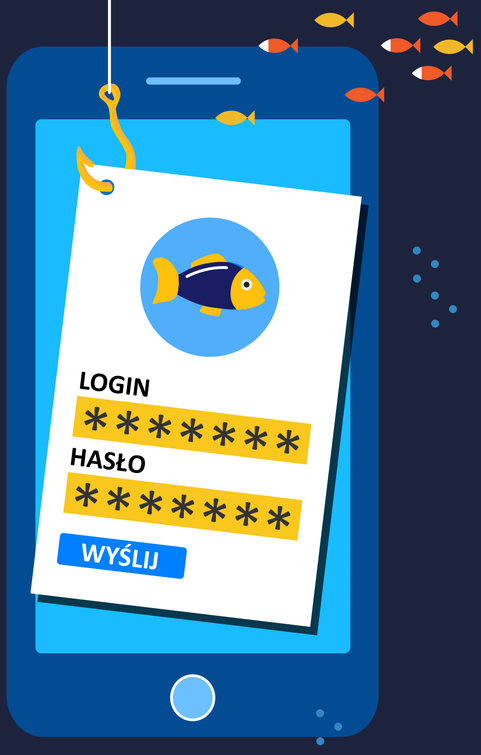
ZAGROŻENIA W SIECI

SPÓJRZ DWA RAZY, ZANIM KLIKNIESZ

Możesz stracić swoje pieniądze, dane osobowe, a nawet osobiste pliki, jeśli urządzenie przestanie funkcjonować. Nie daj się usidlić!



JAK TO SIĘ MOGŁO STAĆ?

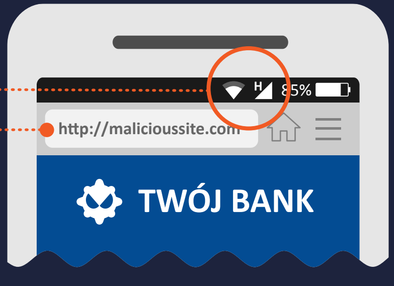
Ataki metodą phishing: Służą do oszukiwania użytkowników poprzez imitowanie wiarygodnych organizacji i wyłudzanie w ten sposób danych osobowych. Są one rozsyłane pocztą e-mail, w wiadomościach SMS oraz poprzez komunikatory mediów społecznościowych.

Przeglądanie stron internetowych: Do zainfekowania urządzenia mobilnego może dojść poprzez zwykłe przeglądanie stron internetowych.

Pobieranie plików: Szkodliwe linki i załączniki mogą zostać dołączone bezpośrednio do wiadomości e-mail.

DLACZEGO JEST TO SKUTECZNE?

Urządzenia mobilne są **stale podłączone** do Internetu.



Mniejszy rozmiar ekranu w urządzeniu mobilnym stanowi często utrudnienie w obsłudze. Przeglądarki w urządzeniach mobilnych wyświetlają adresy URL na ograniczonej przestrzeni, wskutek czego sprawdzenie, czy dana domena jest prawdziwa, stwarza trudności.

Domyślny użytkownik wierzy w osobisty charakter urządzenia mobilnego.

CO MOGĘ ZROBIĆ?

Uważaj na SMS-y i telefony od firmy, która prosi o ujawnienie danych osobowych. Aby sprawdzić, czy dana wiadomość/telefon jest prawdziwa, możesz zadzwonić bezpośrednio do firmy na jej oficjalny numer telefonu.

https://

Używaj zabezpieczonego połączenia HTTPS podczas przeglądania stron internetowych za pomocą urządzenia mobilnego. Informacja o zabezpieczeniu znajduje się na początku adresu URL.

Nigdy nie klikaj linka lub załącznika znajdującego się w podejrzanej wiadomości e-mail/SMS. Natychmiast usuń taką wiadomość.

^BE:%}
W@RY
*)Z#$=

Zachowaj ostrożność, jeśli tekst na odwiedzanej stronie zawiera błędy gramatyczne, literówki lub odznacza się niską rozdzielczością.

Jeśli to możliwe, zainstaluj aplikację bezpieczeństwa do urządzeń mobilnych, która ostrzeże Cię o podejrzanej aktywności.

EUROPOL EC3 European Cybercrime Centre | POLICJA | NASK | #MobileMalware