

Phishing Tackle: how Identrica fights identity fraud

“Phishing” is the fastest-growing problem for Internet banking.

Identrica can solve it – at a commercially viable cost.

The problem...

The number of “phishing” attacks – where innocent e-banking customers are duped into revealing their passwords and identity details – is growing exponentially. The direct cost of these frauds runs into many millions, but the real cost to banks is that customers are reluctant to switch from expensive High Street accounts to Internet banking.

Classic “phishes” were often badly-written e-mails asking customers to validate their account details by clicking on a link – which takes them to a bogus website where they are invited to “log on”, revealing their passwords and other identity details. Their bank accounts were then raided. So far the banks are still picking up the bill.

Recent attacks have become much more sophisticated. Simply previewing an e-mail can have browser “favourites” changed to point to a fake bank site instead of the real one. Or a “Trojan horse” program can lie dormant until a (genuine) bank site is visited: then the program records the login details and covertly e-mails them to the phisher. Customers don’t have to be stupid or even specially careless to get caught. So what can be done?



...and how to fix it

The best solution is Two-factor Authentication (2FA). Customers need both to *know* something (their password or PIN) and to *possess* something unique to them. Then it doesn’t matter if they are fooled into giving away their password and other “secrets” – unless the phisher physically steals their token, he can’t get in.

ATM cards are the commonest form of 2FA – but of course they don’t work across the Internet. So for Internet applications the physical “token” is conventionally a smartcard, a USB stick or an electronic “authenticator”. All of these work well – but they are expensive to buy, and complex to use and administer. This makes

them unsuitable for high-volume, low-margin applications like Internet banking.

The affordable solution

Identrica uses the customer’s mobile phone as the “token”. This innovative solution simply asks the user to make an unanswered (so *free*) call from their registered mobile phone as part of the normal log-on procedure. As soon as the phone rings the customer can hang up. Because the customer provides his or her own “token” the bank has no capital outlay and minimal administration costs. *Identrica* can be used both for initial log-on and for individual transaction authorisation.

Identrica is a “zero-install” solution, with no need for a separate authentication server and no extra hardware for customers to carry – or lose. With nothing more than their standard mobile phone they can securely access their accounts from home, office, Internet café, WiFi hotspot or PDA.

Identrica can save banks money by countering the burgeoning threat of Internet identity theft. Offering robust Two-factor Authentication, conveniently and at a fraction of the cost of other products, Identrica is the only practical, commercially viable solution available today.

Simple, secure, affordable authentication

