

Customer Awareness Tips Against Computer Attacks

Cyber criminals have raided the accounts of thousands of internet bank customers around the country in one of the most sophisticated attacks of its kind.

The fraudsters used a malicious computer program called a “Trojan” that hides on home computers to steal confidential passwords and account details.

Trojans hide in websites, emails or downloads. Once installed on a computer, they can record every key stroke entered on the keyboard, steal confidential information or even open up a PC’s security file so that it can be controlled remotely from another country.

To protect your home computer, we provide the following tips:

- Make sure you have anti-virus software on your computer and that it is up to date.
- Most anti-virus software come with protection firewalls which should be set at the highest security level that is available.
- Never open an e-mail attachment from someone you don’t know.
- Never double-click on an e-mail attachment that ends in .exe. It is an “executable” file and can do what it likes in your system.
- Be alert to junk emails that pretend to be from banks, internal revenue or online shops like Amazon and Ebay. These emails invite the unwary to click on a link to a webpage containing a Trojan.
- If you think your machine has already been infected and you find suspicious withdrawals from your account, contact us immediately.
- Always keep your contact information (i.e. email address, phone number, home mailing address) current with us so that we will be able to contact you in the case we detect suspicious activity on your account.