NATIONAL Australia Bank has moved to crack down on internet banking scams, flagging the introduction of a tough new security regime that will offer customers a one-time PIN via SMS on their mobile phones before using the bank's site. The security measures - known in the industry as two-factor authentication - are designed to put a stop to internet banking fraud, or 'phishing'. Phishing involves fraudsters sending out fake bank emails requesting customers register their password with fraudulent banking websites. The details are then harvested and either used to steal money from the accounts, or sold to other criminals.

Under the new security regime, which will be piloted in September and rolled out at the end of the year, National's one million internet banking customers will be offered the option of registering their mobile phone number with the bank, which will SMS a unique PIN to the phone during each transaction. Customers will then enter the PIN on the website to confirm the transaction.

The one-time PIN gives extra protection for customers whose user IDs and passwords are stolen.

National manager for internet banking Peter Bottomley said while fraud was "extremely limited" relative to the number of transactions processed by the bank, the new measures would provide extra security to customers. But they were not foolproof, he warned.

"It's really presenting some very clever people with a new challenge," he said. "The industry has seen that phishing incidents were posing a threat to our customers, so we've been looking at ways to provide customers with another level of security."

Mr Bottomley said the bank's research showed that most customers had mobile phones with them when they did their banking.

The bank has rejected two other security methods - tokens and smart cards - as being too difficult and cumbersome for customers to use. Tokens are small key-ring size devices that generate random PINs, while smart cards have a unique radio signal, but require specialised readers to be plugged into a computer before they can be used.

"We looked at all the options available, and it was about achieving a balance between security and convenience," he said. "SMS was the closest to the existing customer experience."

While SMS PINs are used by HSBC in Singapore, two-factor authentication is limited in Australia.
Both ANZ and Westpac provide extra security for business banking customers, and are looking at extending the technology to retail clients. ANZ uses smart cards, while Westpac uses tokens.

Internet banking fraud has received significant public attention over the past year, with the number of phishing scams multiplying rapidly. Banks and credit card companies have been working with the Australian Federal Police to help crack down on the scams.

This report appears on australianIT.com.au.