



kodeks bezpieczeństwa

W kodeksie bezpieczeństwa znajdziesz wskazówki, jak bezpiecznie korzystać z bankowości internetowej i mobilnej oraz jak chronić się przed cyberprzestępcami.



Pamiętaj, jeśli zauważysz coś podejrzanego lub coś Cię zaniepokoi, zgłoś nam to jak najszybciej.



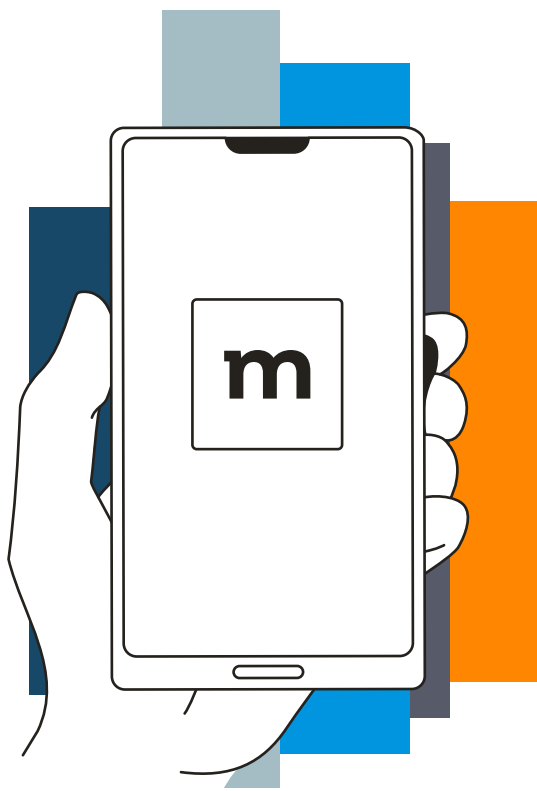
zachowaj ostrożność, gdy logujesz się na konto

- **sprawdź poprawność adresu** strony logowania, a najlepiej **samodzielnie wpisz go** w pasku adresu w przeglądarce
- **nie podawaj danych** do logowania na stronach, do których linki otrzymasz SMS-em, mailem, na portalach społecznościowych lub przez komunikatory
- **zadbaj, żeby nikt nie widział** Twojego loginu, kiedy go wpisujesz
- **nie zapisuj loginu** do konta w przeglądarce, ani nikomu go nie udostępniaj
- jeśli zauważysz coś nietypowego, np. dodatkowe pole do wprowadzenia loginu, tokena, QR tokena, dodatkowych danych lub strona wygląda inaczej niż zwykle – nie loguj się, tylko **zgłoś nam to jak najszybciej**
- **unikaj logowania** z cudzych komputerów i urządzeń mobilnych oraz z publicznych sieci Wi-Fi

potwierdź zmianę rachunku do płatności i nietypowe prośby o przelew



- jeśli dostaniesz wiadomość o zmianie rachunku do płatności lub zauważysz inny niż dotychczas numer rachunku na fakturze, **potwierdź tę zmianę** telefonicznie lub osobiście
- zawsze potwierdź **innym kanałem komunikacji** lub osobiście nietypowe prośby o przelew z osobą, która wysłała Ci taką wiadomość (nawet jeśli prośbę o przelew wysłał Twój znajomy, ktoś z rodziny, współpracownik lub przełożony)



pamiętaj o zasadach bezpieczeństwa, gdy korzystasz z aplikacji mobilnej

- potwierdzaj operacje w banku za pomocą **mobilnej autoryzacji lub QR tokena**
- włącz **powiadomienia** o przelewach wychodzących
- włącz **blokadę ekranu** telefonu
- korzystaj z **najnowszej wersji aplikacji** mobilnej

uważaj, gdy ktoś przez telefon prosi o Twoje dane lub wykonanie operacji



- nigdy **nie podawaj swoich danych wrażliwych** (np. loginu czy danych karty) osobie, która prosi o nie przez telefon, nawet jeśli podaje się za pracownika banku lub policji
- zachowaj szczególną ostrożność, **gdy ktoś prosi Cię o przekazanie pieniędzy** – to może być oszust, który podaje się np. za członka rodziny, Twojego znajomego, policjanta lub prezesa firmy



zadbaj o bezpieczeństwo urządzeń, z których logujesz się do banku

- zadbaj o aktualizacje systemu operacyjnego swojego urządzenia, żeby mieć zawsze **najnowszą wersję** - to pozwoli wyeliminować luki bezpieczeństwa
- korzystaj z **programów, które chronią** komputery i urządzenia mobilne przed złośliwym oprogramowaniem (np. antywirus, firewall)
- aplikacje i programy pobieraj tylko z **oficjalnych sklepów** (Google Play, App Store), nie pobieraj ich z niezauważanych źródeł

uważaj na SMS-y, maile i QR kody – linki w nich zawarte mogą prowadzić do fałszywych stron, a otwarcie załącznika może instalować złośliwe oprogramowanie



- **nie otwieraj linków** z wiadomości bez upewnienia się, kto faktycznie ją wysłał i nigdy nie podawaj swoich danych na stronie, na którą taki link przenosi
- zwróć uwagę na **format załączników** z wiadomości – szczególnie uważaj na pliki, które mają w nazwie kilka rozszerzeń (np. faktura_10.pdf.exe, przelew.pdf.zip, wypłata.jar.doc) takie pliki mogą zainfekować Twoje urządzenie złośliwym oprogramowaniem
- jeśli masz wątpliwości, czy wiadomość jest wiarygodna, **skontaktuj się z nadawcą** w inny sposób (np. telefonicznie), dane kontaktowe znajdź na oficjalnej stronie firmy
- zachowaj ostrożność, **gdy korzystasz z kodów QR** – jeśli nie masz pewności, czy kod QR jest bezpieczny i pochodzi z zaufanego źródła, nie skanuj go



uważnie czytaj powiadomienia, którymi potwierdzasz operacje bankowe

- **dokładnie sprawdzaj**, czy dane w powiadomieniu dotyczą zleconej przez Ciebie operacji – jeśli coś się nie zgadza (np. numer rachunku odbiorcy przelewu, kwota lub rodzaj operacji), nie potwierdzaj jej
- jeśli dostaniesz powiadomienie o operacji bankowej, która nie została przez Ciebie zlecona, **odrzuć ją**
- skontaktuj się z nami, jeśli dostaniesz **nietypowe powiadomienie lub podejrzaną wiadomość**

uważaj na fałszywe sklepy i oszustwa na portalach sprzedażowych



- **zawsze sprawdzaj sklepy internetowe** – zwłaszcza, jeśli oferują produkty, których cena jest podejrzanie niska, np. wyprzedaże (poszukaj opinii o sklepie na niezależnych stronach, sprawdź, czy dane sklepu w regulaminie są zgodne z danymi w publicznym rejestrze KRS lub CEiDG)



uważaj na oferty tak dobre, że mało realne, możesz przez nie stracić dane lub pieniądze

- zachowaj czujność zawsze, **gdy ktoś obiecuje Ci duże zyski** z inwestycji przy minimalnym ryzyku i dużej presji czasu
- **sprawdzaj na stronie** Komisji Nadzoru Finansowego, czy firma inwestycyjna ma potrzebne zezwolenia oraz czy nie znajduje się na liście ostrzeżeń publicznych KNF

chronić dane swojej karty



- **nie podawaj danych karty** na stronach, do których link dostajesz w mailach, SMS-ach lub na komunikatorach oraz nie przekazuj takich danych innym osobom (np. w rozmowie telefonicznej)
- gdy płacisz kartą w sklepie lub restauracji, **nie trać karty z oczu** – dopilnuj, żeby płatność odbywała się w Twojej obecności
- gdy wypłacasz pieniądze z bankomatu, **zwróć uwagę**, czy na urządzeniu nie ma obco wyglądających listew lub nakładek, w których mogą być ukryte urządzenia kopiujące dane z Twojej karty
- gdy wpisujesz PIN karty, koniecznie **zasłoń klawiaturę**, żeby nikt nie mógł go zobaczyć i nigdy nie przekazuj go innej osobie
- **dostosuj limity** na karcie do kwoty Twoich zakupów
- zwracaj uwagę, na którym urządzeniu **dodajesz swoją kartę do płatności Google Pay/Apple Pay** - jeśli dodasz kartę na nie swoim urządzeniu, inna osoba będzie miała dostęp do Twoich pieniędzy
- dane karty służą **wyłącznie do wykonywania płatności** - nigdy nie podawaj ich, aby odebrać pieniądze