Ekonomiczny Uniwersytet Dziecięcy

Jak nie stracić pieniędzy w sieci?

Katarzyna Kubiszewska

Politechnika Gdańska
Data: 27.04.2023


p

Przypadek nr 1

Na lotnisku w Polsce poszkodowany użyczył telefon obcemu mężczyźnie, który wykonał jedno połączenie.

Na koniec miesiąca poszkodowany otrzymał fakturę na 39 tys. zł

Co się stało?

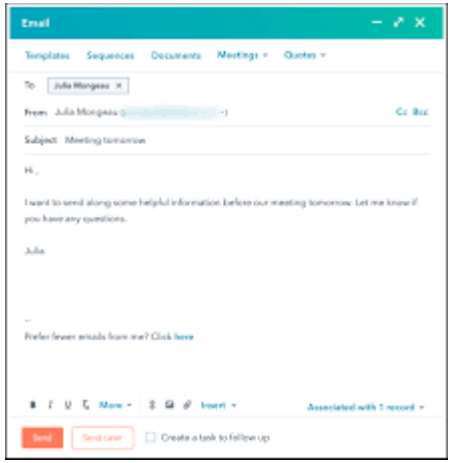
Przypadek nr 2

Poszkodowany otrzymał emaila z informacją o zablokowaniu jego konta bankowego.

W celu odblokowania, musiał zalogować się na rachunek używając przesłanego w mailu linka.

Po kilku dniach okazało się, że wszystkie środki z konta zniknęły, a dodatkowo zaciągnięto kredyty na kwotę 13 600 zł.

Co się stało?



Przypadek nr 3

Poszkodowanemu „skończył” się internet komórkowy. Będąc w centrum handlowym, skorzystał z otwartej sieci udostępnionej przez centrum i wykonał jeden przelew.

Po kilku dniach okazało się, że wszystkie środki z konta zniknęły, a dodatkowo zaciągnięto kredyty na kwotę 9 600 zł.

Co się stało?

Jakie błędy popełniono w każdym z przypadków?

Nr przypadku	*Błędy*
Nr 1	
Nr 2	
Nr 3	

O czym będziemy dziś rozmawiać?

O jakich *przestępstwach w sieci słyszeliście?*

Aby kradzież się powiodła, cyberprzestępca musi zdobyć dane, które umożliwią mu:

Dostęp do naszego konta. Tymi danymi są:

- login,
- hasło.

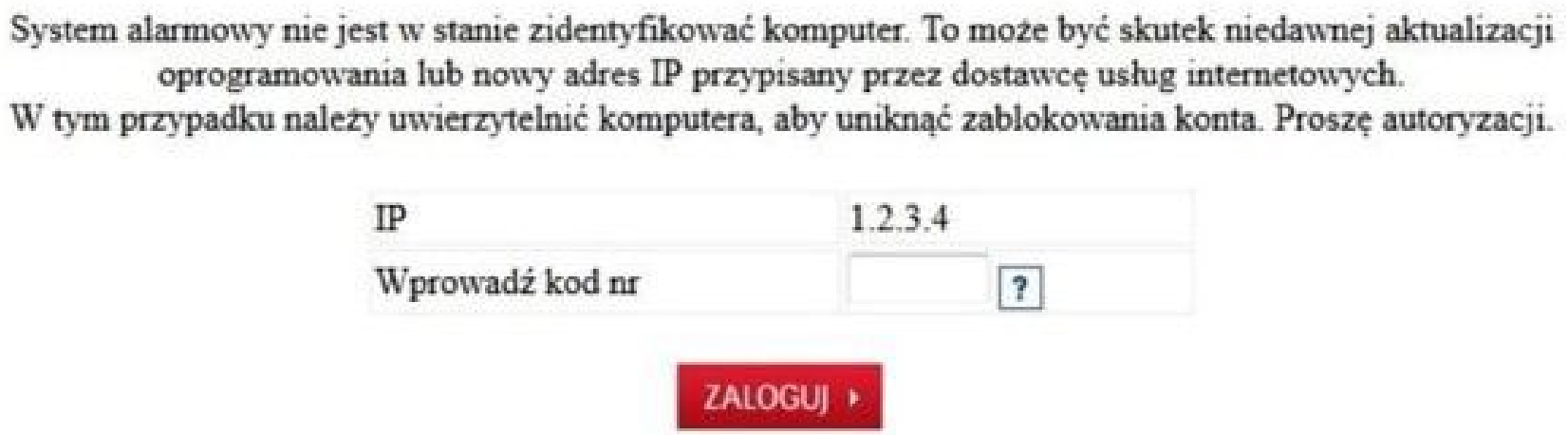
Uzyskanie informacji niezbędnych do przelania środków. W tym celu haker spróbuje od nas pozyskać:

- kody SMS;
- kody zdrapki (coraz rzadziej używane);
- numer i rodzaj telefonu wraz z oprogramowaniem (np. wersja systemu Android).

Jak cyberprzestępca może wyłudzić dane?

PHISHING, czyli próba wyłudzenia danych

„Proszę autoryzacji” czyli o fatalnej polszczyźnie


System alarmowy nie jest w stanie zidentyfikować komputer. To może być skutek niedawnej aktualizacji oprogramowania lub nowy adres IP przypisany przez dostawcę usług internetowych.
W tym przypadku należy uwierzytelnić komputera, aby uniknąć zablokowania konta. Proszę autoryzacji.

IP	1.2.3.4
Wprowadź kod nr	?

ZALOGUJ

Źródło: strona PKO BP, www.pkobp.pl/bankowosc-elektroniczna/ipko/bezpieczna-bankowosc/uwaga-na-nowe-zagrozenia-w-sieci/.

Ale polszyzna się poprawia.....

Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane ×

mBank przez s7.jupe.pl 14:15 (7 minut temu)

do mnie

Szanowny kliencie,

mBank

Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

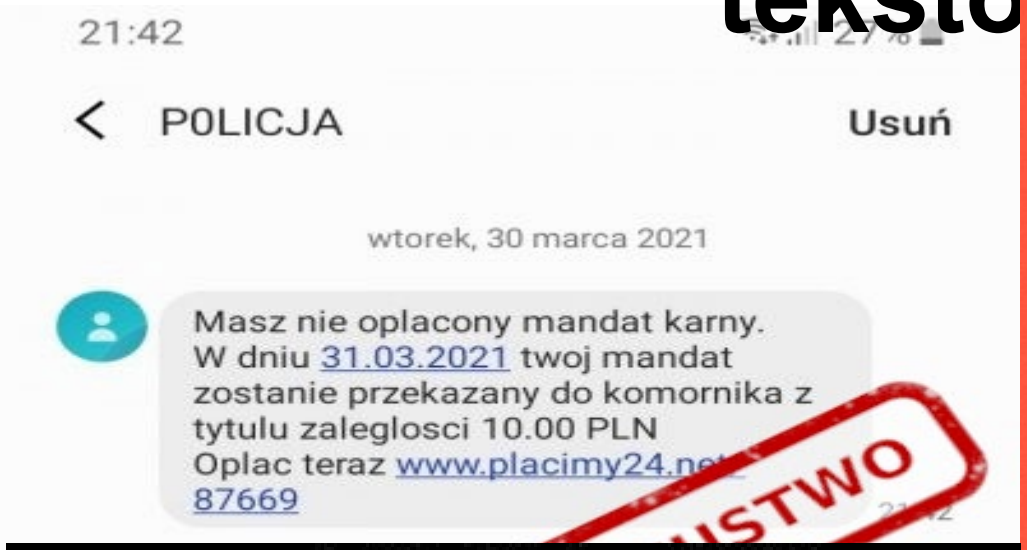
Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.

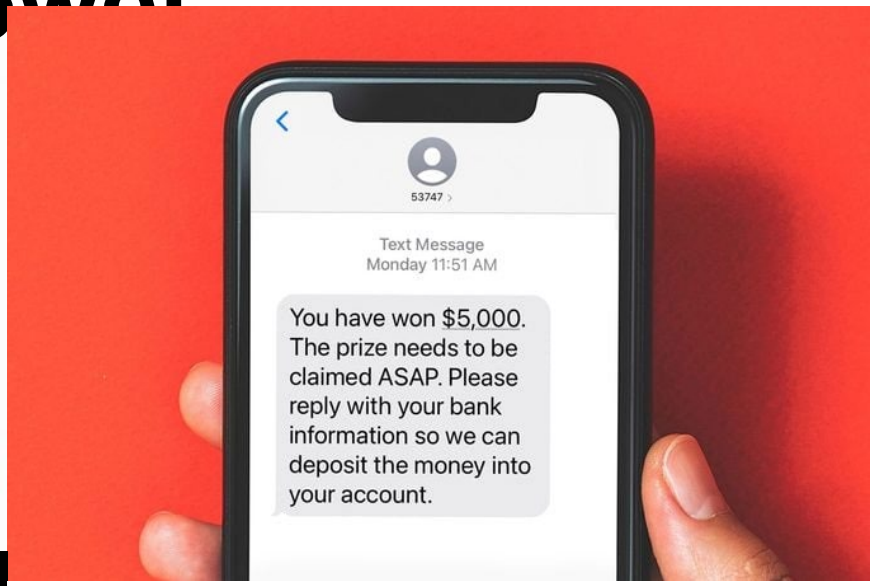
Pozdrawiamy,
Zespół mBanku

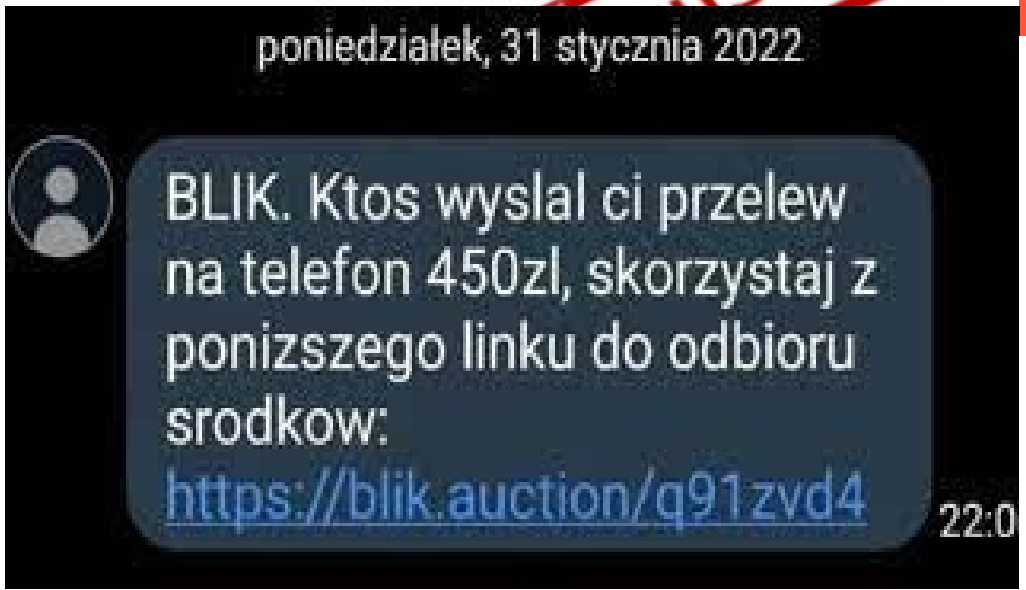
mBank S.A. z siedzibą w Warszawie przy ul. Senatorskiej 18, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość wg stanu na dzień 01.01.2013 r. wynosi 168.555.904 złotych.

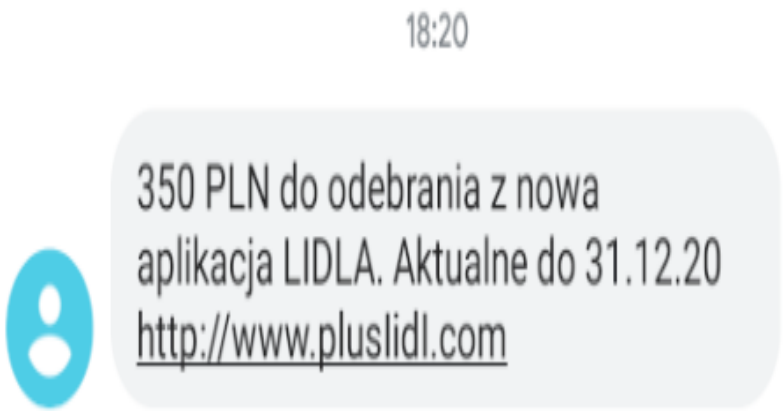
Źródło: strona Bankier.pl, www.bankier.pl/wiadomosc/Zlodzieje-znow-podszywaja-sie-pod-mBank-3285634.html

SMISHING, czyli wyłudzanie danych za pomocą wiadomości tekstowej





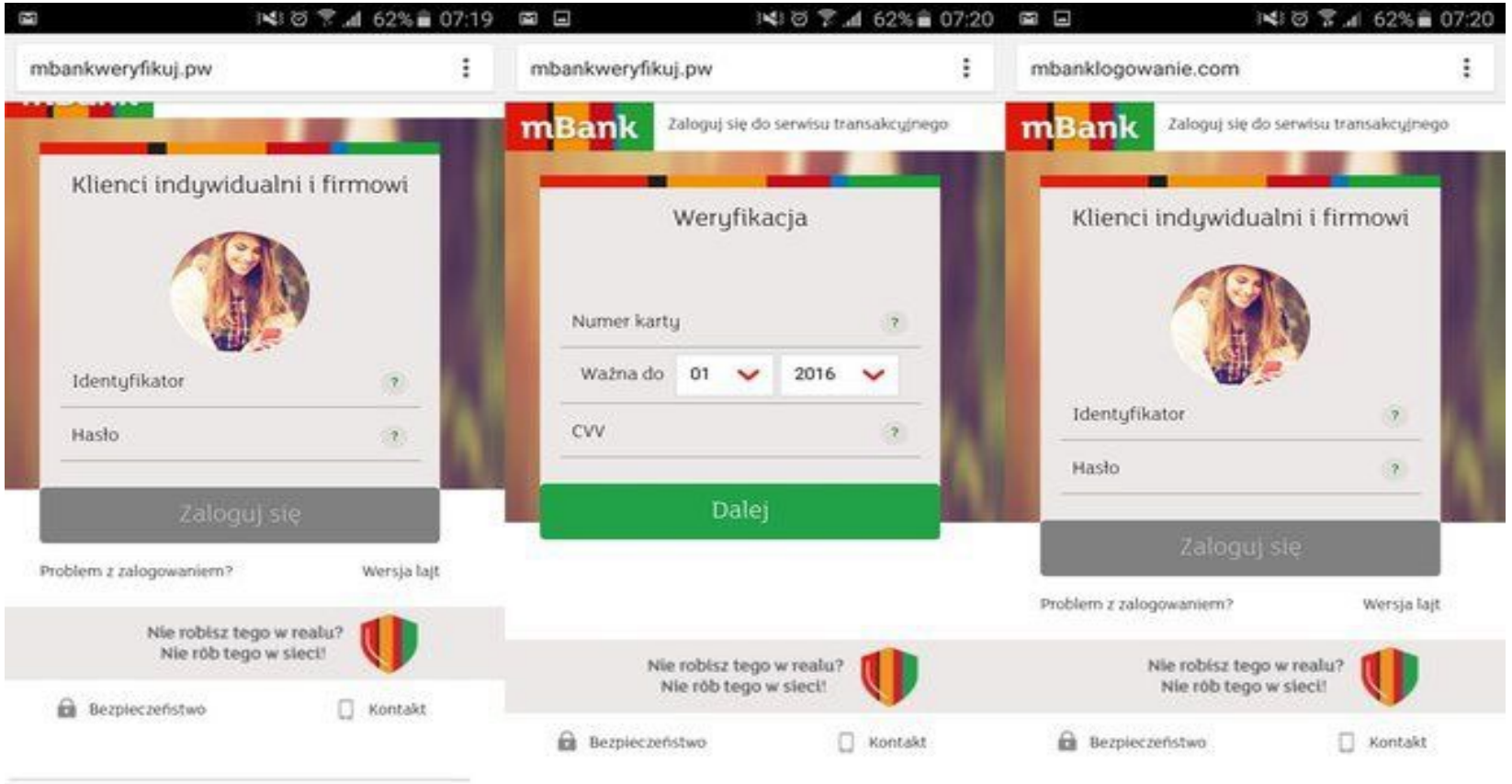




Niemiłe skutki miłej rozmowy - VISHING

Spróbujcie przeprowadzić taką rozmowę?

Strona banku: autentyczna czy fałszywa?



Źródło: strona Bankier.pl, www.bankier.pl/wiadomosc/Do-trzech-razy-sztuka-Znowu-phishing-wycelowany-w-mBank-7340502.html

online.mbank.pl/pl/Login

Crossref Metadata... | polityka kulturalna... | Serbia GDP per cap... | Interest rate spread... | Bosnia and Herceg... | Internetowy Podręc... | Statystyka opisowa...

Link do głównej | Zaloguj się do serwisu transakcyjnego

Klienci indywidualni i firmowi

Identyfikator

Hasło

Zaloguj się

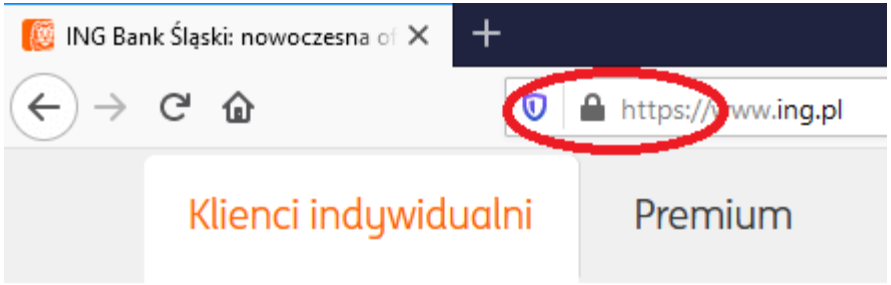
Odblokuj dostęp | Problem z zalogowaniem?

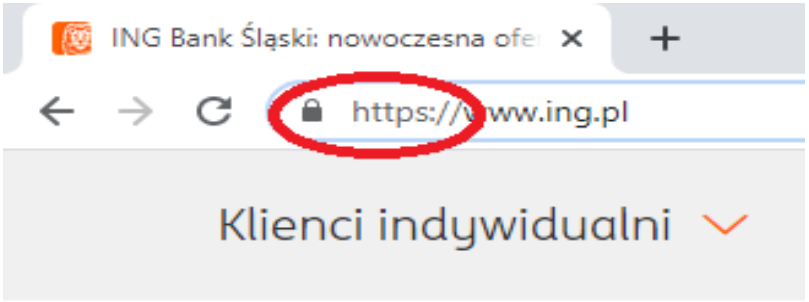
Private Banking

CompanyNet

Sprawdź, jak chronić się przed cyberprzestępcami. Nowe informacje!

Symbol kłódki i protokół https:// w adresie strony





ING

ING

Trojany czyli wirusy

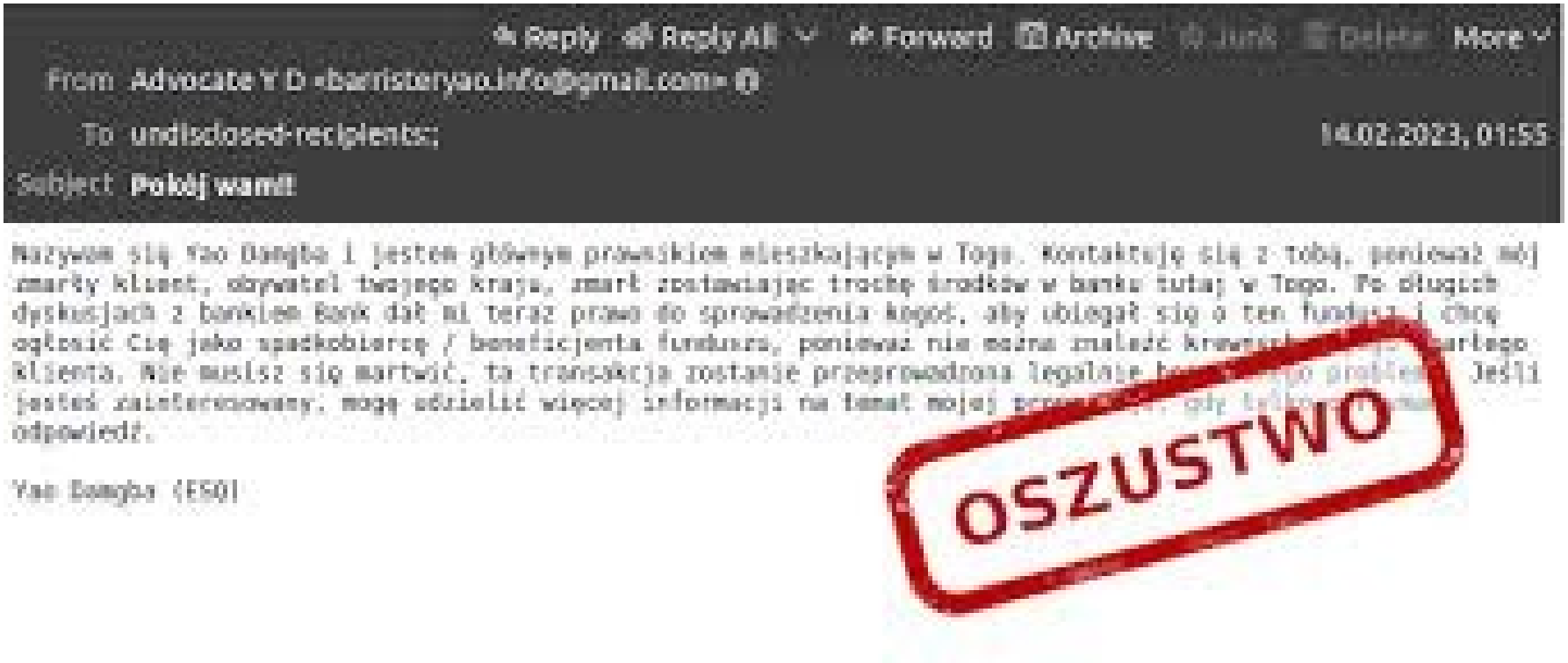
Trojan wysyła drogie SMS-y

Trojan szpiegujący

Trojan podmienia numer konta

Trojan podmienia stronę banku

Oszustwo nigeryjskie



NIE DAJ SIĘ NABRAĆ

"NA WNUCZKA" I "NA POLICJANTA"

JAK DZIAŁAJĄ OSZUŚCI?

1. Dzwoni telefon, podnosisz słuchawkę
2. Osoba, z którą rozmawiasz przekonuje, że jest Twoim wnuczkiem, krewnym, jego znajomym lub inną bliską osobą z Twojej rodziny
3. Osoba ta informuje, że pilnie potrzebuje pieniędzy

4. Telefon dzwoni ponownie. Osoba informuje, że jest policjantem i przekonuje, że przed chwilą dzwonił oszust, a Ty musisz pomóc go zatrzymać
5. Zostajesz poinformowany, że potrzebne są pieniądze, które masz przekazać nieznanej Ci osobie. Pamiętaj, Policja nigdy nie prosi o przekazanie pieniędzy i nigdy nie dzwoni z takim żądaniem

Inne oszustwa

oszustwo na OLX,
oszustwo na BLIK,
oszustwo na paczkę,
oszustwo na Facebook,
oszustwo na Booking,
oszustwo na Bitcoina,
oszustwo na PGE SMS,

Co zrobić gdy padliśmy ofiarą oszusta w sieci?

Co zrobić gdy padliśmy ofiarą oszusta w sieci?

Krok 1- zawiadomienie policji

Krok 2 – reklamacja do banku

Krok 3 – raport BIK

Krok 4 – można skontaktować się z prawnikiem, z pytaniem, czy pozew przeciwko bankowi jest zasadny

Zasady bezpiecznego korzystania z sieci

OD NIEBEZPIECZNEGO ZAŁĄCZNIKA DO UTRATY PIENIĘDZY


MEMYTUTAJ.PL
MILK
DZIĘKUJĘ ZA UWAGĘ