Important information regarding falsified e-mails, phishing, and spyware

What is phishing?
People are increasingly using the Internet for convenient services, such as Online-Banking or online shopping. Unfortunately, criminal elements are also using the Internet to gain access to your personal information: they will send e-mails intended to misrepresent a well-known service provider as the sender. These e-mails are remarkably authentic in appearance and are called phishing e-mails.

How can you recognize a phishing e-mail?
You receive an unexpected e-mail – ostensibly from your bank or another service provider. But in reality someone else is misrepresenting themselves as your bank or your service provider. These e-mails generally ask you to enter information about your bank account and sometimes also your PIN (access code) - either by e-mail or via a website that is reached using a link (hyperlink) that is embedded into the e-mail.
Criminals attempt to deceive you by using terms such as "security and data maintenance" or "investigation of irregularities". Frequently, you will also find notices such as "your account has been blocked", "your account information must be reconfirmed", or even "you are carrying a large balance in your account, please verify the transactions". The intent is to increase the likelihood that you will click on the hyperlink, to log in, or to answer a series of questions.

Spyware
Criminals also use so-called spyware. This software can be surreptitiously installed on your computer, and has the ability to search for sensitive data, such as account information or passwords, or to record your keyboard entries while running in the background. The data are then also unnoticeably forwarded to an unknown e-mail address or an unknown server. Criminals install spyware on Internet pages, e-mails, or e-mail attachments. As soon as an infected object is opened, the spyware is installed on your computer without you being aware of this.
So-called viruses, worms and Trojan horses modify operating system processes and are therefore able to a record keyboard entries and screen displays, and to forward these to unauthorised others. If you start such programmes intentionally or unintentionally (for instance due to a lack of awareness about their origin), these activities can take place completely undetected.
We therefore advise that you delete suspicious e-mails without opening these. Please do not open suspicious attachments, even if these appear to be coming from an e-mail address known to you. Deactivate the auto preview function to prevent e-mails from being automatically opened.

What you should know...
Piraeus Bank will never ask for your account information or your PIN (access code) by e-mail. Please do not respond to such e-mails, and also do not follow the instructions contained in these – even if you are told that your account will be blocked or deleted, or you are threatened with a fine.

If suspicions arise please inform us at our branch office in Frankfurt am Main, or call our free hotline service at + 49 69 240011 414.