## Use of Spyware – i.e. 'keyloggers' and 'trojans'

Criminals are also responsible for the use of spyware ('keyloggers' and 'trojans') – software that is secretly installed onto your computer and is capable of capturing your keystrokes or searching your computer for account details or credit card details.

The criminals embed spyware in a webpage, e-mail, spam mail or attachments, and when you open the infected item, the software is secretly installed onto your computer.

**Delete suspicious e-mails without opening them** and don't open suspicious attachments, even if they appear to have come from someone you know.

## Virus protection

Protect your computer by ensuring you have an effective virus protection program that you regularly keep updated.

## For further information

Visit www.citibank.com and click on the section marked **"about e-mail fraud."** Additional information can be found at www.antiphishing.org

## How to report a 'phishing' attack related to Citibank

Go to www.citibank.com, click on **"about e-mail fraud"** (bottom of homepage) and go to **"report a spoof."** Alternatively, you can visit your local Citibank website.

rev0704

**Citigroup Security and Investigative Services**

Fraud Management Program Office

# 'Phishing' plus Spyware

## i.e 'keyloggers' and 'trojans'

citigroup

## What is ‘phishing’?

The more you use the internet, the more you rely on its convenience for services such as banking, online shopping and others. Unfortunately, the internet is also **exploited by criminals** who send out e-mails that purport to come from one of those services. These e-mails look surprisingly genuine, and are commonly called **‘phishing’ e-mails.**

***Delete suspicious e-mails without opening them.***

## BEWARE:

Although secure website addresses begin with **https:** (“s” indicating they are secure) and have the padlock icon on the bottom right, these criminals have been able to “spoof” these features, and you cannot rely on them totally. When you double click the padlock icon, a dialogue box will appear indicating who owns the license, e.g., "Issued to www.citibank.com." However, criminals use fraudulent pop-ups with legitimate web sites (pop-ups are windows that suddenly appear and contain a menu of commands) to capture personal information, and sometimes the pop-ups appear to be log-in screens. Therefore, absolute reliance on the padlock icon can be risky.

## How to recognize a ‘phishing’ e-mail

You may receive an unexpected e-mail from your bank or one of the other services you use, but actually it will be someone posing as your bank or service. It usually asks you to send your account details and sometimes your PIN either by return mail, or through a website. **You could be encouraged to navigate to that website via an embedded hyperlink within the e-mail.**

The criminals cleverly attempt to trick you by using words such as “security and maintenance” or “investigation of irregularities.” They might say things like “your account has been frozen”, “we need to reconfirm your details”, “your credit card has been cancelled” or even “you have a large sum of money in your account, please verify the withdrawals.” This is intended to increase the likelihood of you clicking on the hyperlink to log in or complete a set of questions.

## What you need to know

If your PC is not adequately protected with up-to-date virus and firewall software, or is not regularly ‘patched’ with software fixes, be wary of clicking on a hyperlink embedded in an e-mail. If you need to go to your banking or online shopping service, ensure that you manually type their advertised web address into the web address line.

Your bank will never ask for information or your confidential PIN via an e-mail instruction, **so don’t panic.** Resist the temptation to reply or follow the e-mail instructions – even if you are being told that your account has been frozen or cancelled, or that you may incur a financial penalty.

If you are suspicious, contact the company cited in the e-mail using a telephone number you know to be genuine and verify the e-mail **– do not reply to the possible ‘phishing’ email.**

***Protect your computer with up-to-date virus software.***