
Dostajesz SMS-a 📱: **„Twoje konto zostało zablokowane. Aby je odblokować, kliknij w poniższy link."** Albo: **„Masz niezapłacony mandat. Ureguluj płatność tutaj, aby uniknąć dodatkowych kosztów."** W wiadomości jest link. W stresie klikasz... i wpadasz w pułapkę. 😨

🎯 **Czym jest smishing?**
To oszustwo polegające na wysyłaniu fałszywych wiadomości SMS. Oszuści podszywają się pod banki, urzędy czy firmy kurierskie 🚚, próbując wyłudzić Twoje dane logowania, dane karty lub nakłonić Cię do zainstalowania złośliwego oprogramowania. 💸

🛡 Jak się bronić?
✅ **Nigdy nie klikaj w podejrzane linki** – szczególnie jeśli wiadomość wygląda na zbyt pilną lub groźną.
✅ **Sprawdzaj nadawcę SMS-a** – nawet jeśli nazwa wydaje się zaufana, numer telefonu może być fałszywy.
✅ **Kontaktuj się z instytucją bezpośrednio** – jeśli masz wątpliwości, zadzwoń na oficjalną infolinię. 📞
✅ **Zabezpiecz swój telefon** – używaj programów antywirusowych i aktualizuj system. 🔒

📌 Jeśli kliknąłeś w podejrzany link:
👉 Natychmiast skontaktuj się z bankiem, by zablokować konto.
👉 Zmień swoje hasła do bankowości internetowej i innych ważnych kont.
👉 Przeskanuj telefon antywirusem i usuń złośliwe oprogramowanie.

Nie daj się złapać na fałszywe SMS-y 📩. Oszuści liczą na Twoje roztargnienie. Bądź czujny i zawsze weryfikuj każdą wiadomość! 🛡

#Smishing #BezpieczeństwoOnline #OszustwaSMS #UważajNaLinki #BezpiecznaBankowość #EBO #EBOeBankOnline #EBOMobilePRO