citi handlowy

read CitiService News

February 2024 | edition No. 2

Beware of phishing

MORE >>

Important – submit your company declaration (FINREP)

MORE >>

CitiDirect MobileToken: Discover the new fast login method

MORE >>

Cross border transfers: SHA as the default charging option

MORE >>

Bank holidays: February and March 2024

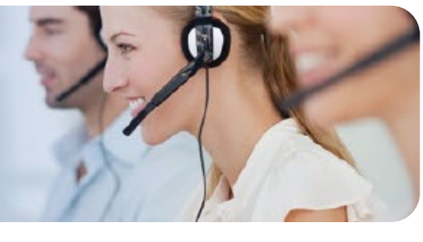
MORE >>

Service Shortcuts:

- Extract from the Table of Fees and Commissions — Check >>
- Foreign Exchange Rates — Check >>
- Market Analyses — Check >>
- Client Zone — Check >>
- Newsletter archive — Check >>
- Electronic Banking: Online trainings — Sprawdź >>
- Electronic Banking: Video Instructions — Check >>
- Electronic Banking: Manuals and documents — Check >>

Contact with CitiService:

tel.: 801 24 84 24; 22 690 19 81



Enterprises face many complex and ever-changing threats related to e-mail communications – from account takeover and business e-mail compromise to spear phishing and vishing. Cyber criminals often use malicious links for phishing attacks or malware infections.

When an employee clicks on such links or opens an attachment, the company can be exposed to a variety of threats, from identity theft to leaking confidential information and loss of funds. Attackers may use e-mails containing links and attachments that appear authentic and legitimate, but are intended to phish. To protect yourself against a cyber-attack, it is worth taking a closer look at the message before opening the attachment or clicking on the link.

Here are a few easy steps to verify if the e-mail you have received was sent by our bank:

1. Recipients' mails verify e-mails based on the address of sender. Please note that in the case of CitiDirect system e-mails it is always citidirectbe.notifications@citi.com, and in the case of CitiManager it is citicommercialcards.admin@citi.com. The e-mails from Citi Handlowy will always come from domain @citi.com.
2. Citi Handlowy uses SPF, DKIM, and DMARC e-mail authentication mechanisms to enhance e-mail security and prevent spoofing and phishing attacks. If your company's mail server is set to recognize such certificates, the malicious e-mail would either be blocked from delivery or sent to the spam folder.
3. Please familiarize yourself with the logo and communication style of our bank, including by visiting our home page, to help you distinguish them. Our statements are encrypted, and notifications such as balances will always have masked details.
4. The website of the Citi Handlowy bank has a secure URL address: HTTPS (at the beginning of the URL address). HTTPS uses secure certificates to verify the server's permissions and encrypt transmitted data. HTTP links are less secure and more likely to lead to unsafe sites.

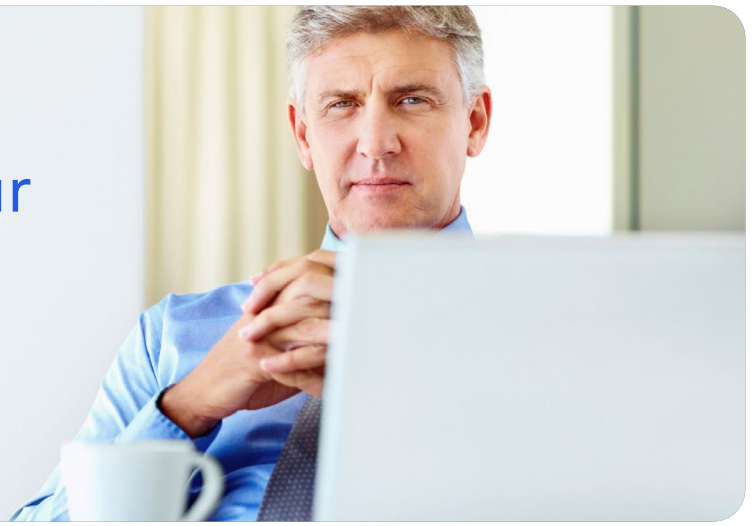
A thorough verification of the sender's e-mail will allow you to distinguish our communication from cybercriminals' attempts to impersonate our bank in order to steal valuable information and company funds.

To learn more about some common scams, as well as cybersecurity best practices, visit https://www.citibank.pl/poland/citidirect/english/security/electronic-banking-security.htm or sign up for a free „Online Safety" training.

BACK >>

citi handlowy

Important – submit your company declaration (FINREP)



We would like to inform you that Bank Handlowy w Warszawie SA has started the process of updating the data related to employment in companies of our clients in connection with the requirements of the Act of August 29, 1997 on the National Bank of Poland and Resolution No. 71/2016 of December 22, 2016. The purpose is to properly determine the entity category, a client of the Bank (based on the number of employees), in accordance with the FINREP financial reporting instructions.

A bank is obliged to submit to supervisory institutions, every year, information on the number of clients served in particular categories. Therefore, please confirm whether your company belongs to the category "large enterprise" or "small and medium-sized enterprise (SME)". This classification is based on the number of employees, with the limit of 250 employees (contracts of mandate, contracts for specific work, and seasonal workers are not included).

Therefore, please **complete** your FINREP Classification Declaration and submit it by **February 20, 2024** in one of the following ways:

1. via *eWnioski* (eRequests) – see Instruction here >>
2. by sending your Declaration with a qualified signature by e-mail directly to a Relationship Manager or to the address citiservice.polska@citi.com.
3. The declaration should be signed in accordance with the representation provided in the extract the extract from the register, the appropriate power of attorney or representation on the KWP.
4. You may also deliver (send) the handwritten original of your Declaration to the following address:

   City Handlowy
   Bank Handlowy w Warszawie S.A.
   Strefa Dokumentacji Klienta
   ul. Goleszowska 6
   01-249 Warszawa

   with the note: FINREP declaration
5. Link to FINREP classification Declaration

BACK >>

Designate the Administrator of your Business Cards >>

in order to manage your Business Card program for employees without unnecessary formalities and without the need to contact the bank.

citi handlowy

CitiDirect MobileToken: Discover the new fast login method

CitiDirect Mobile Token at Citibank is now available in 101 countries and is intended to eventually replace MobilePASS, which is gradually being de-activated for users who use several log in methods.

Why is it worth changing the login method and moving to a new, upgraded mobile token? **CitiDirect Mobile Token** is a relatively new login credential avalible from 2022 on the CitiDirect mobile app that enables users to login both to CitiDirect® desktop and mobile. Setup is simple, activation takes just minutes, and login is easier than before!

CitiDirect Mobile Token enables users to easily and quickly – in just a few minutes – confirm their identity and gain secure access to CitiDirect from their computer or mobile application. Combined with CitiDirect biometric authentication (fingerprints or face recognition), it offers a convenient way to login to CitiDirect.

Security Managers can enable **Mobile Token** now for the users in their company/organization by following these easy steps: CitiDirect® Mobile Token Enablement Guide for Security Managers. Then the users can easily activate their Mobile Token: Mobile Token activation video and log into CitiDirect: Login video

Why should you try CitiDirect **Mobile Token**?

EASY-TO-USE

- Modern and mobile friendly design
- Clear and contextual instructions
- Real-time progress indicators and visual feedback

SECURE

- Device binding
- Strong verification protocols
- Time-based controls and built-in security parameters

CONVENIENT

- Activation takes less than 2 minutes
- Login via a quick QR code scan - add biometrics as an option
- Reactivation at your fingertips

Install **CitiDirect BE Mobile** application, where you can check your balance and authorize payments **at any time, even when you don't have access to a desktop.** The application has simple and transparent interface and strong security mechanisms, such as ability to confirm login to the system using biometrics. **CitiDirect BE Mobile** will help you to:

- authorize and release payments
- check the account balance
- display a preview of transaction history and details of the payments made
- search for payments
- link between company profiles
- authorize the changes requested by Security Managers
- use biometric authentication (fingerprints or face recognition)

The application is available for Apple iOS and Android.

More information can be found in the following materials:

CitiDirect Mobile Token FAQ >>

CitiDirect BE Mobile >>

BACK >>

citi handlowy

Cross border transfers: SHA as the default charging option

Please be reminded that SHA is the default charging option for foreign payments to banks located in the European Economic Area, regardless of the currency of the transaction. This is due to the guidelines of the Payment Services Act implementing the PSD2 directive. The bank cannot interfere with your selected payment option. If you choose OUR option, your payment will be processed accordingly. However, this may lead to the beneficiary's bank rejecting the transaction, as they may not accept this cost option.
At the same time, if no charging option has been selected, the system will set the default option – SHA (Shared), as prescribed by the rules mentioned above.

IMPORTANT NOTE: when ordering payments in the EEA, please pay special attention to the selection of the SHA charging option. Selecting any other charging option may result in rejection of the payment.

NOTE: the National Bank of Romania, as part of its migration process to ISO 20022 standards, has decided not to allow the BEN/OUR option. As of February 2, 2024, payments in Romanian leu (RON) in which the ordering party indicates the BEN or OUR option, will be rejected. Romanian banks will only accept payments ordered with the SHA charging option.

BACK >>

citi handlowy

Bank holidays:
February and March 2024

Please note the following days in **February and March 2024** when orders received will be affected on the following business day due to a currency exchange holiday (i.e., a public holiday in a given country).

FEBRUARY	
5	IE
8	SI
12	CN, HK, JP, SG
13	CN, HK, PT
14	CN
15	CN
16	CN, LT, SG
19	CA, CY
20	CN
21	CN
23	JP, RU

MARCH	
8	RU, UA
11	LT
15	HU
18	CY, GR
20	JP
21	ZA
25	CY, GR
28	DK, IS, NO
29	AT, AU, BE, CA, CH, CY, CZ, DE, DK, EE, EU, ES, FI, GB, HK, HR, HU, IE, IS, IT, LT, LU, NL, NO, PT, SE, SI, SG, SK, ZA
31	Easter

BACK >>