

FORUM WRAP-UP

Combating multi-channel banking fraud



SECURITY 2008
Combating multi-channel banking fraud in an increasingly connected world
Thursday June 26th, Sydney

AGENDA

10:00am Registration opens	10:45am Networking break	2:25pm The evolving nature of identity theft
11:00am Anticipating multi-channel fraud	11:00am Anticipating multi-channel fraud	How fraudsters use multiple channels to steal identities
11:30am Introduction from the Chair: Stephen Overton, Planning Security Consultants, VeriSign & Chase	11:30am Thinking like a fraudster	Cybercrime trends: Stephen Wilton, Loyalty Consulting
1:00pm Fraud, advanced information, and attacks on integrity	1:30pm Interactive roundtable session	3:30pm Networking break
1:30pm Fraud, advanced information, and attacks on integrity	1:30pm Interactive roundtable session	3:30pm Securing the mobile channel
1:30pm Fraud, advanced information, and attacks on integrity	1:30pm Interactive roundtable session	4:00pm Panel session: Assessing the accuracy of credit solutions for online banking fraud
1:30pm Fraud, advanced information, and attacks on integrity	1:30pm Interactive roundtable session	4:00pm Panel session: Assessing the accuracy of credit solutions for online banking fraud
1:30pm Fraud, advanced information, and attacks on integrity	1:30pm Interactive roundtable session	4:00pm Panel session: Assessing the accuracy of credit solutions for online banking fraud

Developed by:   

Security gets personal

A financial institution is going the extra mile by bringing security to individual PCs

BY CHARIS PALMER

BCU has become the first financial institution to adopt PC level security for Internet banking after signing a deal with security solutions provider TrustDefender. The regional credit union will provide the solution to its customers at no cost, and argues it is a level of security protection not offered by any other bank or financial institution in Australia. Launching the service at *Online Banking Review's* security forum, Gillian French, general manager of marketing with BCU told the audience, "People are not using Internet banking, or purchasing online as much as they could".

French says "This is more than just an innovative solution, it's a powerful tool that will encourage more members to regularly use Internet banking, and ultimately we hope it will bring more customers to BCU".

The solution performs a security "health check" on the consumer's PC or mobile device, identifying any unknown crimeware that may exist on the machine before the consumer logs on to online banking.

BCU already offers one-time password tokens and is a member of the VeriSign/Australia Post VIP network. Head of technology David Lang says "We felt we needed to be doing a little bit more than that".

Lang says "We can take every effort to protect Internet banking use, but we can't go out and protect the actual systems of

our members, and members often don't understand the intricacies of anti-virus software".

It's a view loosely shared by AusCERT general manager Graham Ingram. Ingram says that with the growing incidence of zero-day exploits which target anti-virus software, consumer education has a limited effect. "We can do all the user awareness [raising] in the world, but still people click on the .exe [file] and run it. All the education comes quickly undone when we've got a population that is click happy."

TrustDefender co-founder Andreas Baumhof says "We've had anti-virus engines for 15 years and still viruses are a real problem...we need to have much more innovation in trying to solve the problem".

French says "We know that cybercrime is now bigger than the illicit drug trade and with people using social networking sites, accessing more websites and purchasing online, the risk that cybercrime will happen is increasing at a significant rate - particularly if you do your Internet banking on the same PC that your teenage daughter uses".

BCU members will gain free access to the TrustDefender solution when banking with BCU, but can also choose an upgrade to use the solution with other institutions or eCommerce providers for a flat fee of \$US19.95.

French says by covering the cost for its members the barrier of price has been removed. "If they want to

then extend that protection to other transactions on the net they can upgrade to the gold version which will provide them with additional security on other sites."

And the software can be installed in less than a minute, removing the barrier of inconvenience, which French says stops many people from taking measures to protect themselves online.

Point solutions are no longer good enough for the way fraudsters are working

Benn Dullard, technical director, Eunexus

When you get the upgrade pack for Web 1.0 to Web 2.0 just let me know

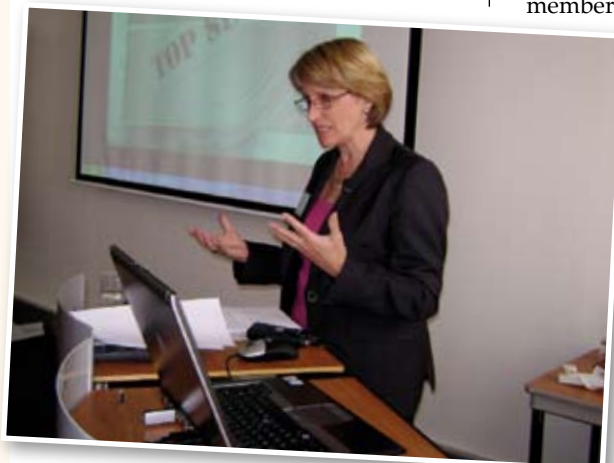
Nick Ellsmore, CEO, SIFT

The success of any mobile solution is going to require an increase in convenience and security

Rob Goldberg, partner, KPMG

The Russian bride is becoming a high motivation for people to send money - people are being hooked heavily

Graham Ingram, general manager, AusCERT



BCU marketing manager Gillian French explains the credit union's position on security

The future for fraud fighting

Second factor authentication could be on borrowed time, as real-time monitoring proves the more secure way forward

BY CHARIS PALMER

National Australia Bank is hoping to remove its dependence on two-factor authentication as it relies more heavily on real-time transaction monitoring to detect and prevent fraud.

"Where we're really seeing maximum benefit at the moment is by moving towards real-time monitoring" says Tim Cullen, head of direct channels with NAB. The bank credits its one-time password SMS solution with delivering what Cullen argues is the lowest online fraud level of the big four banks. But, he says, the bank has had to combine the technology solution with a "carrot and stick" approach to really make an impact. "We dropped our transaction limits from \$5,000 to \$2,500 unless customers took out SMS security... When you've got over a million customers and you change their transaction limits, that's certainly a stick."

Earlier this month the bank introduced an SMS security authorisation limit, meaning for external funds transfers under \$300 customers will no longer be required to enter an SMS code to authorise payment.

Cullen says "What we want to get to is real-time monitoring to try to remove the dependence on authentication and really take a risk-based approach... So if the customer only has a dollar to lose you don't apply the same level of protection as someone who has \$10,000 dollars to lose".

The move comes as security experts continue to predict attacks on two-factor authentication by more sophisticated fraudsters. "To all those people who go out and tell me two-factor authentication systems are

going to fix this problem, I tell them two-factor was defeated in 2004," says Graham Ingram, general manager of AusCERT.

However, he argues, "If you have two-factor authentication, sure it may be defeated, but it's unlikely the bad guys are going to deploy that against you while they can still get people who are just using username and password".

Cullen agrees fraudsters are becoming more sophisticated but says the bank is yet to experience any fraud of its SMS solution. "We're very conscious of the fact that through man-in-the-middle attacks there are risks, but we're also very conscious that with our SMS solution we advise the customer of the amount of the transaction and what account they are using, so we're confident it will serve us well into the future. For how long, we don't know."

Andreas Baumhof, chief technology officer of security software vendor TrustDefender says institutions are simply keeping pace with online fraudsters. "What they're not looking at is driving that one step further and providing real business benefits for customers."

Wayne Howarth, fraud policy and authorisation manager with Citibank, says the bank is moving to SMS security, but the challenge remains to offer secure online banking that is easy to use and customer-friendly. "Security is a concern for customers,

but so is just getting on with life and making sure they can do their transactions easily."

Cullen says "At the end of the day it's a trade-off between customer experience, risk and cost, and finding that balance is something we grapple with".

"We could put a range of draconian measures in place that would get us to zero losses. It would also probably get us close to zero online customers."

For now, Cullen says current measures are proving satisfactory with customers and "Our Internet banking satisfaction would be at 95 per cent". Cullen argues while the bank has made it slightly harder for customers to transact they're actually happier.

In future Cullen is predicting biometrics will play a role in securing online banking transactions. "I think we'll see more use of biometrics around risky transactions, so voice may play a role. Where someone wants to do a more risky transaction you'll ring them on the mobile phone and get them to do a voice validation. It's a very easy and non-imposing type scenario."



TrustDefender's Andreas Baumhof, Citibank's Wayne Howarth and NAB's Tim Cullen

Developed by:



Endorsed by:



Sponsored by:

