HOW TO TAKE CARE OF SECURITY?

I. SECURE DEVICES

a) Use transaction websites only on verified devices. Avoid logging in to applications or websites from computers and mobile devices of other persons
b) Use additional software (e.g. antivirus, firewall) that protects your computers and mobile devices
c) Update the computer operating system regularly
d) Do not change the security settings of the device and, in particular, do not remove restrictions set by the producer
e) Applications and programs must be downloaded only from official sources
f) Block the device screen by means of additional security measures (e.g. password, PIN).

1. Mobile devices

Smartphones and tablets are more and more frequently replacing other personal devices. Similarly to computers, mobile devices require protection against viruses.

When thinking about safety of their phone or tablet, many users are afraid of losing them or that somebody could steal them. Meanwhile, what we should be afraid the most is that somebody could take control over them.

When using mobile applications, remember:

a) Use of antivirus software is obligatory
b) The screen must be blocked with a password and PIN
c) Install updates of applications and the operating system
d) Download and install applications only from official app stores
e) Do not use links from text messages or e-mails if you have any doubts that they could originate from an unsecure and untrusted source
f) Do not connect mobile applications with your accounts on other devices
g) Do not read QR codes of unknown origin
h) Be cautious when installing applications requiring authorisation to read and send text messages
i) Switch off Wi-Fi and Bluetooth when not used.

Note! No instructions ever ask you to install additional applications or certificates.

2. Computer

A secure computer must have:

a) updated and legal operating system
b) firewall type software
   Firewall is one of the methods to secure computers, networks and servers against intruders. Firewall has become an indispensable software for all computers connected to the web. A firewall on your home computers checks the entire web traffic and restricts access of unknown software or users.
c) antivirus software as well as anti-spyware and anti-adware software
   This software detects, secures, eliminates, removes and repairs damage caused by viruses. If an application contains malicious software, the antivirus will take proper measures to exclude the virus and ensure secure access to the started software. It is important that the antivirus software is frequently updated. This allows it to be "up-to-date" with the world of viruses. Updates allow the software to collect information about the latest viruses and add instructions helping to eliminate viruses and repair the damage they cause. Antivirus developers that are well recognised on the market update their virus definitions daily.
d) antispam software
   This is a type of software that blocks unsolicited e-mail correspondence. The software filters messages and uses the so-called "black lists" of addresses and domains used by spammers. In most cases, such a software allows to change the settings of rules (e.g. determine the key words found in advertising materials). This allows to block messages containing such words in the message title from entering our inbox. However, this

software is not perfect and may sometimes block correspondence we want to be delivered, therefore checking the spam folder and verifying if all messages stored there should have actually been transferred there is important.

II. SECURE PASSWORDS

a) Use complex passwords and make sure it is difficult to guess them (at least eight characters, including special characters, numbers, capital and lowercase letters)
b) In your passwords, do not use typical expressions and information that can be easily linked to you (e.g. name or surname) or that are easy to guess (e.g. current month, year)
c) Change your passwords regularly and do not share them with anybody
d) Use unique passwords for websites. Do not use the same passwords you use in other systems, on Internet forums or websites.

III. SECURE E-BOK LOGGING

a) Never share your identifier (login) or access password with other persons. The logging password for the website is set separately
b) When entering the identifier (login) and password, make sure nobody is watching
c) Do not log in applications on computers available in public areas
d) Use safe passwords and try to avoid passwords that are easy to guess
e) Do not write your passwords down and remember to change them regularly
f) Before leaving your computer, log out and close the browser
g) Check the date of last successful and unsuccessful logging
h) If additional fields to be completed, e.g. personal data or one-off password, appear on the logging page or if you notice any irregularities, do not provide your data and report the issue to the Customer Service Office.

IV. SECURE APPLICATION INSTALLATION

If you decide to download any software to your device, remember:

a) applications should be downloaded from authorised stores. These are: App Store (iOS – Apple), Google Play (Android), Windows Phone Store (Windows Phone) and Windows Store (Windows 8.1) – use only these stores as the software offered there is digitally signed and verified in terms of security
b) never download applications from untrusted sources and avoid downloading applications from third parties (e.g. sent via Bluetooth or in a text message)
c) be cautious when installing applications requiring authorisation to read and send text messages.

V. SECURE E-MAILS

a) Do not open suspicious e-mails and attachments
b) Be extra cautious about attachments having several file extensions at the same time, e.g. przelew.pdf.zip, wyplata.jar.doc
c) Check if the actual link address is compliant with what you see in the e-mail content
d) Be cautious about the sender's reliability and the way he/she is titling you
e) Never log in a transaction website from a link you received by e-mail
f) Do not realise transactions based on an e-mail. Check such payment orders carefully.

VI. SECURE WEBSITES

a) Check correctness of the website you are connecting to (certificate and HTTPS connection)
b) Do not enter suspicious and unknown websites - pay attention to the URL addresses of the websites you visit, especially in case of the so-called shortened URLs. Such websites can infect your device with malicious software.

c) Do not provide your personal data on untrusted websites, especially your login and password you are asked for on unknown websites
d) When logging in on websites, type the address of the logging page yourself or use the "Log in" button after you type the website address. Never:
   - use logging links you receive by e-mail or on social media
   - search for the logging website in the Internet browser - this could lead you to fraudulent websites that pretend to the website you want to log in.

VII. SECURE PROFILES AND OFFERS

a) If you received a request from your friend to make a transfer for him/her, be careful - it is possible you are messaging with a fraudster. Contact your friend using a different method to confirm that it is actually him/her who is requesting the given transfer.
b) Before you buy anything, check who you are buying the goods from: how long the given company has existed, whether it is possible to call it or what opinions other buyers published about it.
c) Do not trust job offers sent directly to your mail box, especially those particularly attractive. When you are looking for work, use only websites you know.

VIII. SECURE TELEPHONE CONVERSATIONS

a) Do not share your private data until you are sure who you are talking to. Employees of all institutions can be verified - call the Customer Service Centre and ask for confirmation of their identity.
b) Do not trust unknown persons contacting you who want you to provide your data (passwords, PINs).