004) (2004)
35. State Bank of India. Internet Banking: Welcome Aboard, State Bank of India (2006)
36. Toyama, K., Kiri, K., Ratan, M.L., Nileshwar, A., Vedashree, R., MacGregor, R.F.: Rural Kiosks in India, Microsoft Corporation (2004)
37. United Nations Conference on Trade and Development. Information Economy Report 1005, United Nations, New York and Geneva (2005)
38. Vodafone. Africa: The Impact of Mobile Phones The Vodafone Policy Paper Series (2005)
39. Westpac Banking Corporation. Internet Banking Terms and Conditions, Sydney (2006)
40. Woo, J.: Invasion or giving up of Internet privacy? A personal divide emerges. In: Pacific Telecommunications Conference (Honolulu, 2001) (2001)
41. World Bank Global Economic Prospects 2006: Economic Implications of Remittances and Migration. World Bank, Washington DC (2006)
42. Yee, K.-P.: Aligning Security and Usability. IEEE Security and Privacy 02(5), 48–55 (2004)
43. Zelizer, V.: The social meaning of money. Basic Books, New York (1994)