AIB alerts customers as Internet Banking fraudsters target Ireland

8th May 2009

Online banking is growing in Ireland with AIB's Internet Banking service showing continued growth with over 570,000 customers (up 18%) now regularly banking online, driven mainly by convenience, ease of use and control. The number of transactions completed online also continues to grow strongly (up 27%) in 2008.

This migration of customers online has not gone unnoticed and 2009 has seen an increase in ‘cyber’ criminals beginning to target Irish banks. For example, the number of phishing attacks on AIB in April 2009, surpassed the total number experienced in 2008. Contrary to common belief, these ‘cyber’ criminals are not individual hobbyists, but well organised criminal networks, leveraging a broad range of skill sets to defraud customers across the globe.

AIB has invested significantly to protect its Internet Banking customers, with two factor authentication introduced in 2005. AIB’s Code Card is a two-factor authentication token which delivers a higher level of security by requiring “something you know” (your registration number and Personal Access Code) plus “something you have” (a unique code card) to complete a range of services.

There are two standard modes of attack used by the cyber criminal to attack Irish customers – Phishing and Trojan / Virus. In addition fraudsters are also keen to recruit customers as Mule Accounts. (See Notes to editors for more detail). AIB recommends that consumers be alert when banking online and encourages customers to protect themselves from such attacks by following these guidelines:

Phishing - AIB Internet Banking **NEVER** sends unsolicited emails to customers.

If you receive an email -

- *Do NOT click any links, do NOT open any attachments
- *Forward the e-mail to alert@aib.ie and then delete the e-mail
- *Do not provide Codes from your Codecard

Trojans - AIB Internet Banking **NEVER** requests a code from an AIB Code Card at Log in

- *If you are requested to provide this DO NOT
- *DO NOT use your PC until it has been cleaned with up to date anti-virus and anti- spyware software

Mules - Be suspicious of any local adverts which offer a job as a payments clerk and which require you to receive funds into your account for immediate onward transfer

- *DO NOT allow your account to be used by a 3rd party to transit funds

General

- *Use a PC you trust which has up to date anti-virus and anti-spyware software
- *Always verify the "last login" date and time when you login to AIB Internet Banking
- *Consult www.aib.ie/securitycentre for up to date information and alerts

AIB recently began the rollout of its new look Internet Banking service to customers. This significant redesign is based on feedback provided by customers and offers easier access to a range of banking services and online products. (See Notes to editors for more detail).

Sean Jevens, Head of eChannel Development, AIB, said:

"The internet has become a critical way for our customers to bank with us and we are continuing our investment to allow them manage their money at a time and place they choose. However, as with all banking channels we need customers to be alert to stay safe when banking online.

"Although more of our customers are now aware of phishing, in recent months the number of attacks reported and the volume of email addresses being targetted, in particular work email addresses, has increased significantly. Trojans are a recent and dangerous development in that they are more difficult for customers to spot. The process of recruiting mule accounts is also very sophisticated and customers need to be very careful that they do not allow themselves to become party to a fraud by allowing their personal accounts to be used to transfer fraudulent funds".

- ends -

For further information, please contact:

Ronan Sheridan
Group Press Officer
AIB Group
Bankcentre
Ballsbridge
Dublin 4
Tel: +353-1-641 4651

or

Sean Jevens
Head of eChannel Development
AIB Bank
Bankcentre
Ballsbridge
Dublin 4
Tel: 01 6411230

NOTES TO EDITORS - Some details on key online threats

Phishing:Traditionally the most common type of attack and works as follows:

- *Fraudsters design an email to look like it comes from a reputable bank
- *They also design and launch a site branded to look like the bank in question, which requests various sensitive details from the customer
- *They send copies of this email to as many email addresses as they can find
- *The email will ask the customer to “click on a link” or “button” in the email to complete an action, e.g. “Your Internet Banking Access Is about to expire”
- *Instead of directing them to a legitimate site, this link will direct them to a fraudulent site where customers are asked to complete a range of details, e.g. name, date of birth, login details, code card numbers etc.
- *Fraudsters use these harvested details to login and transfer money to their own mule accounts

Trojan / Malware

Traditionally a relatively rare attack, the Trojan has become increasingly common in 2009 and is a more difficult threat for customers to spot. A Trojan is in effect a piece of malicious software which has infected the customer’s PC without them knowing it. *Trojan / Malware* is more recent but growing threat and operates as follows:

- *Fraudsters build a specific piece of malicious code (Trojan) which they inject into existing web sites, e.g. social networks, popular download sites or distribute via email
- *The malicious code is designed to install itself on the customer’s PC in the background
- *It is typically designed to monitor Internet access to a specific site, e.g. URL of a specific Internet Banking site
- *When the Trojan detects access to this site it can:
- - Keystroke log customer details in an attempt to steal login security details / Card Numbers etc.
- - It can also intercept an existing customer session and inject some additional details, e.g. prompt for additional security information
- *The Trojan will sit in the background and collate the various pieces of information as detailed above.
- *Once the required information has been collated, the Trojan will send this information to a remote server for action and in some cases delete itself
- *The fraudsters use the harvested details to login and transfer money to their own mule accounts

Consult www.aib.ie/securitycentre *which explains all the common security threats and includes an interactive security demonstration*

Mule Accounts

The above attacks are critical in collecting the online banking security details of customers. However this is only one element, as cyber criminals also require local accounts into which they can transfer any funds they collect, commonly known as 'mule' accounts.

Fraudsters use a variety of options to identify "mule accounts" which they can use as to receive funds from compromised accounts. In some instances, criminals have advertised jobs for account / payments clerks in local papers to lure the public into assisting them by using their account as an exit point for funds which they then request you to transfer on.

New AIB Internet Banking service launches:

On 23rd April 2009, AIB launched a newly designed and improved version of its popular and award winning AIB Internet Banking service. This new design is available to customers on www.aib.ie and is being rolled out on a phased basis.

The new service has been completely redesigned based on customer feedback to improve usability and to make features more accessible. For example, new Mini Statement and Quick pay features allow customers to review their transactions and complete their payments in even fewer clicks.