

# 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**  
Smart Internet Technology  
Cooperative Research Centre  
Griffith University  
School of Information and  
Communication Technology  
Nathan, QLD, 4111, Australia  
c.demosthenous@griffith.edu.au

**Gunela Astbrink  
Michele Furlong**  
GSA Information  
Consultants  
PO Box 1141  
Toowong, QLD, 4066,  
Australia  
g.astbrink@gsa.com.au  
mfurlong@inet.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.*