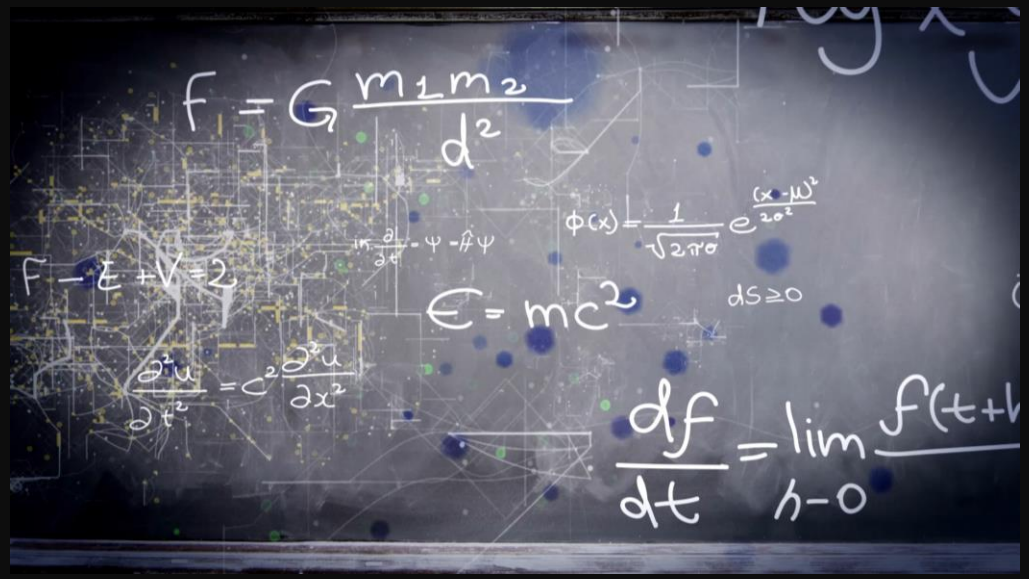
Socjotechnika w cyberatakach

Na co uważać i jak się bronić?



Beata Zalewa

Agenda

- Wprowadzenie do socjotechniki
- Rodzaje ataków socjotechnicznych
- Psychologia socjotechniki
- Przykłady skutecznych kampanii socjotechnicznych
- Obrona przed atakami socjotechnicznymi
- Podsumowanie i dodatkowe zasoby

Zaczynamy !

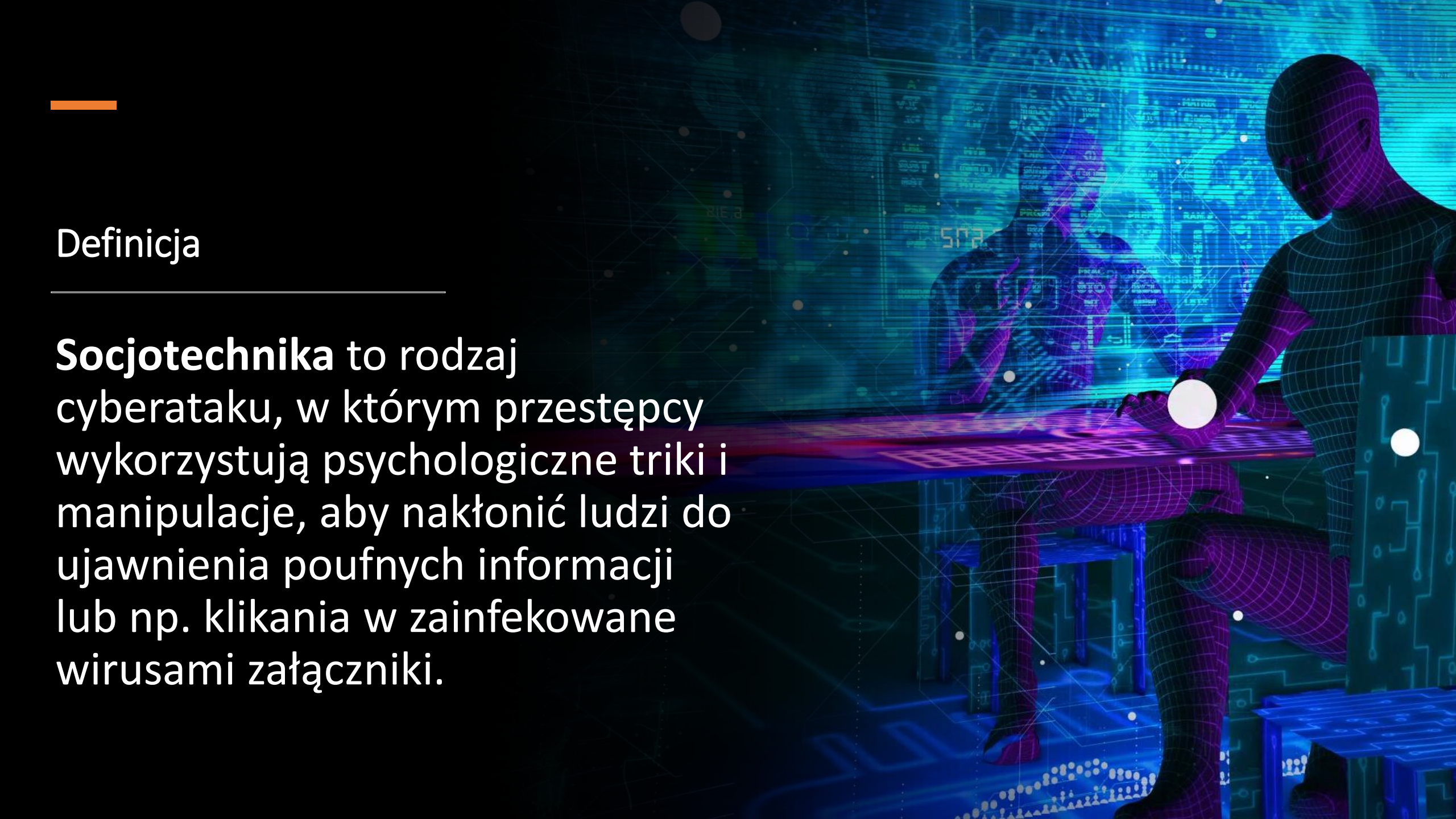
„Łamałem ludzi, nie hasła.”

Kevin Mitnick

Nawet 94% skutecznych włamań do sieci cybernetycznych zaczyna się od błędu ludzkiego.

Definicja

Socjotechnika to rodzaj cyberataku, w którym przestępcy wykorzystują psychologiczne triki i manipulacje, aby nakłonić ludzi do ujawnienia poufnych informacji lub np. klikania w zainfekowane wirusami załączniki.



Znaczenie czynnika ludzkiego w cyberbezpieczeństwie

- Błędy ludzkie jako główna przyczyna włamań
- Socjotechnika
- Znaczenie świadomości i edukacji
- Psychologiczne mechanizmy wykorzystywane w atakach
- Kultura organizacyjna wspierająca cyberbezpieczeństwo

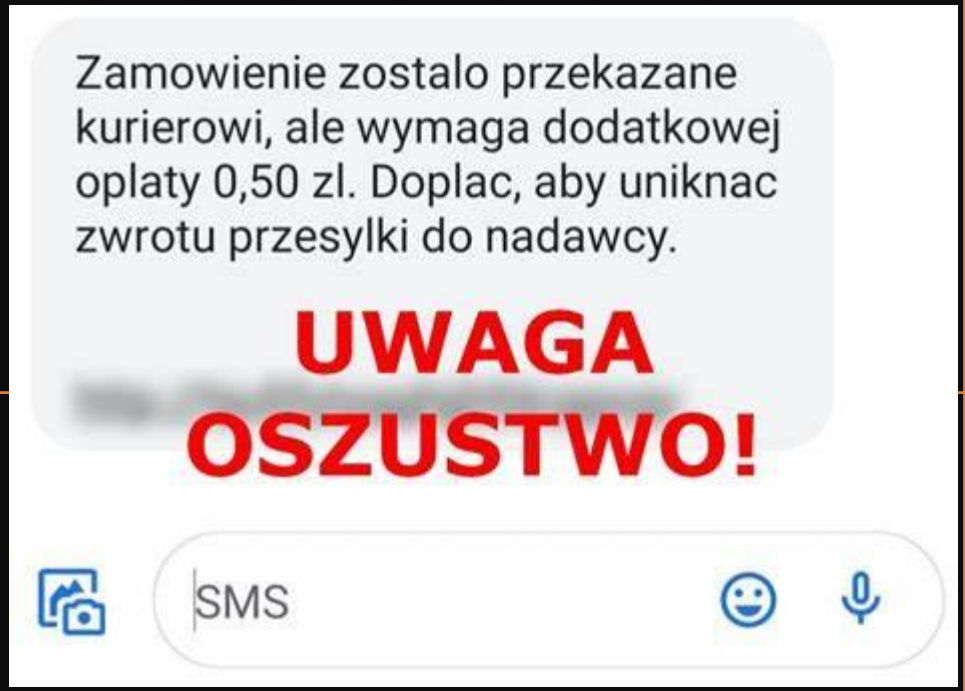
Rodzaje ataków socjotechnicznych

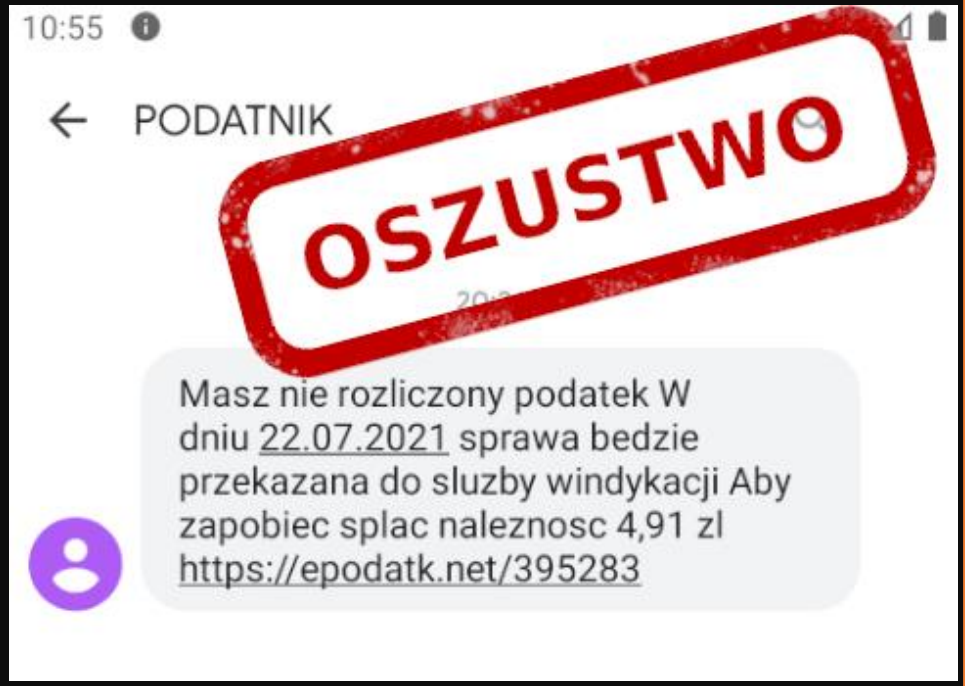
Phishing

Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS (smishing).

Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami.

Phishing oparty jest o metody manipulacji użytkownikiem systemu bez próby forsowania technicznych zabezpieczeń.



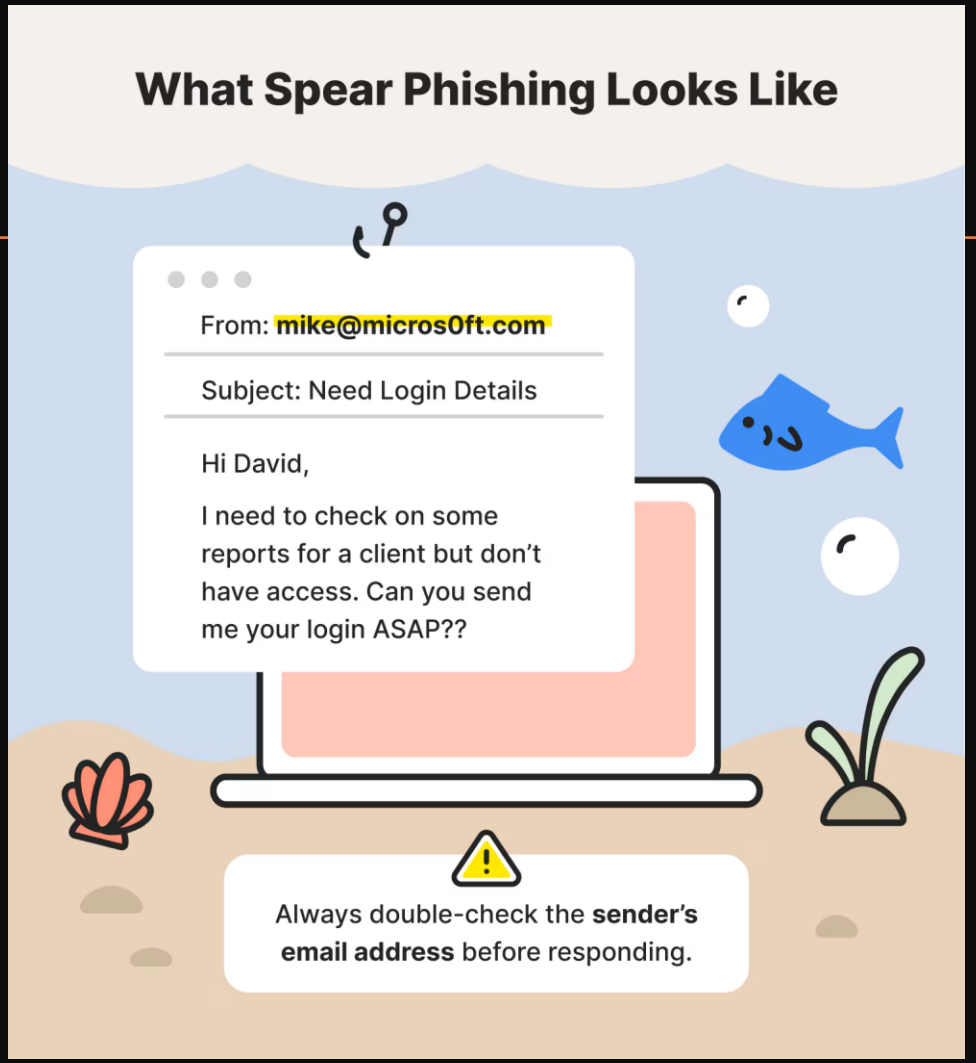


Spear phishing

Atak typu spear phishing jest bardziej wysublimowaną formą phishingu.

Przestępcy przed jego przeprowadzeniem wykonują wnikliwą pracę wywiadowczą, by uzyskać jak najwięcej informacji o osobie lub grupie osób będących celem oszustwa.

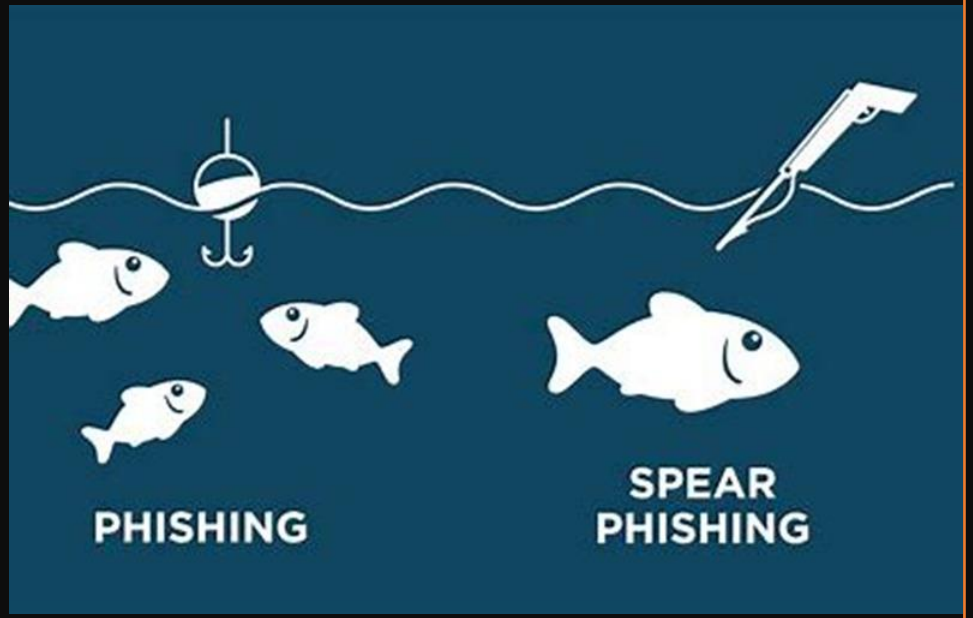
Oszuści podszywają się pod konkretne osoby lub organizacje, które ofiara zna i którym ufa, wysyłają do niej fałszywe wiadomości, często zawierające informacje z życia prywatnego celem zwiększenia ich wiarygodności.



Phishing vs Spear phishing

Phishing bazuje na bardzo dużej ilości wysyłanych wiadomości lub intensyfikacji innych form dotarcia. Oszuści kontaktują się z tysiącami przypadkowych osób, nie czyniąc w zasadzie żadnych, dodatkowych starań w celu zwiększenia skuteczności, bo sama skala działania przynosi dla nich oczekiwane efekty.

W przeciwieństwie do tradycyjnej formy phishingu **spear phishing** jest zdecydowanie bardziej skuteczny. Wymaga od oszustów większego zaangażowania, a także niemal bezpośredniego kontaktu z ofiarą, jednak dobrze przygotowany atak może zmylić nawet najbardziej świadomego zagrożeń użytkownika sieci.



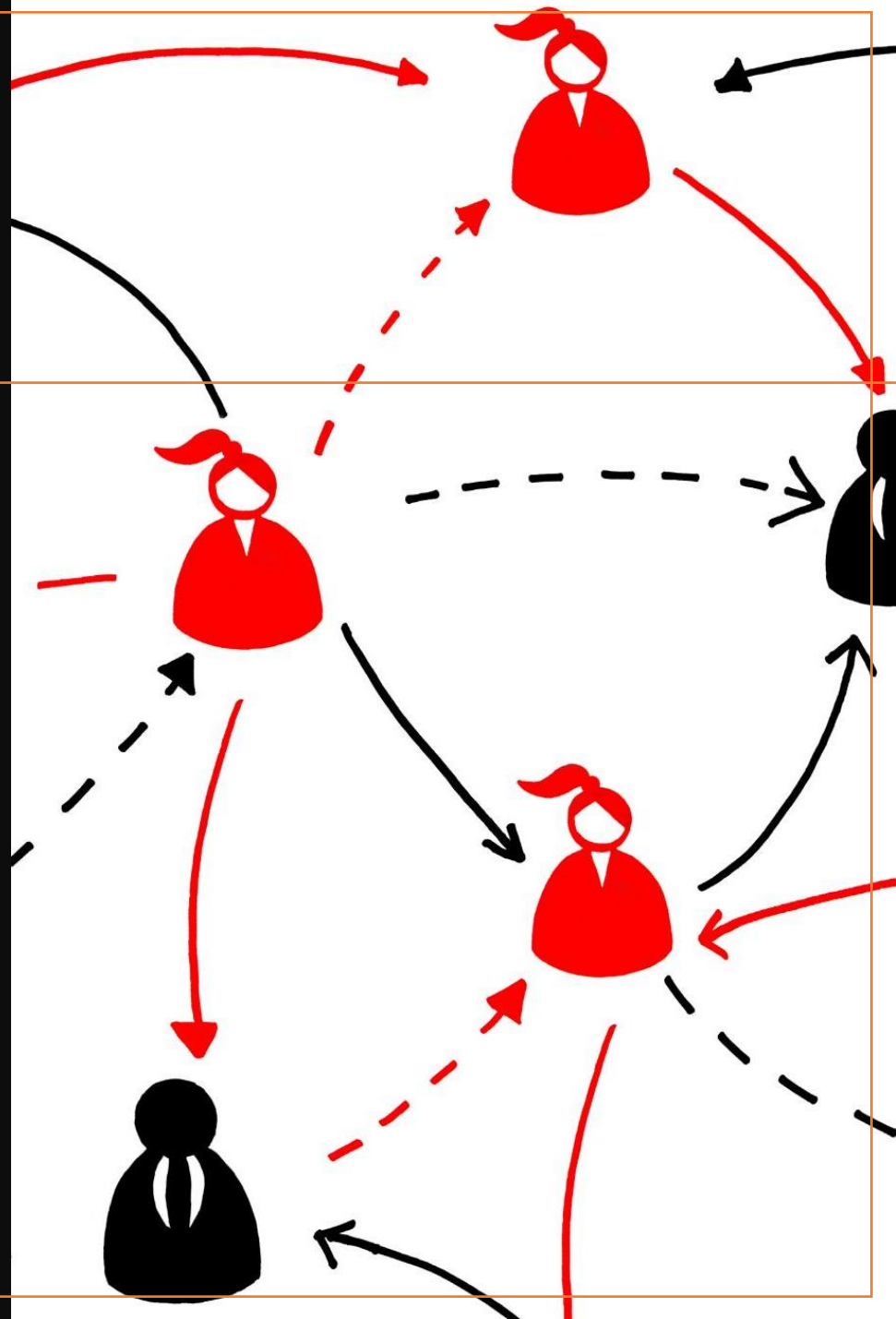
Whaling phishing

Whaling phishing, znany również jako **whaling**, to zaawansowana forma phishingu, która celuje w wysokiej rangi przedstawicieli organizacji, takich jak dyrektorzy generalni (CEO), dyrektorzy finansowi (CFO) i inni członkowie zarządu.

Znany też jako BEC (Business Email Compromise). Nie należą one do rzadkości, a wyłudzone kwoty bywają olbrzymie. W sierpniu 2015 r. firma Ubiquiti Networks, amerykański producent sprzętu sieciowego, straciła w ten sposób ponad 46 mln dolarów.

Pretexting (podszywanie się)

Preteksting, czyli scenariusz zgrozy, ma miejsce, gdy cyberprzestępca tworzy fałszywy scenariusz, aby nakłonić ludzi do ujawnienia poufnych informacji. Na przykład atak pretekstingowy może polegać na tym, że atakujący podszywa się pod wsparcie IT firmy i prosi o dane logowania w celu rozwiązania problemu.



Baiting (przynęta)

- Osoba jest uwodzona przez zwodniczą obietnicę, która przemawia do jej ciekawości lub chciwości.
- Przynęta polega na tym, że atakujący np. pozostawia w lobby lub na parkingu pamięć USB ze szkodliwymi plikami w nadziei, że ktoś z ciekawości włoży ją do urządzenia, a wtedy złośliwe oprogramowanie, które zawiera, może zostać wdrożone.
- W cyberataku typu baiting, napastnik może wysłać do skrzynki odbiorczej ofiary wiadomość e-mail zawierającą załącznik ze złośliwym plikiem. Po otwarciu załącznika instaluje się on na komputerze użytkownika i szpieguje jego aktywność.

Tailgating (podążanie za kimś)

- **Tailgating** to forma ataku socjotechnicznego, która umożliwia złodziejom, hakerom i innym złośliwym podmiotom wejście i nieautoryzowany dostęp do nieograniczonego regionu.

- Dlatego też, w przeciwieństwie do innych cyberataków online, które polegają na cyfrowym włamaniu do sieci firmowej, atakujący fizycznie narusza system bezpieczeństwa firmy, aby przesyłać strumieniowo, uzyskiwać dostęp i narażać na szwank jej poufne dane.

Vishing (oszustwa głosowe)

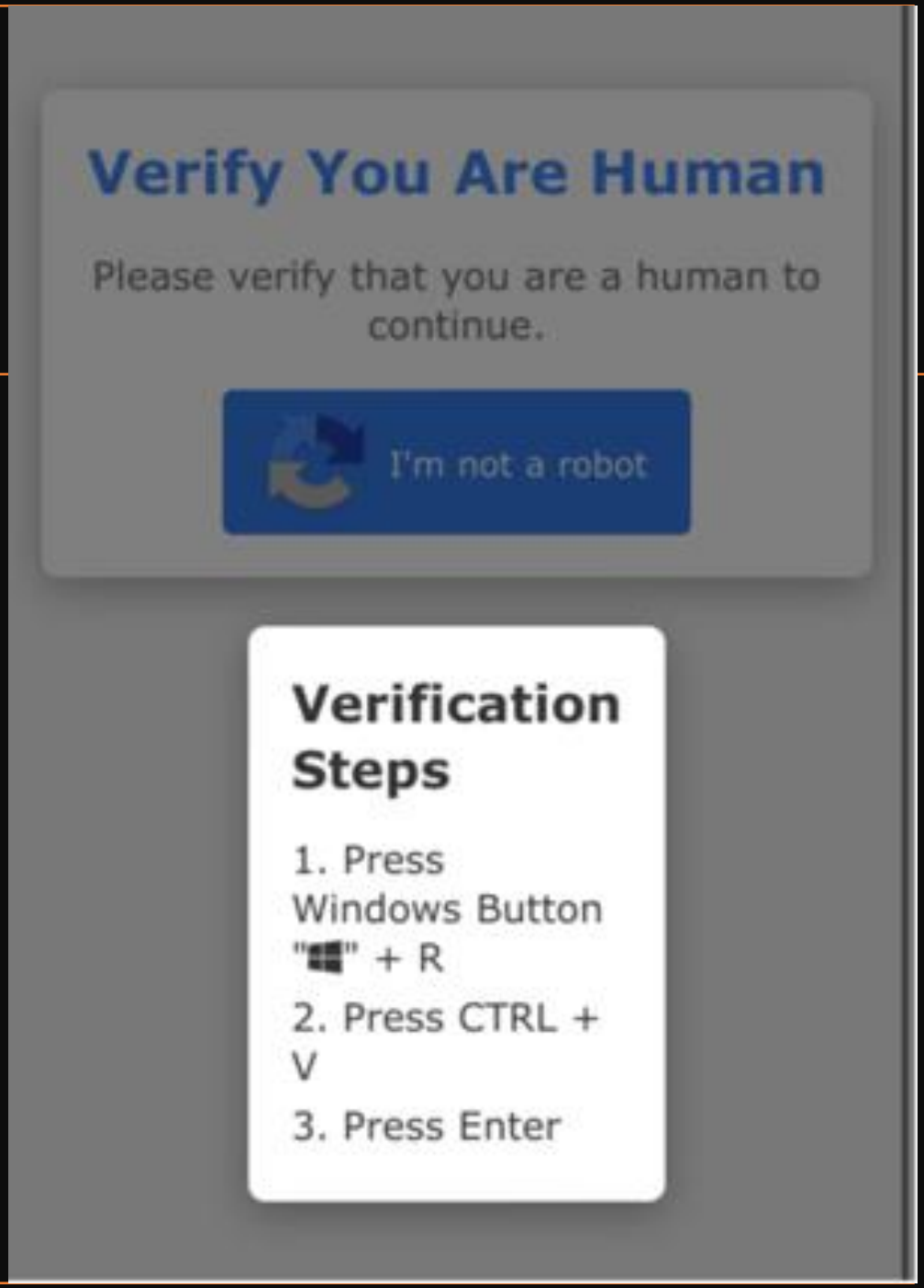
- Vishing w swej istocie sprowadza się do wyłudzenia danych (ang. phishing), ale konkretnie poprzez rozmowę telefoniczną.
- Polega to na tym, że dzwoniący podaje się za pracownika naszego banku, doradcę inwestycyjnego, instytucję zaufania publicznego czy inny podmiot dla nas istotny i prowadzi rozmowę w taki sposób, że ofiara ujawnia swoje szczegółowe dane.
- W międzyczasie albo chwilę po rozmowie telefonicznej (w zależności od zręczności złodzieja) konto ofiary zostaje opróżnione, a bardzo często także obciążone kredytem na wiele tysięcy złotych.

Impersonation

- Jedną z najczęstszych technik stosowanych w inżynierii społecznej jest podszywanie się pod znane osoby lub marki.
- Osoby atakujące często podszywają się pod kogoś innego, aby uzyskać dostęp do poufnych informacji lub systemów.

Pastejacking

Pastejacking to metoda wykorzystywana przez złośliwe witryny do przejęcia kontroli nad schowkiem komputera i zmiany jego zawartości na coś szkodliwego bez Twojej wiedzy.



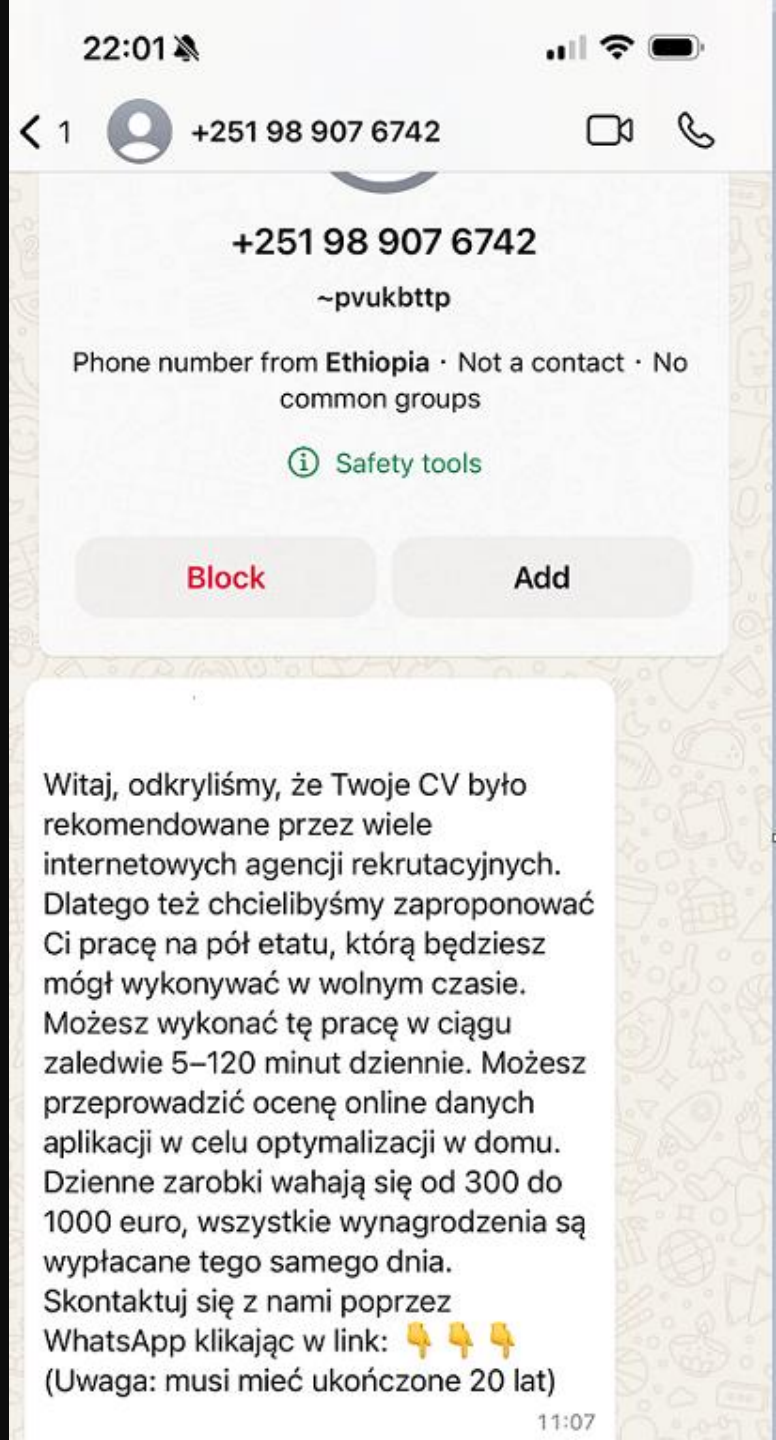
Spoofing

-)
- Pracownik banku podczas rozmowy telefonicznej prosi Cię o weryfikację danych?
- A może dostawca energii dzwoni, aby poinformować o rosnącym zadłużeniu na koncie?
- **Wymienione wyżej sytuacje stanowią przykład spoofingu.**
- Oszustwo polega na podszywaniu się przez przestępcę pod pracowników różnego rodzaju instytucji, w celu wyłudzenia informacji lub skłonienia ofiary do zainstalowania szkodliwego oprogramowania.

Psychologia socjotechniki

Wykorzystywane mechanizmy psychologiczne

- Autorytet
- Pilność/presja czasu
- Strach
- Ciekawość
- Empatia



Wpływ socjotechniki na osoby indywidualne i organizacje

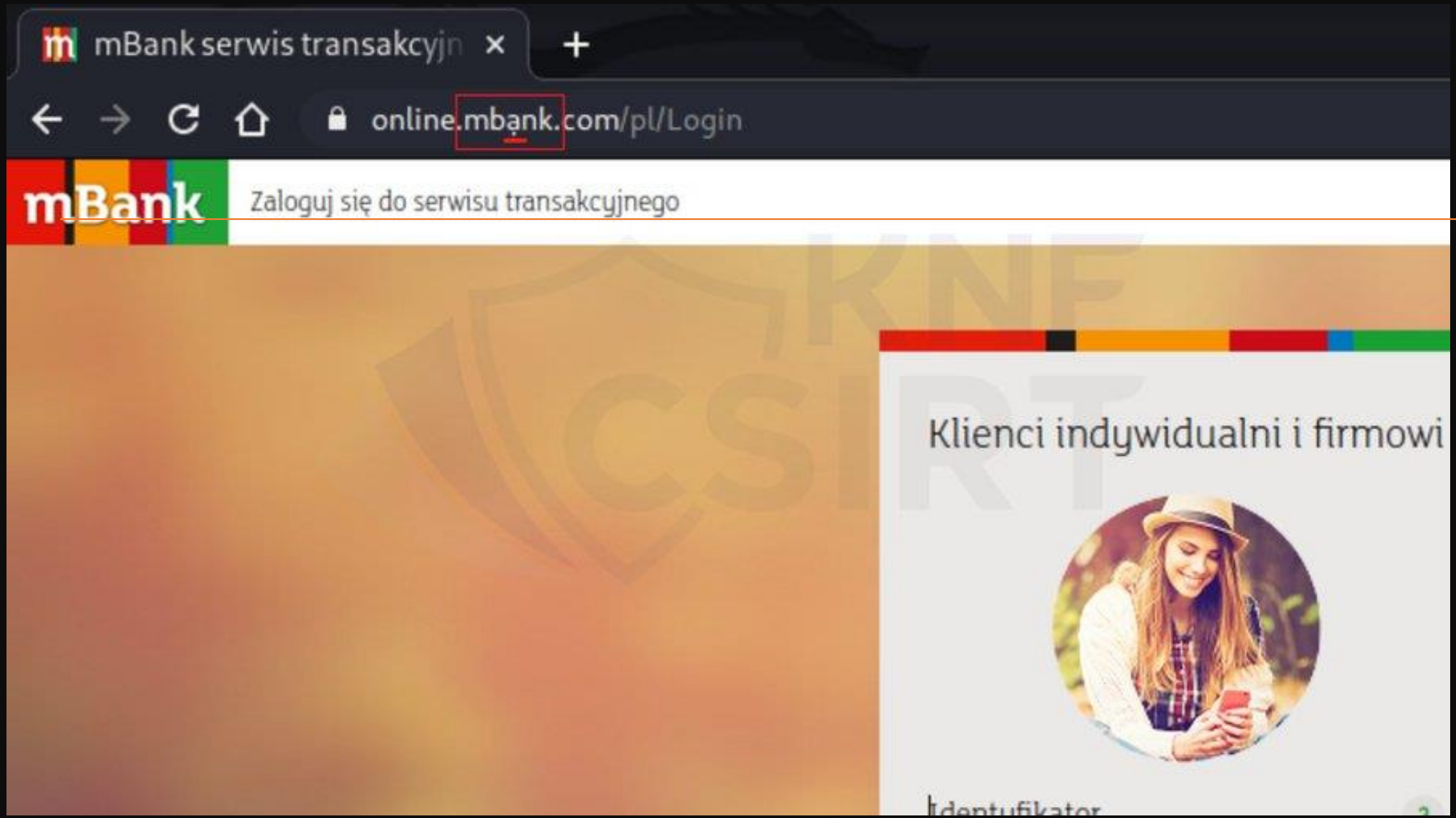
- Ataki socjotechniczne mogą mieć poważne konsekwencje, w tym straty finansowe, kradzież tożsamości, utratę reputacji i inne.
- Mogą one mieć wpływ zarówno na osoby prywatne, jak i organizacje.

AI – wróg czy przyjaciel

AI – wróg czy przyjaciel

Przykłady skutecznych kampanii socjotechnicznych

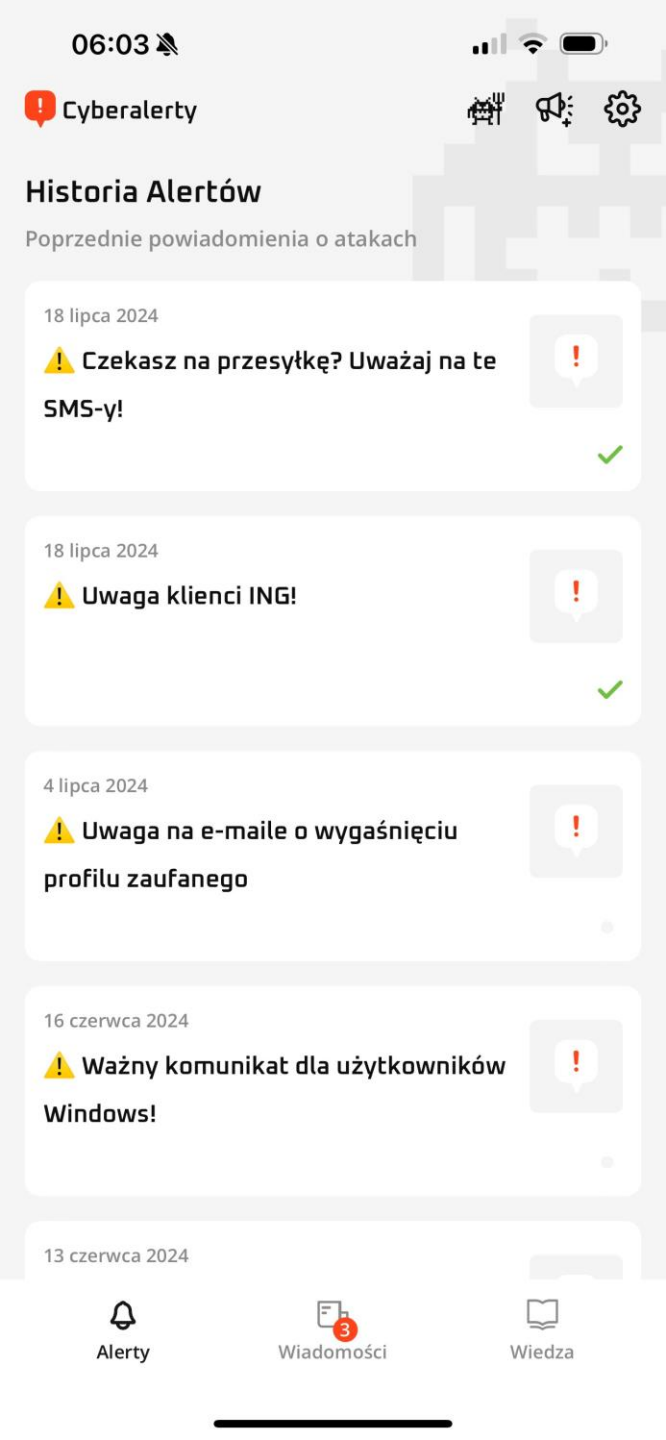
- Atak na Twittera w 2020 roku - podszywanie się pod pracowników
- Oszustwo CEO Fraud - wyłudzenie 47 milionów dolarów od Ubiquiti Networks
- RSA Security Hack - atak phishingowy prowadzący do naruszenia bezpieczeństwa


mBank serwis transakcyjn
online.mbank.com/pl/Login
mBank
Zaloguj się do serwisu transakcyjnego
Klienci indywidualni i firmowi
Identyfikator

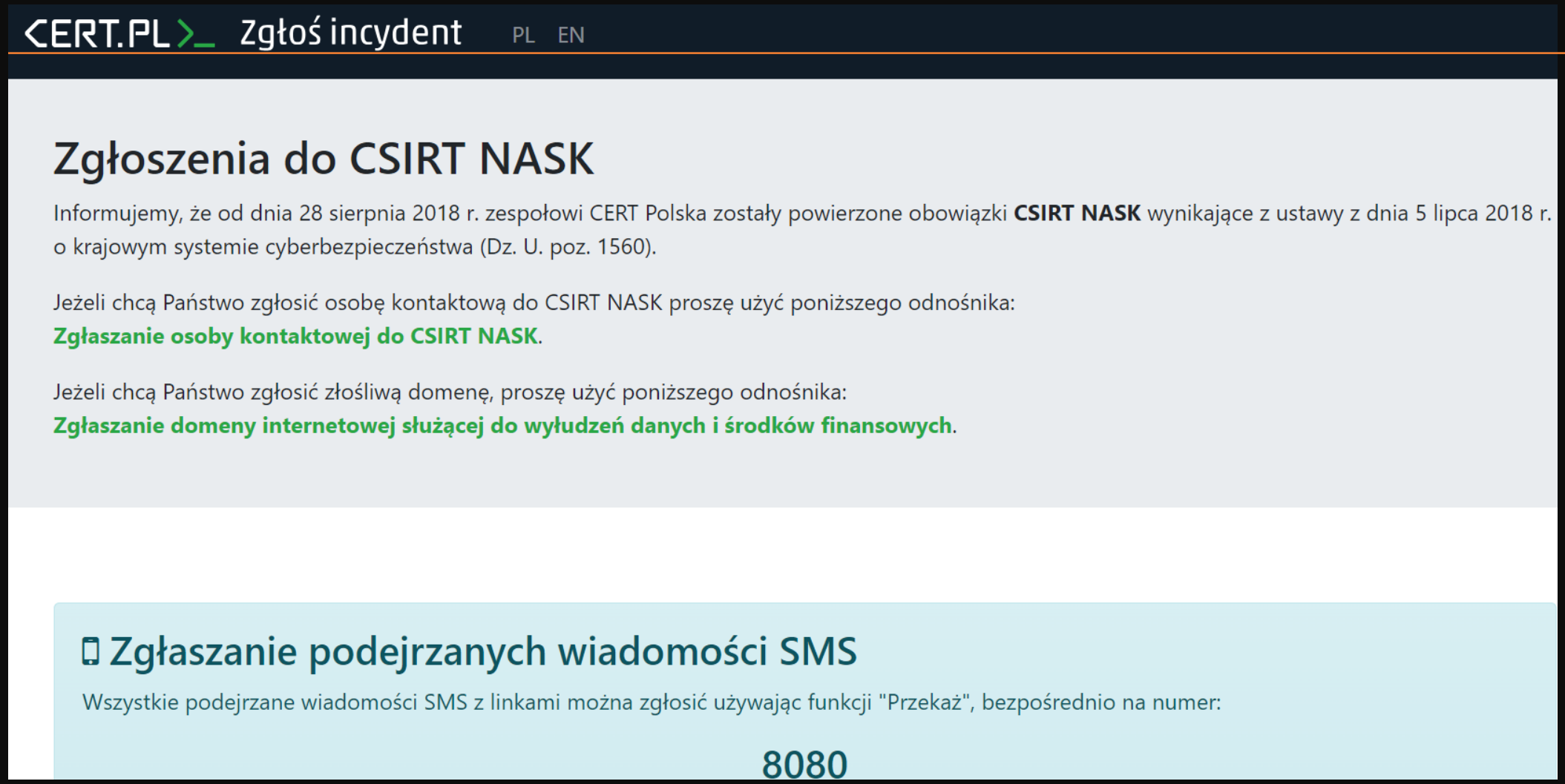
Obrona przed atakami socjotechnicznymi

Obrona przed inżynierią społeczną

- Świadomość i technologia
- Zabezpieczanie danych osobowych
- Skuteczne szkolenie w zakresie świadomości bezpieczeństwa
- Edukacja i szkolenia pracowników
- Implementacja polityk bezpieczeństwa
- Narzędzia techniczne (filtry antyspamowe, uwierzytelnianie dwuskładnikowe)
- Kultura organizacyjna wspierająca cyberbezpieczeństwo

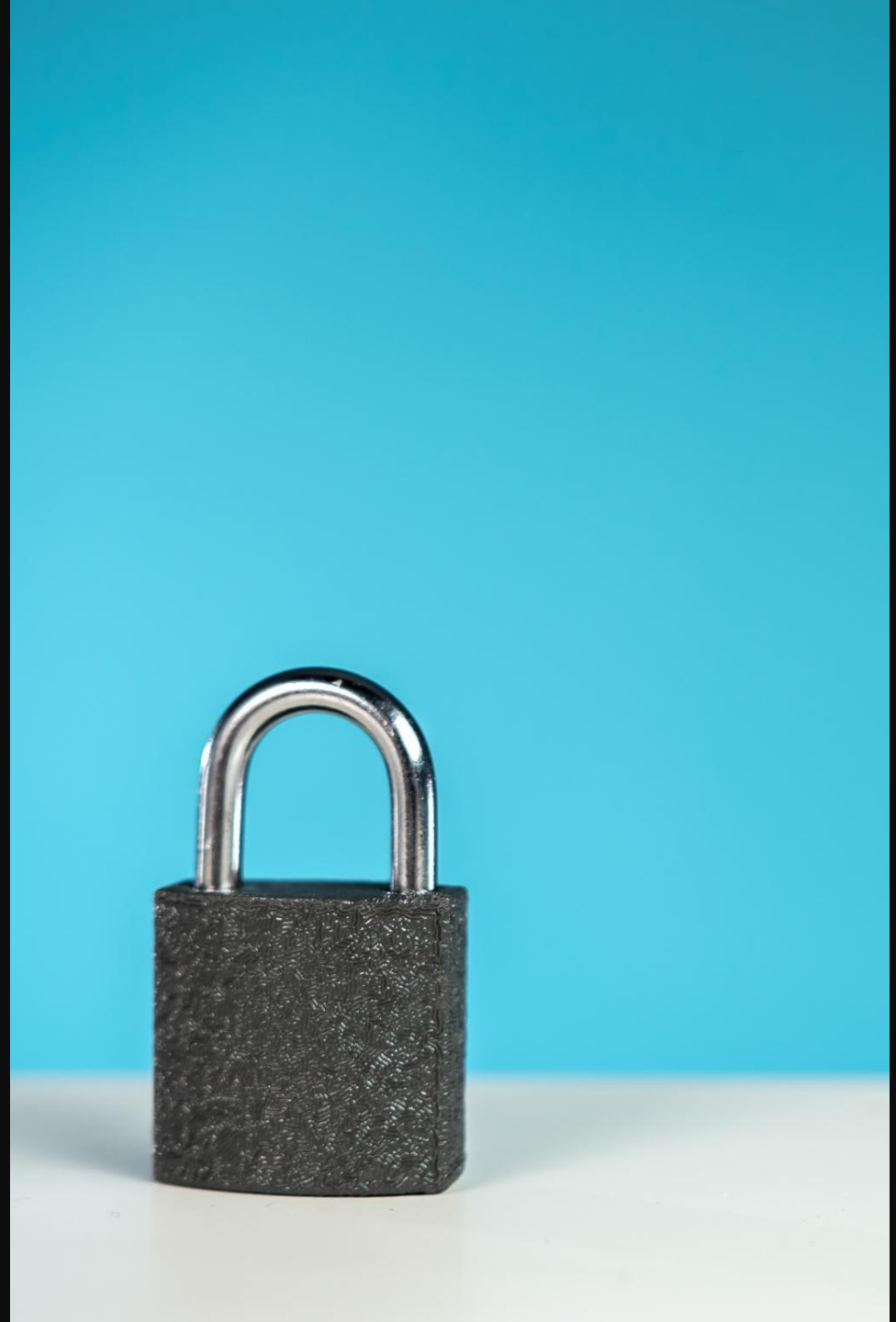


Obrona przed inżynierią społeczną



Sprawdzone metody zabezpieczania danych osobowych

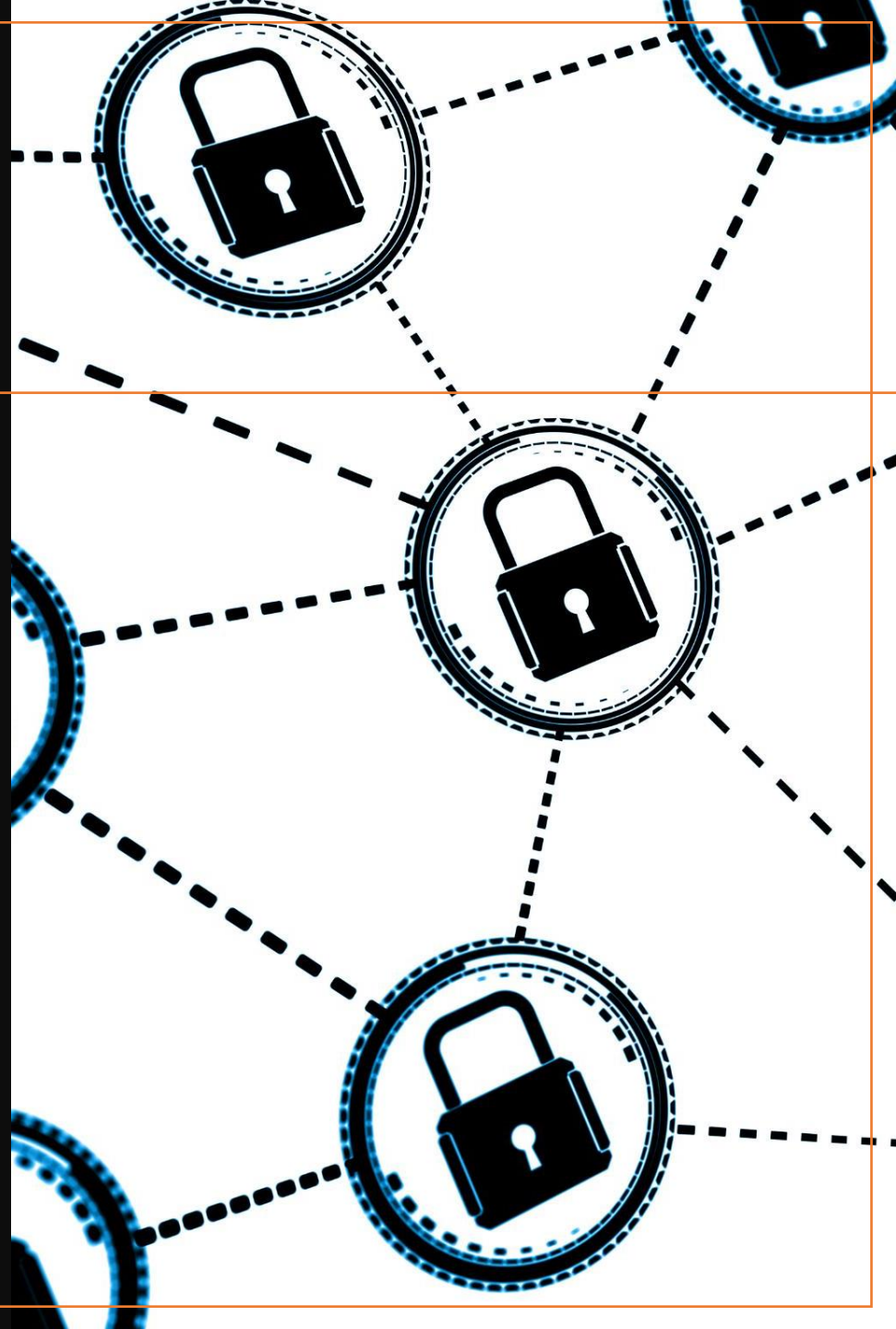
- Silne hasła
- Zapobieganie publicznym sieciom Wi-Fi
- Bycie uważnym online
- Używanie manadżerów haseł



Podsumowanie i dodatkowe zasoby

Wnioski

Ataki Social Engineering stanowią poważne zagrożenie dla jednostek i organizacji. Jednak poprzez zrozumienie zagrożenia, prawidłowe szkolenie i zachowanie ostrożności w udostępnianiu informacji, można skutecznie zabezpieczyć się przed atakami tego typu.



Bibliografia

https://centuria.pl/blog/ataki-hakerskie-oparte-o-socjotechnike-czyli-czlowiek-jako-najslabsze-ogniwo-cyberbezpieczenstwa/

https://vestigio.agency/pl/blog/spoofing-co-to/

https://www.realornotquiz.com/

Discord: server 17 53c, NTHW (Not The Hidden Wiki)

https://incydent.cert.pl/

https://niebezpiecznik.pl/

https://zaufanatrzeciastrona.pl/

https://sekurak.pl/

https://www.youtube.com/watch?v=Jr8yEgu7sHU

@pidak.ai – profil na FB (Projektant graficzny)
https://www.facebook.com/profile.php?id=61565008707818

- **Email**: info@zalnet.pl
- **Twitter**: beatazalewa
- **Github**: beatazalewa
- **LinkedIn:** beatazalewa
- **Blog**: beatazalewa.com