Human error puts online banking security at risk

November 7 2007

Using an SMS password as an added security measure for internet banking is no guarantee your money is safe, according to a new Queensland University of Technology study which reveals online customers are not protecting their accounts.

Mohammed AlZomai, from QUT's Information Security Institute, said one in five online transactions was vulnerable to obvious attacks despite added security methods such as SMS passwords being adopted.

Mr AlZomai said the study had found that the security threat had more to do with the usability of the SMS system and human error, rather than any technical security problem.

"In response to the growing threat to online banking security, most banks have implemented special methods for authenticating a transaction," he said.

"A typical method is sending a one-time-password via SMS to the customer's mobile phone for each transaction.

"This means the customer must manually copy the password from their phone in order to confirm the online transaction."

But Mr AlZomai said customers were failing to notice when the bank account number in the SMS message was not the same as the intended account number.

He said if this occurred it was a clear sign hackers had infiltrated the system.

As part of the study, QUT developed a simulated online bank and asked participants to play the role of customers and undertake a number of financial transactions using an SMS authorisation code.

Mr AlZomai said he then simulated two types of attacks - an obvious attack which was where five or more digits in the account number were altered, and a stealthy attack which was where only one digit was changed.

"It is worrisome that obvious attacks were successful in 21 per cent of cases," he said.

"And when transactions faced a stealthy attack, 61 per cent of attacks were successful."

He said this study showed that a significant number of users were unable to identify the attack.

"This is a strong indication that the SMS transaction authorisation method is vulnerable," he said.

"According to our study only 79 per cent of users would be able to avoid realistic attacks, which represents an inadequate level of security for online banking."

Mr AlZomai said while this study highlighted the importance for customers to be vigilant when they were banking online, banks also had a responsibility to their customers.

"We hope this research will allow online banks and other online service

providers to be better prepared for these emerging risks."

Source: Queensland University of Technology