Wyobraź sobie, że dostajesz e-mail od swojego banku 🏦. Wygląda autentycznie – logo, kolorystyka, a nawet podpis. W wiadomości czytasz: **„Twoje konto zostało tymczasowo zablokowane. Kliknij tutaj, aby je odblokować."** W pośpiechu klikasz link, logujesz się na stronie... ale coś jest nie tak. Strona zbyt długo się ładuje, by na końcu pojawił się komunikat o błędzie.😨

🎯 **Co się wydarzyło?**
To klasyczny przykład phishingu – oszustwa, które polega na wyłudzaniu Twoich danych, np. loginu, hasła czy numeru karty. Oszuści tworzą fałszywe strony, które wyglądają niemal identycznie jak te należące do banków lub innych instytucji. W ten sposób kradną Twoje dane, a Ty możesz stracić pieniądze. 💸

🛡 Jak się chronić?
✅ **Nigdy nie klikaj w podejrzane linki** – banki nie wysyłają linków do logowania w e-mailach czy SMS-ach.
✅ **Sprawdzaj adres strony** – upewnij się, że zaczyna się od „https://" i ma kłódkę 🔒. Kliknij na nią, by sprawdzić certyfikat został wystawiony dla Twojego banku.
✅ **Nie podawaj danych osobowych w wiadomościach e-mail** – żadna poważna instytucja nie poprosi Cię o hasło czy PESEL przez e-mail.
✅ **Zgłaszaj podejrzane wiadomości** – poinformuj swój bank o potencjalnym oszustwie.

📌 Jeśli padłeś ofiarą phishingu:
👉 Natychmiast skontaktuj się z bankiem, aby zablokować dostęp do konta.
👉 Zmień swoje hasła na silniejsze 💪 (z cyframi, literami i znakami specjalnymi).
👉 Powiadom policję i zachowaj dowody, np. e-maile.

Nie daj się złapać na haczyk 🎣! Cyberprzestępcy liczą na Twój pośpiech i roztargnienie. Pamiętaj, że Twoje bezpieczeństwo w sieci zależy również od Ciebie. 🛡

#Phishing #CyberBezpieczeństwo #OszustwoOnline #UważajNaLinki #BezpiecznaBankowość #EBO #EBOeBankOnline #EBOMobilePRO