Zwolnij, pomyśl, sprawdź! Nie podejmuj działań pod presją czasu. Zachowaj ostrożność i zawsze weryfikuj tożsamość osób kontaktujących się w imieniu banku lub instytucji.

Infolinia 24h na dobę 7 dni w tygodniu: **800 302 302**

Zgłoś podejrzaną treść: **informacje@pkobp.pl**



Bank Polski

Stop manipulacji.

Nie daj się zaskoczyć.
Zachowaj uważność.

Oszustwa telefoniczne

Oszust może zadzwonić lub wysłać SMS. Często mówi o rzekomym zagrożonym koncie, blokadzie pieniędzy, pilnej operacji bezpieczeństwa, aby wywołać pośpiech i strach.

Uważaj, gdy ktoś prosi Cię o:

- instalację nieznanej aplikacji,
- przelew na „bezpieczne konto",
- podanie danych logowania lub kodu BLIK,
- logowanie do banku przez link w SMS-ie lub e-mailu.

Zapamiętaj!

Pracownik banku nigdy nie kieruje takich próśb.
Zawsze oznaczają one próbę oszustwa.

- Nie ufaj wyłącznie wyświetlanemu numerowi telefonu: oszust potrafi wyświetlić na telefonie odbiorcy prawidłowy numer instytucji czy osoby, pod którą się podszywa.
- Zweryfikuj rozmówcę w aplikacji IKO – gdy ktoś podaje się za naszego pracownika, poinformuj, że **chcesz potwierdzić jego tożsamość w aplikacji IKO.** W aplikacji otrzymasz powiadomienie z danymi pracownika. Nie korzystasz z aplikacji? Rozłącz się i skontaktuj się z nami samodzielnie.

Podejrzane wiadomości i strony internetowe

Co robią oszuści?

- Przesyłają SMS-y lub e-maile z linkami prowadzącymi do fałszywych stron internetowych, które wyglądają jak prawdziwe. Służą one do wyłudzania danych i pieniędzy.

Jak się chronić?

- Jeśli nie masz pewności, od kogo pochodzi wiadomość, nie klikaj w linki. **W naszych SMS-ach i e-mailach nie stosujemy linków.**
- Sprawdzaj adres strony WWW – to on jest wyznacznikiem autentyczności strony. Pamiętaj, że widoczny na pasku przeglądarki symbol kłódki nie świadczy o tym, że strona jest bezpieczna.
- Adres strony internetowej banku wpisuj ręcznie w przeglądarce, nigdy nie loguj się przez wysłany do Ciebie link.

Zysk bez ryzyka to pułapka!

Co robią oszuści?

- Obiecują szybki i pewny zysk „bez ryzyka".
- Reklamują swoje oferty w internecie, często w mediach społecznościowych.
- Pokazują zmanipulowane treści wideo, w których nielegalnie wykorzystują wizerunki znanych osób i firm.
- Często zachęcają do instalacji programu do „inwestowania", aby przejąć dostęp do Twojego urządzenia.

Firmy inwestycyjne działające zgodnie z prawem nie obiecują gwarantowanych zysków i przekazują informacje w sposób rzetelny. Przed zaoferowaniem usług inwestycyjnych zazwyczaj proszą o wypełnienie ankiety w celu oceny Twojego profilu inwestora – m.in. skłonność do ryzyka, wiedzę i cele finansowe.

Jak się chronić?

- Zachowaj rozsądek i krytyczne podejście do ofert wysokiego zysku bez informacji o ryzyku.
- Pamiętaj, że wiarygodność oferty zawsze trzeba sprawdzić, niezależnie od tego, gdzie została opublikowana. Oszuści też korzystają z możliwości reklamowania i sponsorowania swoich ofert.
- Zachowaj ostrożność, **gdy ktoś żąda od ciebie skanu dowodu osobistego, udostępnienia poufnych danych, nakłania do pośpiechu w celu szybkiego przekazania środków.**
- Nie instaluj nieznanych aplikacji i programów oraz uważaj na sugestie instalacji aplikacji zdalnego pulpitu.