Information on security of online payments

Bank Handlowy w Warszawie S.A. (Bank) hereby informs you:

1. The use of Citibank Online and Citi Mobile by the Client shall require the use of appropriate hardware and software enabling the Client to access Citibank Online and Citi Mobile, including:
   a) Having access to a computer or another device with an operating system supporting popular web browsers, like Internet Explorer, Google Chrome, Mozilla Firefox,
   b) Enabling cookies and javascript. (device configuration instruction on www.citihandlowy.pl),
   c) Enabling protocol TSL 1.0 and 1.1,
   d) Installed Adobe Acrobat Reader version 9.0 or higher for PDF files;
   e) Connection with the Internet with the data flow speed Transfer to/from an external network (for a single station) of min. 128 kbs, we recommend 512 kbs
   f) Open ports http (80) and https (443)
2. In the event that a Payment Instruction or another activity of the Client in Citibank Online requires confirmation by an Authorization Code, the Client should verify the data sent in the text message (SMS) containing the Authorization Code by comparing it with the data entered in Citibank Online.
3. When logging in to Citibank Online, the Client should use a hardware secured with a firewall, which helps protect the computer against network attacks.
4. When logging in to Citibank Online and Citi Mobile, the Client should use a hardware with installed the current version of:
   a) anti-virus software,
   b) operating system and
   c) web browser.
5. In case of any doubts if information about the correct and secure use of online payments is authentic or reliable, the Client should confirm its authenticity and reliability on the basis of information available on the website of the Bank (https://www.online.citibank.pl/polish/services/Bezpieczenstwo.htm) or contact CitiPhone.
6. The Client should not open or respond to emails which ask them to provide their personal data or Identification Codes. Such instances should be reported to the Bank.
7. The Client should not open any suspicious links or attachments of unknown origin in received email, SMS and MMS messages.
8. Neither the Bank nor its employees will ask the Client to provide:
   a) login password for Citibank Online,
   b) Identification Codes,
   c) CVC2 number placed on the Debit Card's reverse,
   d) Authorization Codes.
9. When logging in to Citibank Online or Citi Mobile, the Bank never asks the Client for the telephone type or telephone number and never instructs the Client to install any software on the Client's telephone.
10. The Bank provides on the website (https://www.online.citibank.pl/polish/services/Bezpieczenstwo.htm) the information regarding correct and secure use of electronic banking and online payment services.
11. The Bank provides current information on the rules of correct and secure use of electronic banking and online payment services and warnings against significant threats connected with the use of online or mobile banking in a message published in Citibank Online, which is available after logging in and on the website indicated in Clause 10. The Bank may also inform the Client about vital information published in Citibank Online, by sending an email to the Primary Email Address of the Client.

Moreover, the Bank hereby informs you:

1. The Client should not reveal their confidential information, including card numbers, user names (so-called logins) and access codes (passwords) nor should they write them down. If there is a need to save such information, the Client should do it in an encrypted form that prevents other people from reading it.
2. The Client should not store their PIN, e-PIN and CitiPhone PIN and card numbers in one place.
3. The Client should make sure to make their passwords and access codes difficult to guess (e.g. refrain from using birth dates, first and last names or easily accessible information of the user) and to change them on a regular basis.
4. If the Client suspects or discovers that their login data have been lost or intercepted, the Client should contact the Bank immediately via CitiPhone (+48) 22 692 20 90 to block their account.
5. The Client should not save passwords and store access codes in files saved on their computer.
6. The Client should protect their PIN and card details and should not reveal credit card details, such as expiry date and the last 3 digits of the number given on the reverse side of the card to third parties.
7. Before using their PIN, e-PIN or CitiPhone PIN, the Client should make sure they will not be provided to third parties.
8. If the Client loses the device on which the Client uses online banking and executes transactions (i.e. computer, laptop, tablet, phone etc.), the Client should immediately contact the Bank via CitiPhone at (+48) 22 692 20 90.

Bank Handlowy w Warszawie S.A. with its registered office in Warsaw, ul. Senatorska 16, 00-923 Warsaw, entered in the Register of Entrepreneurs of the National Court Register maintained by the District Court for the Capital City of Warsaw in Warsaw, 12th Commercial Division of the National Court Register, KRS 000 0001538; NIP 526-030-02-91; with share capital amounting to PLN 522,638,400, fully paid-up. Citi and Citi Handlowy trademarks are registered trademarks of Citigroup Inc. used under a license. Citigroup Inc. and its subsidiaries are also entitled to the use of certain other trademarks used herein.

04/2016