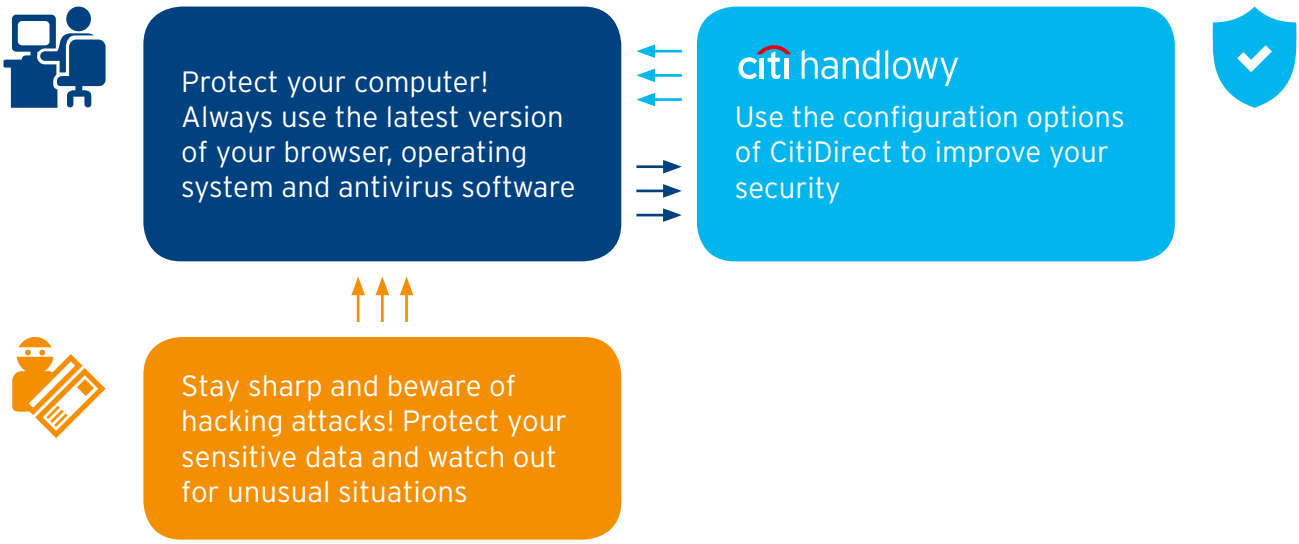
CitiDirect - Best Practices of Safe System Use

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



Protect your computer!

- use the latest version of your operating system and recommended web browsers
- use an up-to-date antivirus program and firewall
- secure your devices, software and credentials used for signing in and authorizing transactions
- protect your personal data – be careful when enjoying the benefits of the Internet
- do not install any software from untrusted sources
- do not respond to e-mails which ask you to provide your personal data or access codes – and please notify us of any such cases
- do not open any attachments and do not click on any links in suspicious e-mail and text messages
- always sign in to an electronic banking system from a trusted computer and network (avoid hot-spots) by keying in a specific URL address – do not search for it with a search engine
- check if the connection is secure (https, SSL, TLS) when you are signing in
- make sure that you are on the real website of your bank – to this end verify the certificate and the data it contains
- do not copy bank account numbers to transfers ("copy-paste"), but enter them manually and check them very carefully
- check systematically if account numbers in payment templates have not been swapped
- always remember to sign out from the service when you're done (click on the "Logout" option)
- notify the Bank of any unusual situations and irregularities faced when using electronic banking services

NOTICE – Please read the security guidelines issued by the Polish Bank Association (ZBP). They are presented HERE.

CitiDirect – use the options to improve your security

- use multi-level authorization – do not allow a situation where a single person can make a payment
- make sure that higher risk transactions, such as high-value transactions, can only be processed with the use of multi-level authorization

NOTICE – even the best designed internal processes can prove insufficient, for example when a single person has full control over transactions in the system.

- consider using templates (predefined payment forms)
- create accounting processes so that it is impossible to modify the beneficiary's account prior to entering a transaction into the system (e.g. in a file imported to CitiDirect)
- request Citi Handlowy to make your account inaccessible to those employees who have departed from your company or are on a long leave (e.g. childcare leave). To do so, use the Activation / Configuration request form (Table 3)
- review the entitlements in the electronic banking system on a regular basis in order to ensure that only the right persons have access to it and that their entitlements required to perform their tasks are up to date, in compliance with the least privilege rule.
- make sure your SafeWord card is not available to anyone but you and do not disclose any card-related details (e.g. card number or PIN)
- protect your SafeWord PIN and do not disclose it to any third parties. PIN is the first and foremost defense against unauthorized use of your SafeWord card in case it is lost or stolen. Do not write down your PIN anywhere and do not keep it so that it can be visible to anyone. And remember to make it hard to guess.

We recommend changing your PIN code regularly, following these 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, re-enter your 4-digit PIN, the one you have just defined in the previous step
6) the card will confirm that your PIN has been successfully changed by showing a SUCCESS message on the screen

NOTICE – memorize your new PIN – if you forget it, the only solution is to get a new SafeWord card.

Beware of hackers!

Recently, we witness the increase of criminal activities on the web, both in Poland and worldwide. We are experiencing an upturn of the trend with the number of incidents where criminals make deceitful attempts to gain sensitive data, i.e. secrets of the system's users, on the rise.

Criminals use advanced social engineering techniques to contact a selected company or person by telephone and impersonate a bank employee (e.g. from Customer Service or HelpDesk). They're asking questions about various details related to the operation of the electronic banking system, like:

- number of authorization levels
- order of authorization sequence
- sign-in data (SafeWord card number)

If a conversation raises your concerns, it is always wise to ask the person you are talking to about some personal details (first and last name) and to confirm them by calling:

» CitiService - 801 24 84 24 or (22) 690 19 81

» Helpdesk - 801 34 39 78 or (22) 690 15 21

NOTICE – Citi Handlowy will never contact the clients to ask about their system passwords, SafeWord card PINs or any other information generated by SafeWord cards.

One of the most widespread methods used by hackers to get confidential data is sending fake e-mails (phishing). Their wording is meant to arouse the recipient's interest to encourage them to open the attached file or click on the provided link. As a result, malicious software is installed on the computer and can be used by the criminal.

Be careful when reading incoming e-mails. If you have any doubts, delete the suspicious message.

NOTICE – please contact the Bank if, when signing in, you can see any alarming signs, which raise your doubts (e.g. a different look of the sign-in page or any non-standard messages).