SECURITY - INTERNET

"Is Internet Banking safe? How can I be sure I am protected?" <customer>

Security and customer protection are critical for any financial service. Internet banking security is an increasing concern for many customers and their financial institution.

The Customer Value Proposition

SAFE – Ensure your customers are safe from malicious attacks on Internet Banking.

TRUSTED – Additional security features are welcomed by customers. The customers of more than 60 Credit Unions are already using and trusting this system to keep them protected while using Internet Banking.

31% of all bank customers used Internet Banking in the June 2007 Quarter.

- MISC Australia, Dec 2007

CONVENIENT – Factor2™ integrates seamlessly into the Internet Banking logon process

EASY TO USE – No requirement to carry physical tokens or to install special access software

The Business Value Proposition

SECURE – Factor2™ provides a tiered structure of security options to provide the best solution for your customers and your business.

RETAIN – Ensure your customers feel safe and continue to use Internet Banking rather than changing to a channel with a high-cost to serve.

ACQUIRE – A strong and secure Internet Banking value proposition is attractive to potential business and personal customers.

SERVE – Simple designs ensure security does not impact the customers ability to perform their online banking.

DEFEND – Protect your brand and reputation and stay ahead of the rest.

Features at a Glance – Factor2™

Factor2™ provides a tiered structure that can be tailored to meet your business needs.

Front line defence - Customer driven protection

- Level 1 security is the inbuilt username and password components of Internet Banking, we recommend teaming this with a captcha phase to provide basic security.
- Level 2 provides Factor2™ Personal Icons, a user interface security mechanism that presents customers with visual cues to ensure increased security at every Internet Banking logon.
- Level 3 Easy to use SMS out of band authentication to protect high value transactions and for creation of new payees and billers
- Level 4 As an alternative to SMS, using hardware tokens for the provision of one-time use passwords, again for use with high value transactions and for creation of new payees and billers.

Factor2™ is designed to integrate quickly into your system to minimise the impact on your Internet service whilst delivering robust and trusted security to your customers.

Server based defence - Behaviourial driven protection

- Level 1 payment level verification engine – rules based behaviourial screening
- Level 2 RSA adaptive authentication solution – global 3rd party, risk based authentication

SECURITY - INTERNET

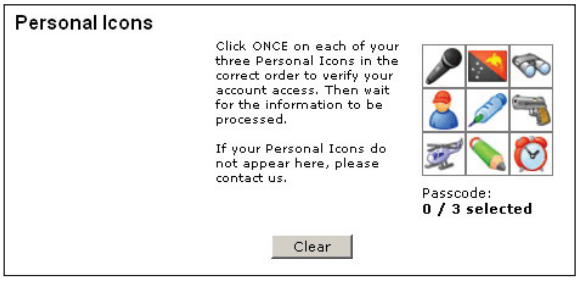
23,630 unique phishing sites detected worldwide in November 2007.

Anti Phishing Working Group, Jan 2008

How do Personal Icons work?

At registration for Internet Banking the customer selects three memorable icons from the catalogue of Personal Icon images

After successful logon with their username and password, the customer must identify these three images from nine randomly generated icons, in the correct order, before proceeding to access their accounts.



Avoid awkward questions

The Board wants to know if your Internet Banking platform is secure and that emerging threats are being managed.

Do you have the answer?

Contact us today for a demonstration.

Contact us today to find out more

Phone +61 2 9283 5221

solutions@rubik.com.au

brochure