

Best practices in the area of safe use of CitiDirect electronic banking system

Please, be advised of the following!

Security of transaction systems in electronic banking and your funds is of great importance to Citi Handlowy. Therefore, we would like to highlight a few simple rules that will allow you to maintain the highest security level while using electronic banking services.

Please be warned against social engineering attacks

Not only in Poland, but also in the entire world we increasingly often witness incidents of criminals' deceitful attempts to obtain sensitive data, which are the secret of the electronic banking system's users.

Criminals usually contact a given company or person on the phone and pretend to be bank's employee (e.g. from the Customer Service or HelpDesk departments). They ask questions about various details connected to functioning of the electronic banking system, for instance:

- the number of authorization levels
- the transaction authorization scheme
- login data (SafeWord card number)

NOTICE – Citi Handlowy will never ask you for your system passwords, SafeWord card PIN or any other information generated by SafeWord cards.

If the course of the conversation raises your concerns, it is always advised to ask your interlocutor to give you their personal data (first and last name) and confirm them by contacting:

- » CitiService (801 24 84 24; 22 690 19 81)
- » Helpdesk (801 34 39 78; 22 690 15 21)

Another social engineering method widely used by hackers is sending an e-mail message which is supposed to arouse the recipient's interest and encourage them to open the attachment or click the link, which in reality causes the computer to install a malicious software (details below).

CitiDirect - the best practices to maintain system security

In order to ensure the highest security standards, please ensure that you regularly review your internal processes .

- Citi Handlowy advises you to use multi-level authorization (as long as it can be reasonably justified for the accounting process) in order to avoid situations where one person is allowed input and release payments acting independently; CitiDirect supports up to 9 levels of authorization
- make sure that higher risk transactions such as high-value transactions are processed with the use of multi-level authorization
- consider using templates, that is, predefined payment forms
- create accounting processes in such a way that it will be impossible to modify the beneficiary's account prior to inputting or uploading transaction into the system (e.g. in a file imported to CitiDirect)
- submit a request to Citi Handlowy to make your account inaccessible to the employees who have left the company or are on a long leave (e.g. childcare leave). To do so, use the [Activation/ Configuration](#) form (table 3)
- review the authorizations in the electronic banking system on a regular basis in order to ensure that the right persons have access to it and they have been assigned up-to-date entitlements, required to perform these tasks according to the so-called minimum entitlements principle

- do not make your SafeWord card available to anyone and do not reveal any information connected to the card (such as card number or PIN)

NOTICE - even the best designed internal processes can prove insufficient when e.g. a single person has full control over transactions effected in the system.

- protect the PIN to your SafeWord card and do not disclose it to third parties. Your PIN is the first and most important protection mechanism. It protects your SafeWord card from unauthorized usage in case of theft or loss. You should not write down your PIN anywhere, nor should you keep it in a visible place. Remember to make it hard to guess.

We recommend changing your PIN code every now and then. In order to do that, follow the below steps:

- 1) turn on your SafeWord card with the ON button
- 2) enter your current 4-digit PIN
- 3) press the „Pin” button on the SafeWord card keyboard
- 4) when you see the NEW PIN message, enter a new 4-digit PIN
- 5) when you see the AGAIN message, enter your 4-digit PIN once more, the same one as in the previous step
- 6) the card will inform you about a successful change of PIN by displaying a SUCCESS message on the screen

NOTICE - memorize your new PIN - if you forget it, your only solution will be to get a new SafeWord card.

PC (computers) protection - best practices

Numerous companies have their own IT safety policies. Contact your IT department if any of the following issues raised your concern.

1. Operating system and web browser

A web browser is a program that lets you open web pages, also those connected with logging into the online banking system. Hackers seek out loopholes in programs and use them to steal information. Because of that, you should remember to always have the latest version of the browser installed on your computer. The same rule applies to the operating system - it should be updated regularly.

Software providers are constantly monitoring the level of security and publish patches that fix software loopholes. Because of that, it is important to use versions that are currently supported by the provider.

A modern web browser is an essential element that ensures safe usage of the online banking system. A good web browser should also be able to warn the user about suspicious web pages.

2. Antivirus software

Installing an antivirus software on your computer is equally important. Such an application should prevent viruses from installing themselves and protect your device from other harmful software. It is worth using software that is recommended by experts, as not every application available on the Internet meets the relevant standards. You should keep in mind that installing applications downloaded from unverified web pages can very often infect your computer with spyware. It is also worth scanning your computer with an antivirus software every couple of days and keeping your virus database up to date.

NOTICE - using up to date versions of your operating system, web browser and antivirus software can help you protect your device from malicious software (malware).

Currently we have observed an increase in activity of malware called Tinba, which represents a potential threat to the entire banking sector. The attack most often occurs through:

- installation of malware with other illegal software
- receiving an e-mail message with a request to click a link, as a result of which malware is installed
- receiving an e-mail message with an attachment containing malware

The Tinba virus works by adding a script to the Customer's web browser, using the Customer's computer vulnerability to the attack. When logging into the online banking it performs additional actions. An attack may look as follows:

- The Customer enters their password and login to the online banking system, and the data is forwarded to the hackers' server
- for a minute or longer, the Customer's computer displays a message similar to: "transmitting data", "please wait", "updating data in progress", etc. or no other message is displayed, and the user may think that the banking system is just operating at slower pace
- during this time, based on the stolen login and password the hackers log into the Customer's online account, check the available balance, prepare a fraudulent transaction and attempt to carry it out
- the hackers may display additional messages to the user who tries to log in, e.g.: "preventive work in progress" or "service temporarily unavailable", and after the transfer "authorization" (when it is additionally required), funds are taken out of the account
- to delay the moment when the fraud is noticed, after the transfer is performed, a trojan horse installed on the infected computer displays a message about alleged maintenance or upgrade work and a forced interruption in the operation of online banking

The aforementioned scheme of operation is used by the perpetrators also in order to add predefined recipients (templates).

Should you notice that the online banking system behaves strangely:

- do not enter any additional information in order to "authenticate" your identity, buy insurance, etc.
- contact the bank immediately to check whether an unauthorized transfer was executed, by calling:
 - » CitiService (801 24 84 24; 22 690 19 81)
 - » Helpdesk (801 34 39 78; 22 690 15 21)

To document the event please make a screenshot (by pressing the PrtScn key on the keyboard, and pasting the image into a new document, for example in „Paint”) and provide it to the bank employee for analysis.

3. Block pop-up windows

Block pop-up windows in your browser's settings, because they are not only a nuisance, but can also be used to spread malware.

4. Log out of the system when you are done working with the online banking

When you finish working with the system, log out of it, using the Log out button. This way you will be able to correctly close the active session.