OBRONA

Dwa rodzaje zagrożeń:

Phishing - fałszywe e-maile, smsy, wiadomości z linkami

Oszustwa związane z interakcją z drugim człowiekiem

Cyberprzestępcy mogą próbować nakłonić Cię do:

- **wykonania** przelewu,
- **przekazania** poufnych danych i informacji, np. kodów autoryzacyjnych, danych do logowania, haseł,
- **zainstalowania** oprogramowania umożliwiającego przejęcie kontroli nad Twoim urządzeniem.

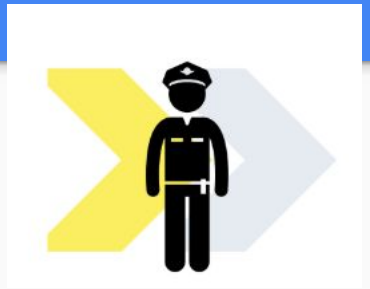
Mogą wykorzystywać różne formy kontaktu m.in.:

wiadomości e-mail

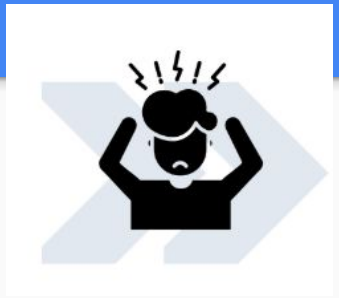
połączenia telefoniczne

wiadomości SMS

Socjotechnika



Zdobywanie zaufania



Manipulowanie emocjami

Wywieranie presji czasowej

Phishing - wyłudzenia danych

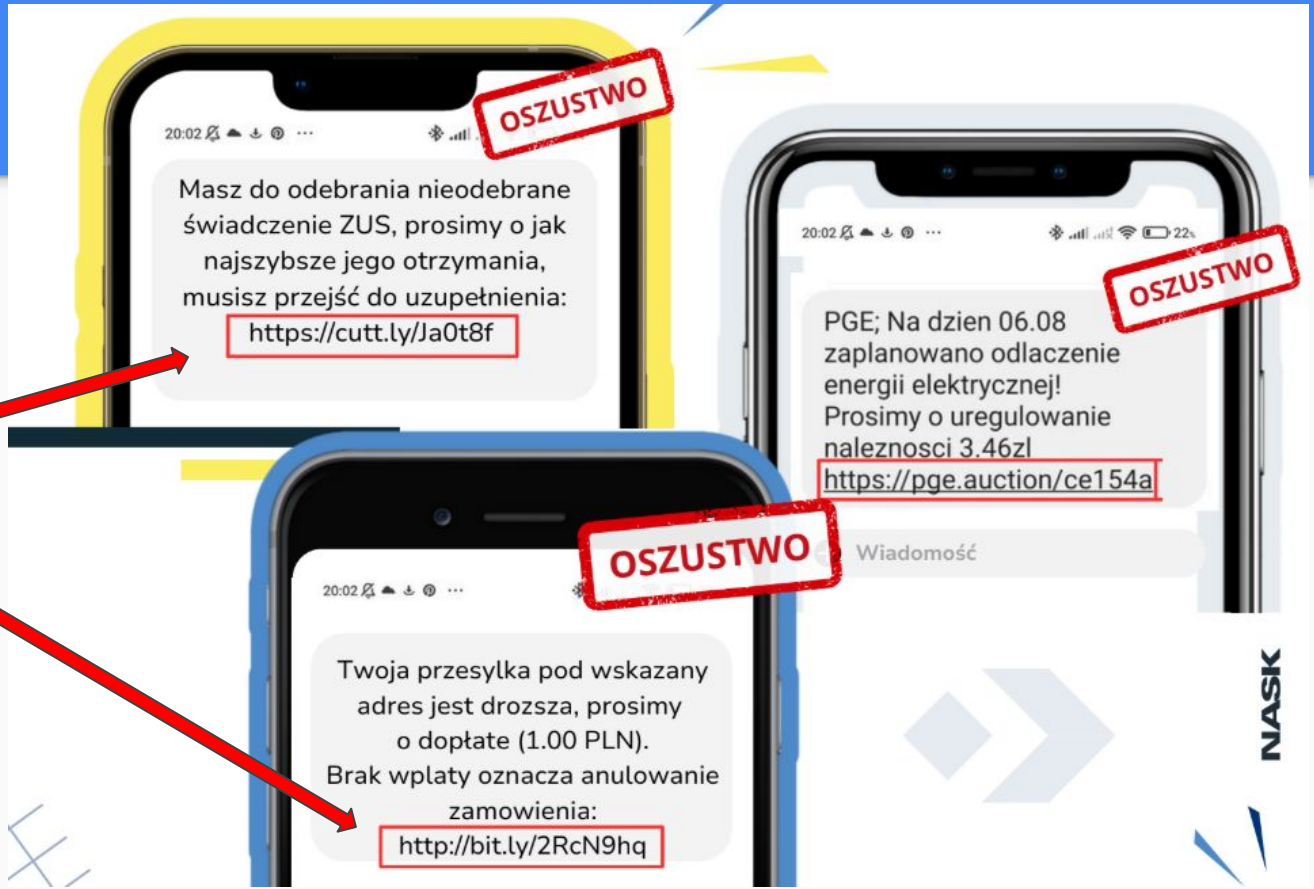
Fałszywe wiadomości, linki, smsy

Przestępcy, pod pretekstem fałszywej wiadomości, **próbują nakłonić Cię do kliknięcia w załączony link, który prowadzi do fałszywej strony** łudząco podobnej do oficjalnej. Może to być na przykład strona banku lub strona służąca do płacenia za zakupy.

Dane, które wprowadzasz na fałszywej stronie, trafiają do oszustów zamiast do zaufanej instytucji. W ten sposób cyberprzestępcy mogą przejąć kontrolę nad Twoim kontem lub wykorzystać Twoje dane do popełnienia innych przestępstw.

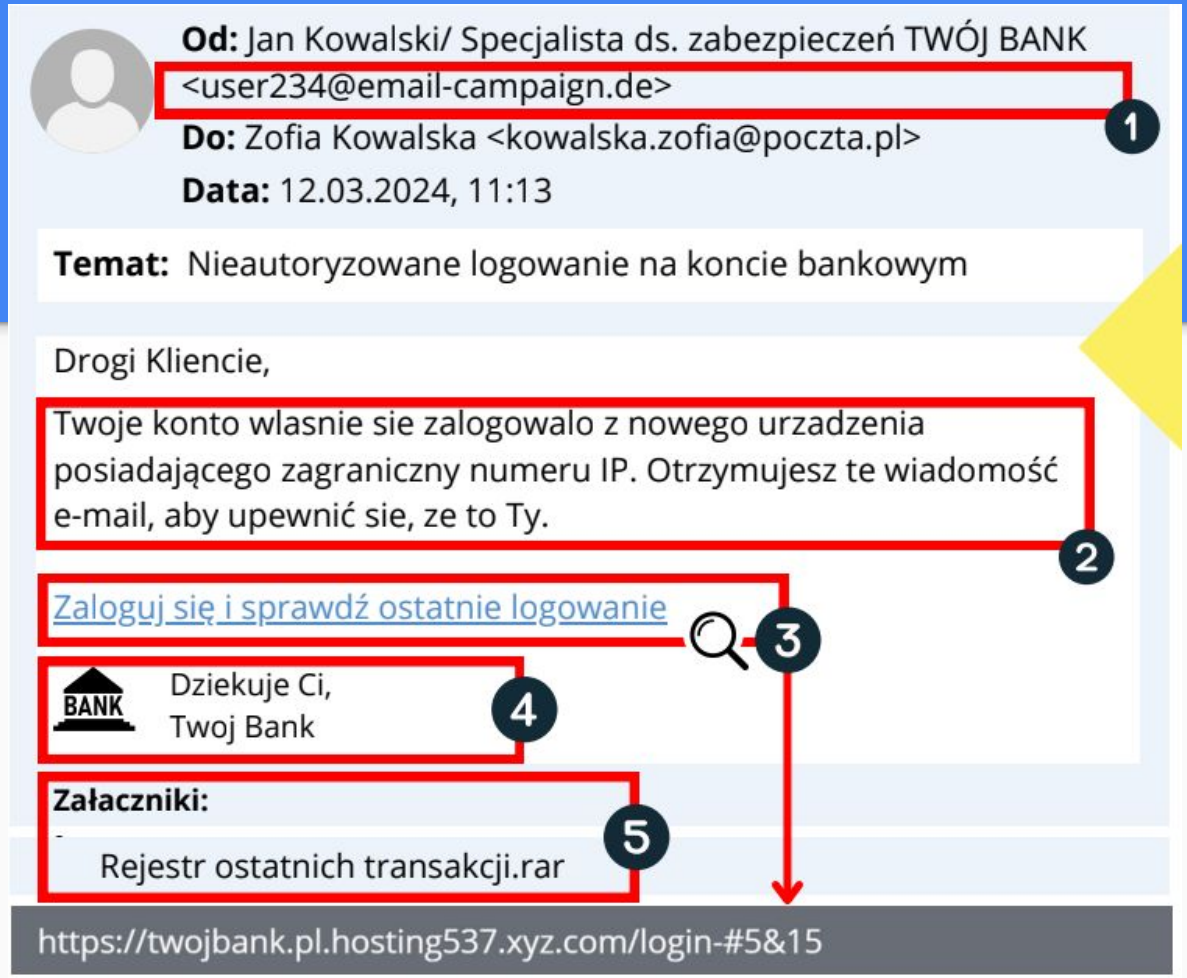
Tematy fałszywych wiadomości

Fałszywe smsy



fałszywe linki

Przykłady:


Od: Jan Kowalski/ Specjalista ds. zabezpieczeń TWÓJ BANK <user234@email-campaign.de>
1
Do: Zofia Kowalska <kowalska.zofia@poczta.pl>
Data: 12.03.2024, 11:13
Temat: Nieautoryzowane logowanie na koncie bankowym
Drogi Kliencie,
Twoje konto wlasnie sie zalogowalo z nowego urzadzenia posiadającego zagraniczny numeru IP. Otrzymujesz te wiadomość e-mail, aby upewnić sie, ze to Ty.
2
Zaloguj się i sprawdź ostatnie logowanie
3
BANK
Dziekuje Ci,
Twoj Bank
4
Załaczniki:
Rejestr ostatnich transakcji.rar
5
https://twojbank.pl.hosting537.xyz.com/login-#5&15

Interakcja z drugim człowiekiem

Oszustwa telefoniczne

Na policjanta, prokuratora lub pracownika innej profesji o dużym zaufaniu publicznym.

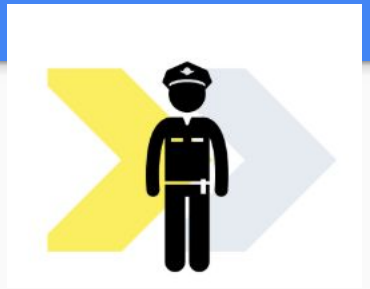
Na pracownika banku lub pomoc techniczną.

Na wypadek spowodowany przez bliską osobę

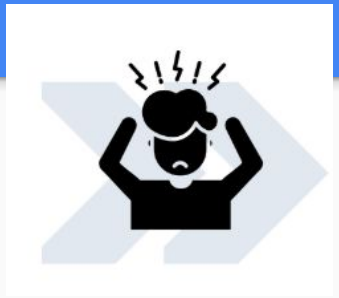
Na wnuczka lub innego członka rodziny.

Na pracownika urzędu skarbowego lub ZUS-u.

Socjotechnika



Zdobywanie zaufania

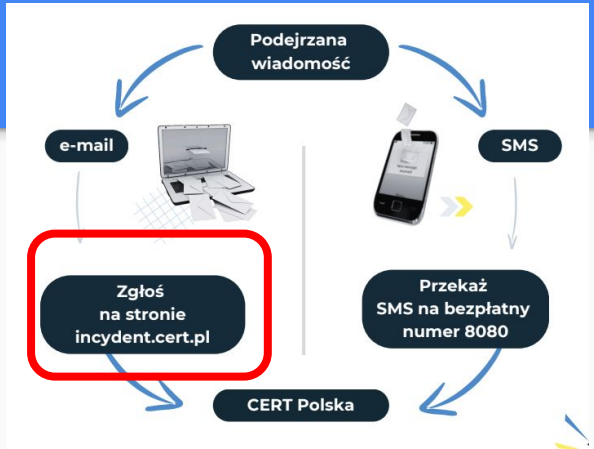


Manipulowanie emocjami

Wywieranie presji czasowej

Jak się chronić przed fałszerstwami socjotechnicznymi?

- **Nie podejmuj żadnych pochopnych decyzji** ani nie działaj pod presją czasu.
- Nie angażuj się w rozmowę, jeśli nie masz pewności, kto jest po drugiej stronie. **Zakończ połączenie i zweryfikuj rozmówcę** dzwoniąc na znany numer instytucji lub udając się do placówki.
- **Nigdy nie podawaj nikomu wrażliwych danych,** takich jak: PESEL, hasła logowania czy kody autoryzacyjne.
- **Nie pobieraj ani nie instaluj aplikacji lub oprogramowania** za czyjąś namową – może to umożliwić nieautoryzowany, zdalny dostęp do Twojego urządzenia.
- **Poinformuj bliskich!** Jeśli otrzymasz nietypowy telefon, skontaktuj się z zaufaną osobą, by pomogła Ci ocenić sytuację i podjąć właściwą decyzję.



Wszelkie niepokojące sytuacje w internecie, np. strony wyłudzające dane, SMS-y z dopłatą do paczki, należy zgłaszać do **CERT** Polska: za pośrednictwem formularza i mailowo na incydent@cert.pl.
Wiadomości tekstowe można przesyłać bezpośrednio na numer 8080 oraz na WhatsAppie - 780 907 000.

Podejrzana wiadomość

e-mail

SMS

Zgłoś na stronie incydent.cert.pl

Przekaż SMS na bezpłatny numer 8080

CERT Polska