Dzwoni telefon. 📞 Na wyświetlaczu widzisz numer, który wygląda jak infolinia Twojego banku 🏦. Po drugiej stronie miły głos: **„Dzień dobry, dzwonię z banku w sprawie podejrzanej transakcji na Pana/Pani koncie. Czy możemy to szybko wyjaśnić?”** W popłochu zaczynasz odpowiadać na pytania, podajesz dane... ale potem okazuje się, że nikt z banku do Ciebie nie dzwonił. 😨

🎯 **Co to jest vishing?**
To oszustwo telefoniczne, w którym przestępcy podszywają się pod pracowników banków, urzędów czy innych zaufanych instytucji. Ich cel? Wyłudzić Twoje dane logowania, kody SMS, a nawet nakłonić Cię do przelania pieniędzy. Wszystko pod pretekstem „ochrony” Twoich środków. 💸

🛡 Jak się bronić?
✅ **Nigdy nie podawaj danych przez telefon** – banki nigdy nie proszą o hasła, kody czy numery kart. ❌
✅ **Zachowaj czujność** – jeśli rozmówca wywołuje w Tobie panikę lub presję, to sygnał ostrzegawczy 🚨.
✅ **Sprawdź numer** – zakończ rozmowę i samodzielnie zadzwoń na oficjalną infolinię swojego banku. 📞
✅ **Nie działaj pod presją** – oszuści liczą na Twój pośpiech. Zawsze daj sobie chwilę na zastanowienie. 🤔

📌 Jeśli podejrzewasz oszustwo:
👉 Natychmiast przerwij rozmowę i zgłoś sprawę swojemu bankowi.
👉 Niezwłocznie zmień hasła do bankowości internetowej.
👉 Powiadom policję, opisując sytuację.

Nie daj się nabrać na fałszywe telefony! 🚫 Zawsze pamiętaj, że bezpieczeństwo Twoich pieniędzy zależy także od Ciebie.

#Vishing #BezpieczeństwoOnline #OszustwoTelefoniczne #BezpiecznaBankowość #UważajNaOszustów #EBO #EBOeBankOnline #EBOMobilePRO