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

- **sprawdzaj poprawność adresu** strony logowania, a najlepiej **samodzielnie wpisuj 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
- **nie zapisuj identyfikatora i hasła** do konta w przeglądarce internetowej
- **zadbaj, żeby nikt nie widział** Twojego identyfikatora i hasła, kiedy je wpisujesz
- jeśli zauważysz coś nietypowego, np. dodatkowe pole do wprowadzenia hasła lub innych danych, nie loguj się, tylko **zgłoś nam to jak najszybciej**
- **unikaj logowania** z cudzych komputerów i urządzeń mobilnych oraz z publicznych sieci Wi-Fi

dobre hasło jest łatwe do zapamiętania a trudne do odgadnięcia



- użyj **minimum 12 znaków**, w tym wielkich i małych liter oraz cyfr i znaków specjalnych
- nie używaj w hasłach informacji, **które łatwo z Tobą powiązać** (np. nazwisko, data urodzenia) lub odgadnąć (np. aktualny miesiąc, rok, ciąg kolejnych liter lub cyfr)
- **stosuj hasła trudne do odgadnięcia**, np. wykorzystaj pierwsze znaki cytatu, powiedzenia, ulubionej piosenki
- **zastąp literę** cyfrą, znakiem specjalnym lub celowo błędem ortograficznym



zadbaj o bezpieczeństwo urządzeń, z których logujesz się do banku

- stosuj **zalecenia bezpieczeństwa** w aplikacji - znajdziesz je w sekcji bezpieczeństwa na pulpicie (ikona tarczy)
- zadbaj o **najnowsze aktualizacje** systemu operacyjnego swojego urządzenia oraz aplikacji mobilnej, to pozwoli wyeliminować luki bezpieczeństwa
- aplikacje i programy pobieraj tylko **z oficjalnych sklepów** (Google Play, App Store, App Gallery), nie pobieraj ich z niezaufanych źródeł
- korzystaj z **programów, które chronią** komputery i urządzenia mobilne przed złośliwym oprogramowaniem (np. antywirus, firewall)
- włącz **blokadę ekranu** telefonu

uważaj na SMS-y oraz maile – linki w nich zawarte mogą prowadzić do fałszywych stron, a otworzenie 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, wyplata.jar.doc), takie pliki mogą zainfekować Twoje urządzenie złośliwym oprogramowaniem
- jeśli masz wątpliwości, czy wiadomość jest wiarygodna, **skontaktuj się z nadawcą** (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



chroń 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 sczytujące 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

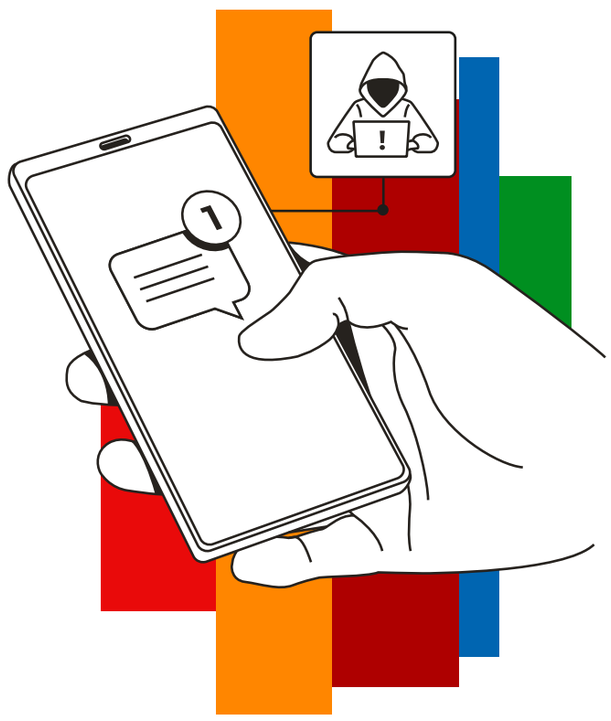
- dane karty służą **wyłącznie do wykonywania płatności** - nigdy nie podawaj ich, aby odebrać pieniądze

potwierdzaj 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 potwierdzaj **innym kanałem komunikacji** lub osobiście nietypowe prośby o przelew z osobą, która wysyła Ci taką wiadomość (nawet jeśli prośbę o przelew wysłał Twój znajomy, ktoś z rodziny, współpracownik lub przełożony)



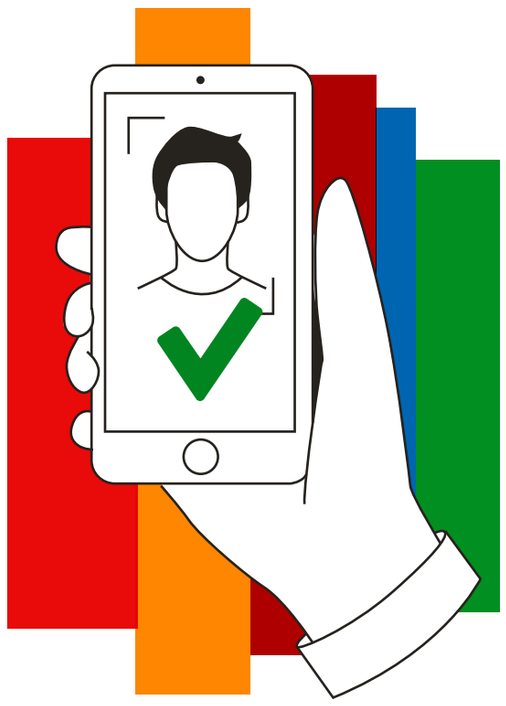
uważnie czytaj powiadomienia lub SMS-y, którymi potwierdzasz operacje bankowe

- **dokładnie sprawdzaj**, czy dane w powiadomieniu mobilnej autoryzacji lub SMS-ie 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 (np. o wypłacie BLIK lub o dodaniu nowego urządzenia do Twojego konta), **odrzuć ją**
- skontaktuj się z nami, jeśli dostaniesz **nietypowe powiadomienie lub podejrzaną wiadomość**

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
- **nie daj się nabrać** na wygraną w konkursie lub loterii, w której nie bierzesz udziału
- zanim wypełnisz formularz zgłoszeniowy do konkursu, loterii lub inwestycji, **zawsze sprawdź, czy strona jest wiarygodna**
- nie ufaj ofertom pracy, które otrzymujesz bezpośrednio na swoją skrzynkę pocztową, szczególnie tym **wyjątkowo „atrakcyjnym”**



upewnij się, że rozmawiasz z pracownikiem mBanku

- pamiętaj, gdy zadzwoni do Ciebie nasz pracownik, **dostaniesz w aplikacji mobilnej** mBanku powiadomienie z jego danymi
- jeśli nie dostaniesz powiadomienia w aplikacji, **koniecznie o nie poproś** – będziesz mieć pewność, że rozmawiasz z naszym pracownikiem, a nie oszustem, który się za niego podaje
- jeśli podczas rozmowy poprosisz o potwierdzenie jej w aplikacji i nie dostaniesz powiadomienia, **rozłącz się** i zgłoś nam taką rozmowę



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

- nigdy **nie podawaj swoich danych wrażliwych** (np. identyfikatora lub hasła do konta, danych karty, czy kodu BLIK) osobie, która prosi o nie przez telefon, nawet jeśli podaje się za pracownika banku, policji lub Twojego znajomego
- pamiętaj – prawdziwy pracownik banku, policji lub innej instytucji **nigdy nie poprosi Cię o takie dane**, a także o wykonanie przelewu z Twojego konta, czy instalację dodatkowej aplikacji/programu oraz nie będzie Cię namawiać do kliknięcia w link
- 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



uważaj na fałszywe sklepy i oszustwa na portalach sprzedażowych

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

- gdy korzystasz z portalu sprzedażowego, nie ufaj kupującym i sprzedającym, którzy chcą przenieść komunikację na maila lub komunikator, zawsze płać za zakupy i komunikuj się **za pośrednictwem tego portalu**

- gdy do wystawionego przedmiotu na portalu sprzedażowym otrzymasz wiadomość z informacją, że ktoś go kupił, a w wiadomości jest link do „odbioru pieniędzy”, **nigdy nie klikaj w taki link**

- jeśli ktoś wywołuje na Tobie presję czasu (np. informuje, że oferta dostępna w sklepie internetowym „zaraz straci ważność”) – **zachowaj szczególną ostrożność**, to może być oszust, który chce uśpić Twoją czujność

- **nigdy nie ufaj telefonom** od osób, które podają się za pracownika portalu sprzedażowego i namawiają do kliknięcia w link (np. do „odbioru wpłaty”), czy podania danych karty lub kodu BLIK, aby zweryfikować Twoje konto

nie podawaj nikomu kodu BLIK



- gdy ktoś poprosi Cię o kod BLIK (np. na komunikatorze), **nigdy go nie podawaj**, nawet jeśli jest to osoba, którą znasz – zadzwoń do niej i potwierdź, czy właśnie do Ciebie napisała

- kod BLIK służy **wyłącznie do wykonywania płatności** – nigdy nie potwierdza się nim tożsamości, ani nie weryfikuje konta w banku