Useful information for Secure Internet Card Use and Card Transactions ("Useful information for Internet Card Transactions")

The "Useful Information for Internet Card Transactions" leaflet is published periodically in order to provide cardholders with information for the secure use of cards and card transactions performed on the Internet.

Internet Card Transactions refer to any transactions performed on the Internet during which goods or services are purchased. This might be done either through the use of a card, a card number or through any other means chosen by the cardholder which authorises the debiting of the card account.

A. Equipment/Software and Personal computer protection (from Malware, Virus, Spyware)/ Firewall

1. Any Internet transaction requires the use of a computer or a smart phone with Internet connection.
2. In case of a remote Internet connection, you are advised to install the wireless equipment correctly. It is recommended that you read the installation instructions carefully and to follow the recommended safety instruction of the manufacturing company.
3. Install on your computer anti-virus software as well as software which protect against spyware and malware viruses. Use this software on a frequent basis in order to detect and to protect your computer against Spyware, Malware and Spam.
4. Ensure that your computers anti-virus and anti-spyware software is up-to-date.
5. Ensure that the operational systems and programmes on your computer are updated with the latest security additions.
6. Use Firewall (or personal firewall) in order to discourage external users from accessing your computer.

B. Security for using Access Codes / PINs on the Safe@Web Service

1. Do not reveal your Access Code / PIN to anyone else.
2. Do not keep your Access Code / PIN in a place which can be accessed by others.
3. The member of the staff of bank of Cyprus will never ask of you to reveal your Access Code/PIN, neither via phone nor via Electronic mail.
4. Do not allow anyone else to watch you while you are entering your Access Code / PIN at a website.
5. Always log-out of a website. Do not simply turn off your browser or your mobile application.
6. Activate the time-out option in order to lock off your computer whilst you are not using on it.
7. For additional security, we recommend that you change your Access Code/PIN on a regular basis.

C. Internet and Electronic Mail Security

1. Do not under any circumstances reveal your security credentials to websites where you have provided your card number.
2. Do not stray away from your computer prior to disconnecting from websites where you have provided data in order to perform card transactions.
3. Avoid using public computers for performing Internet transactions.

4. In case you discontinue using a computer, we recommend that you permanently delete all personal files which are kept on the computer using the appropriate software.
5. The Bank periodically sends its customers promotional electronic messages (via email, SMS, etc). However, customers will never be requested to disclose personal security credentials or access codes through email, pop-up windows or banners.
6. Never reveal personal data such as card numbers, User IDs, Access Codes, digipass codes, bank account numbers, etc., on the Internet, Electronic Mail, or during any electronic transaction.
7. In case you receive a message asking you to "confirm your card number", "confirm your Access Codes", or any message of similar content, please note that this is possibly a fraudulent message or "Phishing" e-mail.
8. In case you receive electronic messages such as spam or messages containing suspicious attachments, it is advisable to erase these at once without responding.
9. Do not reply to and do not download files on your desktop, which have been sent by unknown sources or websites.
10. In case of doubt of the authenticity of a website, remember to check its certificate. Moreover, by clicking on the security lock icon (and again on the website bar) you will see the name of the certificate owner.
11. Do not open files which you did not expect to receive and/or which have been sent from known or unknown sources.

D. Procedure to be followed in the event of loss or theft of personalised security credentials / submission of personalised security credentials to non-secure websites

1. In case you suspect that your login security credentials to a website where you perform card transactions have been stolen or disclosed to others, change them immediately as per instructions provided on the specific website. Moreover, contact the Bank as soon as possible in order to cancel your card and reissue a new one.
2. In case you have received a "Phishing" message with a link to a non-secure email, do not reply to this.
3. If you have replied to a "Phishing" message, and have entered your personal information and other details to a website where you have also provided your card information, contact the Bank immediately in order to cancel your card and reissue a new one.

E. Additional Information

In addition to the above information, the provisions concerning Card and PIN protection, the procedures to be followed in case of suspected non-authorised card use, as well as any other information on Card Use and the responsibilities and obligations which dictate the relationship of the bank, the card account holder and the cardholder, can be found at http://www.bankofcyprus.com.cy/en-GB/Cards/