citi handlowy

czytaj Aktualności CitiService

Luty 2024 r. | Wydanie nr 2

Uważaj na próby wyłudzenia informacji

WIĘCEJ >>

Ważne – złóż oświadczenie o przedsiębiorstwie (FINREP)

WIĘCEJ >>

CitiDirect Mobile Token: odkryj nową metodę szybkiego logowania

WIĘCEJ >>

Przelewy zagraniczne: SHA jako domyślna opcja kosztowa

WIĘCEJ >>

Święta walut: luty i marzec 2024 r.

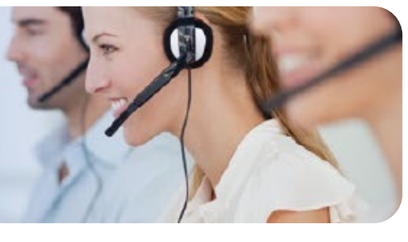
WIĘCEJ >>

Serwisy na skróty:

- Wyciąg z Taryfy Prowizji i Opłat Bankowych — Sprawdź >>
- Tabela kursów — Sprawdź >>
- Analizy rynkowe — Sprawdź >>
- Strefa Klienta — Sprawdź >>
- Archiwum Aktualności — Sprawdź >>
- Bankowość elektroniczna: szkolenia online — Sprawdź >>
- Bankowość elektroniczna: filmy instruktażowe — Sprawdź >>
- Bankowość elektroniczna: podręczniki i dokumenty — Sprawdź >>

Szybki kontakt z doradcą CitiService

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



Przedsiębiorstwa stają w obliczu wielu złożonych i wciąż zmieniających się zagrożeń związanych z komunikacją poprzez pocztę elektroniczną – od przejęcia konta i naruszenia bezpieczeństwa poczty biznesowej po tzw. spear phishing i vishing. Cyberprzestępcy często wykorzystują złośliwe linki do ataków phishingowych lub infekcji złośliwym oprogramowaniem.

Kliknięcie takich linków lub otwarcie załącznika przez pracownika może narazić Państwa firmę na różne zagrożenia, od kradzieży tożsamości po wyciek poufnych informacji oraz utratę środków.
Osoby atakujące mogą używać wiadomości e-mail zawierających linki i załączniki, które wyglądają na autentyczne i wiarygodne, ale mają na celu wyłudzenie danych. Aby się ustrzec przed cyberatakiem, warto przed otwarciem załącznika lub kliknięciem w link przyjrzeć się uważniej takiej wiadomości.

Oto kilka prostych kroków, aby sprawdzić, czy otrzymany e-mail pochodzi z naszego banku:

1. Poczta odbiorcy weryfikuje wiadomości e-mail na podstawie adresu nadawcy. Należy pamiętać, że w przypadku wiadomości e-mail z systemu CitiDirect jest to zawsze citidirectbe.notifications@citi.com, a w przypadku CitiManagera – citicommercialcards.admin@citi.com. Wiadomości e-mail Citi Handlowy są zawsze wysyłane z domeny @citi.com.
2. Citi Handlowy stosuje mechanizmy uwierzytelniania poczty elektronicznej SPF, DKIM i DMARC w celu zwiększenia bezpieczeństwa poczty elektronicznej oraz zapobiegania atakom typu e-mail spoofing i phishing. Jeśli Państwa firmowy serwer pocztowy jest odpowiednio skonfigurowany, złośliwa wiadomość e-mail nie zostanie dostarczona lub trafi do folderu ze spamem.
3. Prosimy o zapoznanie się z logotypem oraz stylem komunikacji naszego banku (m.in. poprzez odwiedzenie naszej strony głównej), aby umieć ją odróżnić. Wysłane przez nas wyciągi są szyfrowane, a powiadomienia, tj. salda, zawsze będą miały zamaskowane szczegóły.
4. www banku Citi Handlowy to adres URL bezpiecznej witryny: HTTPS (na początku adresu URL). HTTPS wykorzystuje bezpieczne certyfikaty, które weryfikują uprawnienia serwera witryny i szyfrują przesyłane dane. Linki HTTP są mniej bezpieczne i częściej mogą prowadzić do niebezpiecznych witryn.

Powyższe kroki oraz wzmożona czujność pozwolą Państwu odróżnić naszą komunikację od próby podszycia się cyberprzestępców pod nasz bank w celu kradzieży cennych informacji oraz środków firmy.

Aby dowiedzieć się więcej o niektórych typowych oszustwach, a także o najlepszych praktykach w zakresie bezpieczeństwa cybernetycznego, odwiedź stronę https://www.citibank.pl/poland/citidirect/polish/bezpieczenstwo/bezpieczenstwo-bankowosci-online.htm lub zapisz się na darmowe szkolenie „Bezpieczeństwo w sieci”.

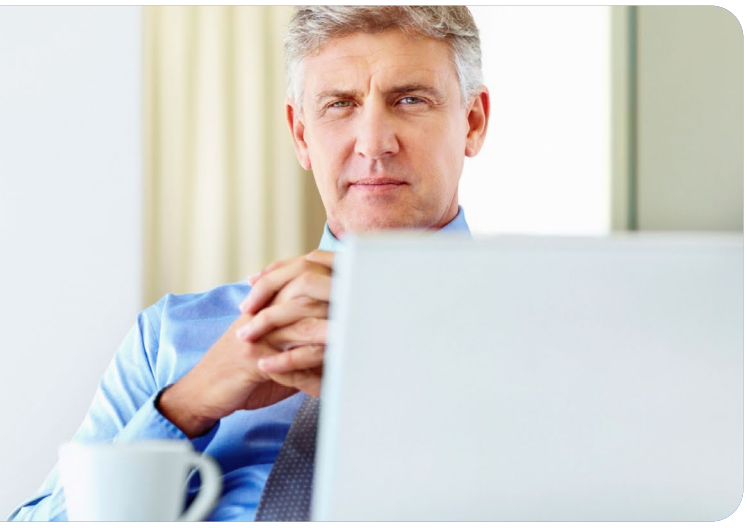
POWRÓT >>

Wyznacz Administratora Kart Business >>

by samodzielnie zarządzać programem kart business dla pracowników, bez zbędnych formalności i potrzeby kontaktu z bankiem.

citi handlowy

Ważne – złóż oświadczenie o przedsiębiorstwie (FINREP)



Informujemy, że Bank Handlowy w Warszawie S.A. rozpoczął proces aktualizacji danych o zatrudnieniu w spółkach naszych klientów w związku z wymogami Ustawy z 29 sierpnia 1997 r. o Narodowym Banku Polskim oraz Uchwały nr 71/2016 z 22 grudnia 2016 r. Celem jest właściwe określenie kategorii podmiotu, klienta banku (na podstawie liczby zatrudnionych), zgodnie z instrukcją FINREP sprawozdawczości finansowej.

Bank jest zobowiązany przekazywać co roku do instytucji nadzorczych informacje o liczbie klientów obsługiwanych w danych kategoriach. W związku z tym zwracamy się do Państwa z prośbą o potwierdzenie, czy Państwa firma należy do kategorii dużego przedsiębiorstwa, czy małego i średniego przedsiębiorstwa (MŚP). Decyduje o tym liczba zatrudnionych, gdzie wartością graniczną jest 250 osób zatrudnionych (nie włączając umów-zleceń, umów o dzieło i pracowników sezonowych).

W tym celu prosimy o **wypełnienie** Oświadczenia dotyczącego klasyfikacji FINREP oraz złożenie go **do 20 lutego 2024 r.** na jeden z poniższych sposobów:

1. poprzez eWnioski – Instrukcja tutaj >>
2. przesyłając Oświadczenie z podpisem kwalifikowanym drogą mailową bezpośrednio do doradcy lub na adres citiservice.polska@citi.com.
3. Oświadczenie powinno być podpisane zgodnie z reprezentacją z wyciągu z rejestru, stosownym pełnomocnictwem bądź reprezentacją na KWP.
4. Oświadczenia podpisane odręcznie można też dostarczyć (przesłać) w oryginale na adres:

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

   z dopiskiem: **oświadczenie FINREP**
5. Link do Oświadczenia dotyczącego klasyfikacji FINREP

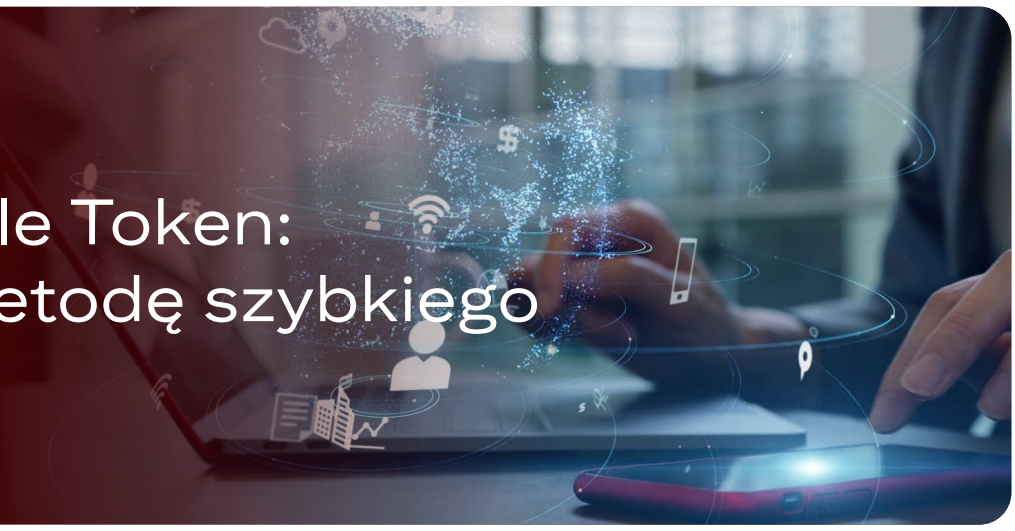
POWRÓT >>

Wyznacz Administratora Kart Business >>

by samodzielnie zarządzać programem Kart Business dla pracowników, bez zbędnych formalności i potrzeby kontaktu z bankiem.

citi handlowy

CitiDirect Mobile Token: odkryj nową metodę szybkiego logowania



Token Mobilny CitiDirect jest już dostępny w 101 krajach w ramach Citi i ma docelowo zmienić MobilePASS, który jest stopniowo dezaktywowany dla użytkowników korzystających z kilku metod logowania.

Dlaczego warto zmienić metodę logowania i przejść na nową, wyższą wersję tokena mobilnego? **CitiDirect Mobile Token** to stosunkowo nowy, bo wprowadzany od 2022 roku, sposób logowania dostępny w aplikacji mobilnej CitiDirect, który umożliwia użytkownikom logowanie do CitiDirect zarówno w wersji na komputer, jak i aplikacji mobilnej. Konfiguracja jest prosta, aktywacja zajmuje zaledwie kilka minut, a logowanie jest łatwiejsze niż wcześniej!

Dzięki CitiDirect Mobile Token użytkownicy mogą łatwo i szybko – w ciągu zaledwie kilku minut – potwierdzić swoją tożsamość i uzyskać bezpieczny dostęp do systemu CitiDirect z poziomu komputera lub aplikacji mobilnej. W połączeniu z uwierzytelnianiem biometrycznym CitiDirect (odciski palców lub rozpoznawanie twarzy) to wygodny sposób logowania do CitiDirect.

Możesz teraz włączyć CitiDirect **Mobile Token** dla użytkowników, wykonując te proste kroki: Token Mobilny CitiDirect – Aktywacja Przewodnik dla Administratorów Systemu. Następnie użytkownik może łatwo aktywować swój Mobile Token: Zobacz film AKTYWACJA >> i zalogować się do CitiDirect: Zobacz film LOGOWANIE >>

Dlaczego warto korzystać z CitiDirect **Mobile Token**?

ŁATWY W OBSŁUDZE

- Nowoczesny wygląd, dopasowany do urządzeń mobilnych
- Zrozumiałe, kontekstowe instrukcje
- Wizualny wskaźnik prezentujący status logowania w czasie rzeczywistym

BEZPIECZNY

- Przypisany do konkretnego urządzenia
- Silne protokoły weryfikacji
- Mechanizmy kontroli w oparciu o czas, wbudowane parametry bezpieczeństwa

WYGODNY

- Aktywacja poniżej 2 minut
- Logowanie za pomocą szybkiego skanowania kodu QR – możliwość dodania uwierzytelniania biometrycznego
- Ponowna aktywacja w zasięgu ręki

Zainstaluj aplikację mobilną **CitiDirect BE Mobile,** w której możesz sprawdzić saldo i wykonać autoryzację płatności **w dowolnym momencie, nawet jeśli nie masz dostępu do komputera stacjonarnego.** Aplikacja ma prosty i przezroczysty interfejs oraz silne mechanizmy bezpieczeństwa, takie jak możliwość potwierdzenia logowania do systemu za pomocą biometrii (odciski palców lub Face ID). **CitiDirect BE Mobile** pomoże Ci:

- autoryzować i zlecać płatności
- sprawdzić saldo rachunku
- wyświetlić podgląd historii operacji oraz szczegółów dokonanych płatności
- wyszukać płatności
- połączyć profile firmy
- autoryzować zmiany wprowadzone przez administratorów systemu
- korzystać z identyfikacji biometrycznej użytkownika (odciski palców lub Face ID)

Aplikacja jest dostępna dla Apple iOS i Android.

Więcej informacji można znaleźć w następujących materiałach:

CitiDirect Mobile Token Często zadawane pytania >>

CitiDirect BE Mobile >>

POWRÓT >>

Wyznacz Administratora Kart Business >>

by samodzielnie zarządzać programem Kart Business dla pracowników, bez zbędnych formalności i potrzeby kontaktu z bankiem.

citi handlowy

Przelewy zagraniczne: SHA jako domyślna opcja kosztowa

Przypominamy, że dla płatności zagranicznych do banków znajdujących się w Europejskim Obszarze Gospodarczym, niezależnie od waluty transakcji, stosuje się jako domyślną opcję kosztową SHA (Wspólne). Wynika to z wytycznych Ustawy o Usługach Płatniczych wdrażającej postanowienia dyrektywy PSD2.

Bank nie ma prawa ingerować w utworzone przez Państwa zlecenia płatności. Dlatego jeśli wybrana zostaje opcja OUR, to z taką opcją płatność zostanie przekazana do realizacji, przy czym może to wiązać się z odrzuceniem danej transakcji przez bank beneficjenta, który nie będzie honorował tej opcji kosztowej. Jednocześnie, w przypadku braku wskazania opcji kosztowej, system ustawia opcję domyślną – SHA (Wspólne), zgodnie z wcześniej przywołanymi zasadami.

WAŻNE: przy zlecaniu płatności w obszarze EOG prosimy zwrócić szczególną uwagę na wybór opcji SHA. Wybór innej opcji kosztowej może skutkować odrzuceniem płatności.

UWAGA: Narodowy Bank Rumunii w ramach migracji na standardy ISO 20022 zdecydował o braku możliwości stosowania opcji BEN/OUR. Od 2 lutego 2024 r. płatności w leju rumuńskim (RON), w których strona zlecająca wskaże opcję BEN lub OUR – będą odrzucane. Banki rumuńskie będą przyjmować tylko płatności zlecone z opcją kosztową SHA.

POWRÓT >>

Wyznacz Administratora Systemu >>

by samodzielnie zarządzać rachunkiem bankowym,
bez zbędnych formalności i potrzeby kontaktu z bankiem.

citi handlowy

Święta walut:
luty i marzec 2024 r.

Prezentujemy Państwu dni w **lutym i marcu 2024 r.**, w których dokonane zlecenia będą realizowane następnego dnia roboczego ze względu na dni wolne od pracy w danym kraju.

LUTY	
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

MARZEC	
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	Wielkanoc

POWRÓT >>

http://www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

Niniejszy materiał marketingowy został wydany jedynie w celach informacyjnych i nie stanowi oferty w rozumieniu art. 66 Kodeksu cywilnego. Linki umieszczane w naszych komunikatach prowadzą do stron internetowych lub materiałów marketingowych naszego Banku lub naszych partnerów, które mają charakter informacyjny. Nie wykorzystujemy linków do zbierania danych wrażliwych od naszych Klientów. Jeśli cokolwiek budzi Państwa zastrzeżenia, prosimy o kontakt z nadawcą komunikatu ze strony Banku. Znaki Citi oraz Citi Handlowy stanowią zarejestrowane znaki towarowe Citigroup Inc., używane na podstawie licencji. Spółce Citigroup Inc. oraz jej spółkom zależnym przysługują również prawa do niektórych innych znaków towarowych tu użytych. Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923 Warszawa, zarejestrowany przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS 000 000 1538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522 638 400 złotych, kapitał został w pełni opłacony.