KOŁO RATUNKOWE DLA FINANSÓW OSOBISTYCH

Z Ł O T A S Z K O Ł A N B P

OSZUSTWA FINANSOWE

Bzdury!
Mnie to nie dotyczy!
Nie znam nikogo, komu by się to przytrafiło!

Najczęściej słyszymy takie odpowiedzi gdy zaczynamy mówić o oszustwach finansowych.

Niestety, to nie fikcja, codziennie zwykły Kowalski spotyka się z atakami socjotechnicznymi ze strony cyberprzestępców,

z licznymi atakami oszustw.

Sny o łatwym zysku, kończą się najczęściej koszmarami

Obietnica wysokiego i bezpiecznego zysku w krótkim czasie,

po mistrzowsku budowane poczucie uczestniczenia w wyjątkowej inwestycji,

to pułapka.

Przekręty finansowe występują najczęściej w sytuacjach kryzysowych. Korzystają z gorszej kondycji gospodarczej kraju, większego stopnia bezrobocia, inflacji, czy też chęci szybkich, wysokich zysków.

Do tego podawane są w przystępnej formie łatwego biznesu –

wystarczy zainwestować

i czekać na zyski

Oszustwa opierają się na dwóch odmianach:

Piramida finansowa polega na tym, że każdy kolejny poziom piramidy czerpie profity bezpośrednio z pozyskanych przez siebie niższych szczebli układu, przekazując wyżej (twórcy przekrętu) procent od uzyskanych zysków.

Schemat Ponziego charakteryzuje się tym, że wszystkie pozyskane w przekręcie pieniądze trafiają do twórcy przekrętu (na górę), a on uznaniowo wypłaca osobom na niższych szczeblach pewien procent od zgromadzonego zysku

Zarówno piramida, jak i oszustwa finansowe, funkcjonuje wyłącznie w czasie, w którym jest stały dopływ nowych (naiwnych) członków. Jeśli jest więcej wpłacających niż pobierających – machina działa.

Pozyskiwanie środków w takiej proporcji nie ma racji bytu w dłuższej perspektywie – zarówno piramida finansowa jak i schemat Ponziego są z góry skazane na porażkę, a zainwestowane tam pieniądze, na stratę.

Mechanizm

jest zawsze ten sam –

„inwestorzy” czerpią zysk z niższych szczebli, a tylko część środków trafia do twórcy oszustwa. Taki psychologiczny trik stoi u podstaw każdej piramidy finansowej. Choć mechanizm działania oszustwa wydaje się powszechnie znany, wciąż powstają nowe piramidy, które doprowadzają tysiące naiwnych inwestorów do ruiny.

Piramidy i oszustwa finansowe

to przekręty,

które raz na jakiś czas mają miejsce

pod przykrywką nowego, świeżego biznesu.

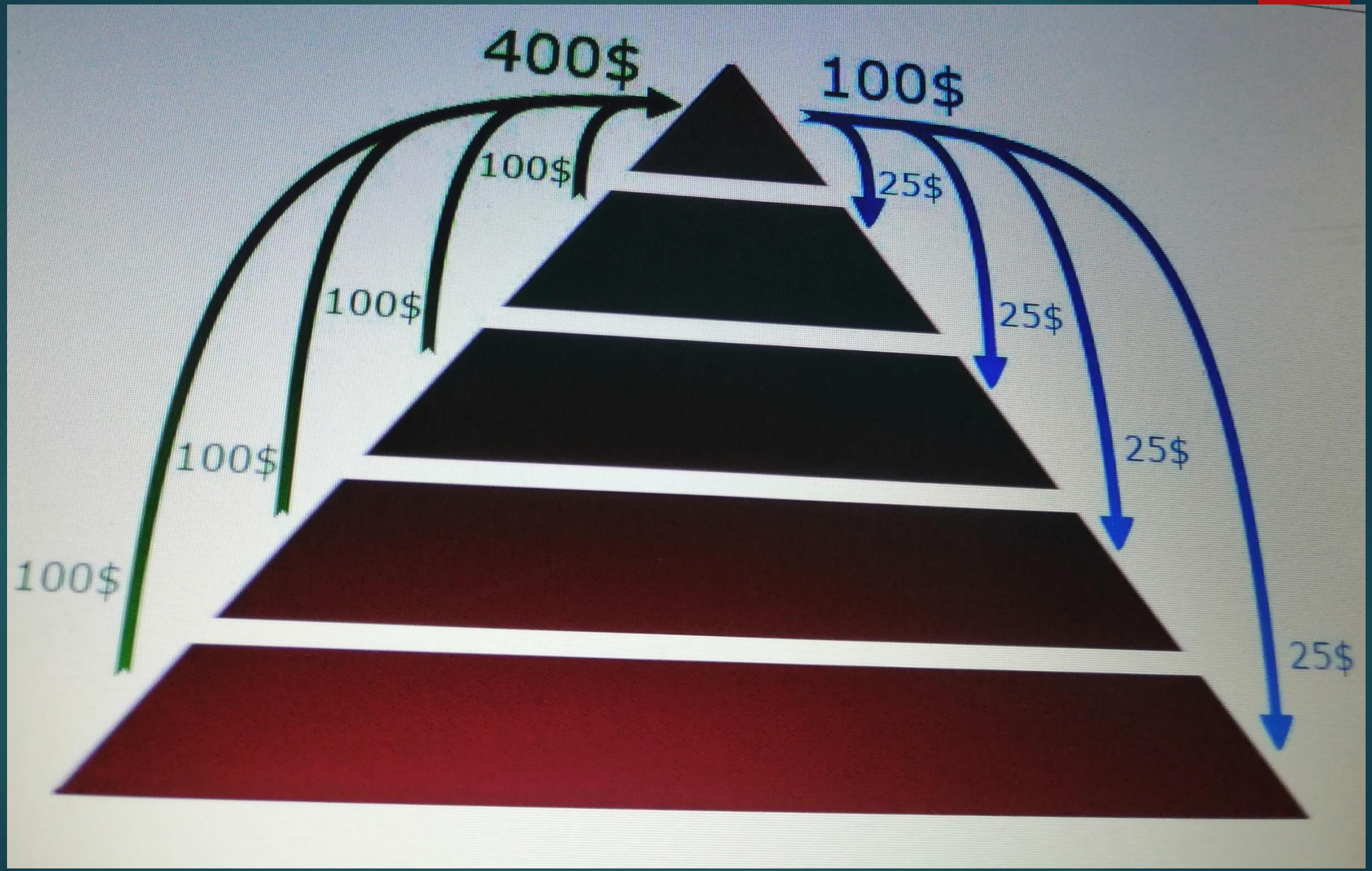
Jak rozpoznać oszukańczy schemat?

Za pierwszą piramidę finansową w najnowszej historii uważa się założoną w 1899 r. w przez nowojorskiego księgowego **Williama Millera** firmę Franklin Syndicate. Miller przekonywał inwestorów skuszonych 10 proc. zyskiem wypłacanym co tydzień, że posiada wyjątkową wiedzę na temat mechanizmów działania systemów finansowych.

Miller w krótkim czasie wyłudził milion dolarów (równowartość dzisiejszych 25 mln dol.). Oszust został skazany na 10 lat więzienia. Po wyjściu z więzienia nie wrócił do świata finansów - otworzył sklep spożywczy na Long Island

Charles Ponzi i Security Company 1919 r.

Stworzony w Bostonie przez włoskiego imigranta fundusz inwestycyjny o charakterze piramidy finansowej, przedsięwzięcie zakończyło się tak wielką aferą, że określenie "schemat Ponziego" stało się powszechnie używanym synonimem piramidy finansowej.


400$
100$
100$
100$
100$
100$
25$
25$
25$
25$

Jak się bronić przed piramidą finansową i innymi oszustwami ?

Zanim powierzymy komuś nasze oszczędności, weźmy pod lupę następujące czynniki:

1. Transparentność zasad

Tak jak nie podpisujesz umowy kredytowej, której nie rozumiesz, tak samo nie wchodź w inwestycje z instytucjami, które prowadzą nie do końca jasną politykę finansowania i czerpania zysków.

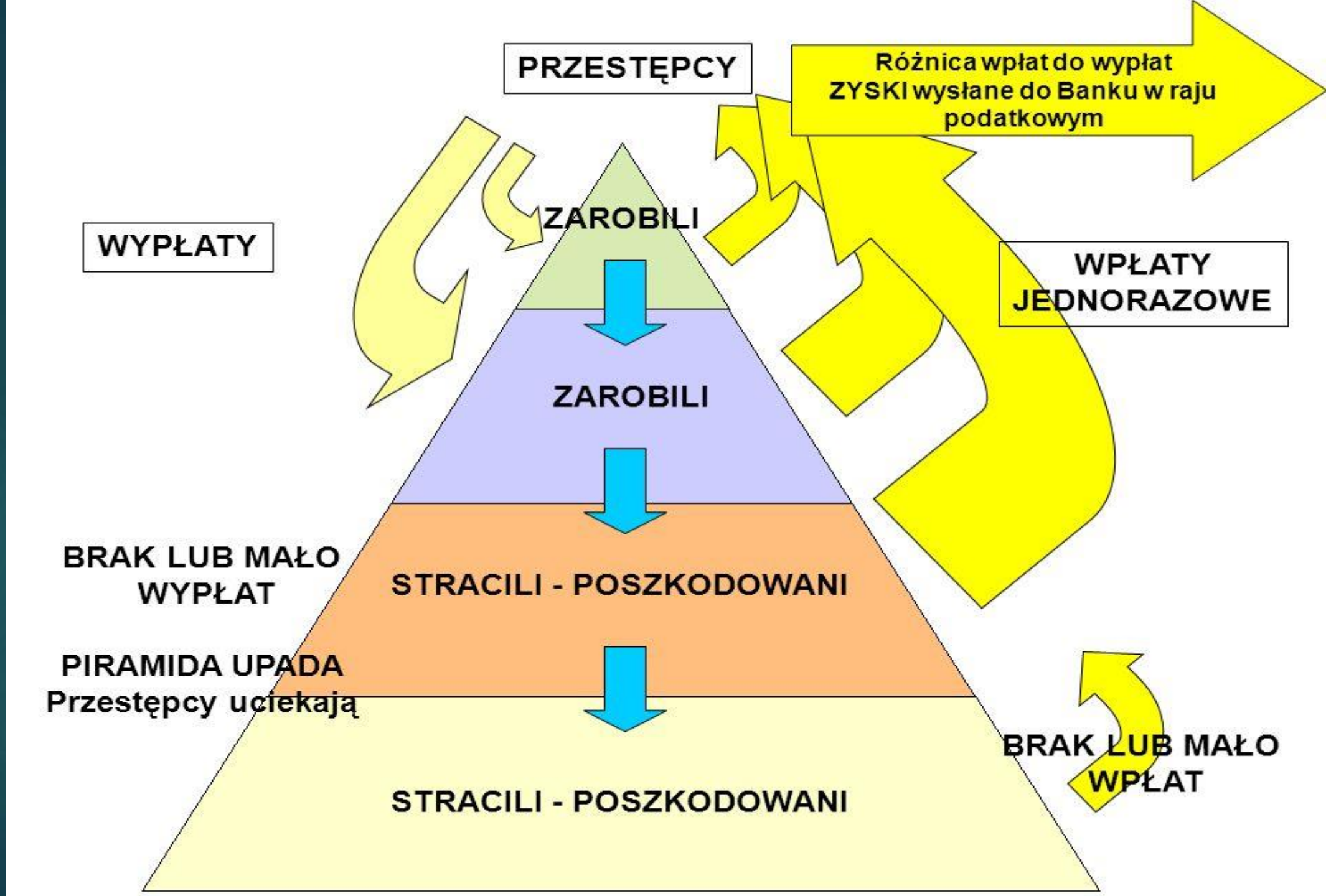
Jeśli cokolwiek budzi Twoją wątpliwość lub niepokój - nie wchodź w niepewny interes.

Dobre finanse to zrozumiałe finanse.

2. Sprawdzaj

Jeśli mimo wszystko chcesz zainwestować, sprawdź koniecznie czy jego działalność oparta **na zezwoleniu Komisji Nadzoru Finansowego**.

KNF prowadzi też wykaz firm, które uważa za podejrzane – lepiej się upewnić.

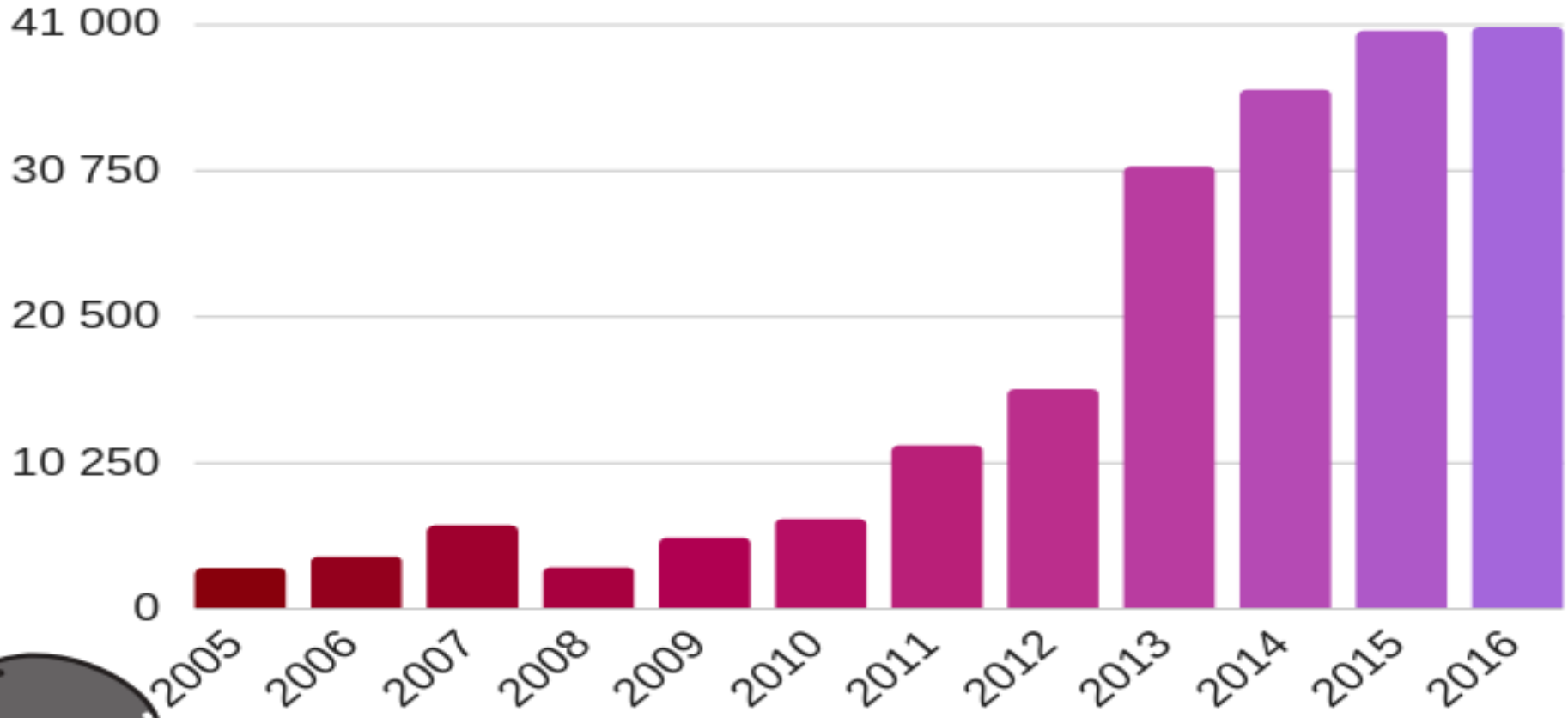

PRZESTĘPCY
Różnica wpłat do wypłat
ZYSKI wysłane do Banku w raju podatkowym
WYPŁATY
ZAROBILI
WPŁATY JEDNORAZOWE
ZAROBILI
BRAK LUB MAŁO WYPŁAT
STRACILI - POSZKODOWANI
PIRAMIDA UPADA
Przestępcy uciekają
BRAK LUB MAŁO WPŁAT
STRACILI - POSZKODOWANI

Za każdym razem, **gdy warunkiem zarobku jest pozyskanie nowych członków piramidy z prowizją za klienta – miej się na baczności**.

Piramida finansowa może też przybrać bardziej atrakcyjną formę propozycji pracy zdalnej (z domu), gdzie **po uiszczeniu kwoty członkowskiej** otrzymać mamy pakiet startowy na rozruch własnego biznesu – zazwyczaj bezwartościowy.

Piramidy finansowe to też łańcuszkowy marketing mailingowy, gdzie po wpłacie niewielkiej sumy na rzecz wyznaczonej osoby z listy, wiadomość należy przesłać dalej i czekać na „zysk”…

Liczba oszustw internetowych w Polsce



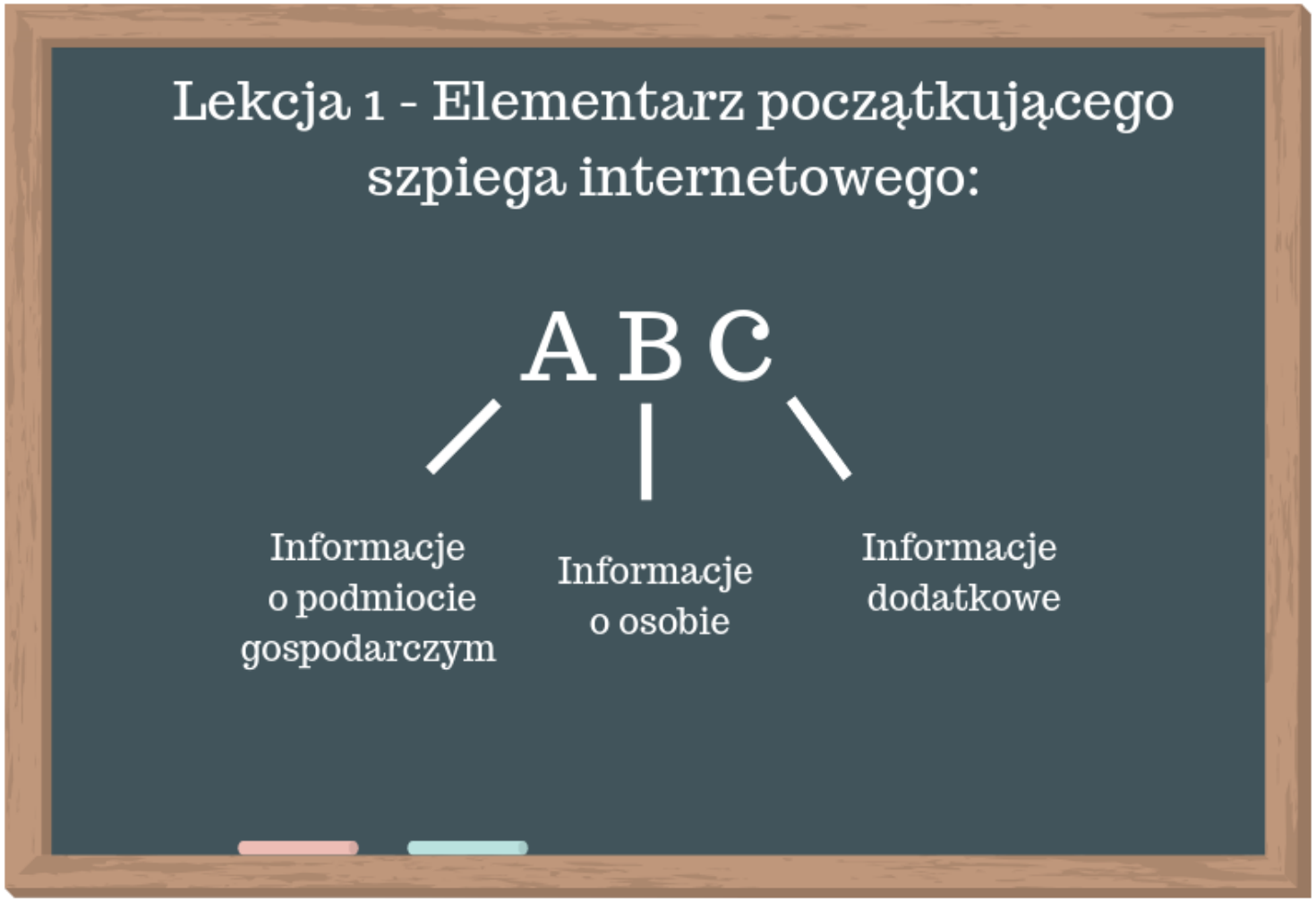
Źródła:
Statystyki Komendy Głównej Policji http://statystyka.policja.pl/
Raport o stanie bezpieczeństwa w Polsce 2016 https://bip.mswia.gov.pl/ s. 264

Lawinowy wzrost liczby oszustw z wykorzystaniem sieci.

Oszuści najczęściej wykorzystują klasyczne metody manipulacyjne i tylko uzupełniają je nowoczesnymi formami komunikacji i płatności.

Starają się wykorzystać chciwość lub naiwność ofiar.

ZOSTAŃ SZPIEGIEM INTERNETOWYM ZŁAP KOŁO RATUNKOWE



Jakie informacje warto sprawdzić w sieci

Jeżeli ogłoszenie jest wystawiane przez firmę, warto odwiedzić portal Ministerstwa Rozwoju i dokonać sprawdzenia w darmowej wyszukiwarce (np. po numerze NIP).

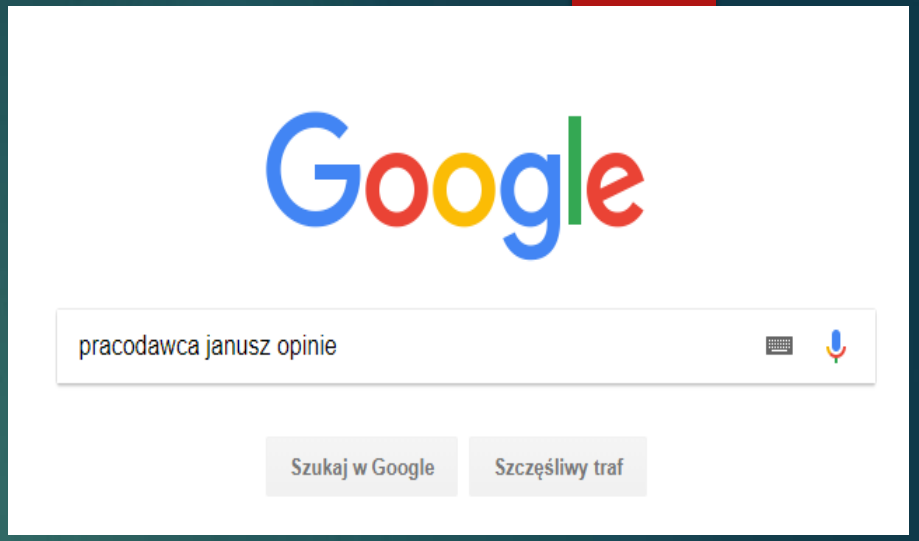
Najważniejsze informacje:

- imię i nazwisko właściciela
- data i miejsce rejestracji podmiotu
- przede wszystkim, czy taka firma w ogóle istnieje?

Link: https://mojepanstwo.pl/

Moje Państwo to potężna wyszukiwarka zawierająca informacje z KRS, rejestrów zamówień publicznych oraz popularnych mediów.

Informacje o osobie



Najprostsze rozwiązania bywają najskuteczniejsze.

Istnieje duża szansa, że ktoś zdążył już „obsmarować” w sieci analizowanego firmę.

W pierwszej kolejności sprawdzamy opinie internautów na forach i portalach społecznościowych,

opinie z serwisów społecznościowych, artykuły.

Pamiętaj, aby do informacji podchodzić z dystansem. Jedna czy dwie negatywne opinie nie są dowodem nieuczciwości.

Link:

https://search.carrot2.org/#/search/web

warto zaczerpnąć informacji z mniej komercyjnego źródła - większość internetowych informacji na temat:

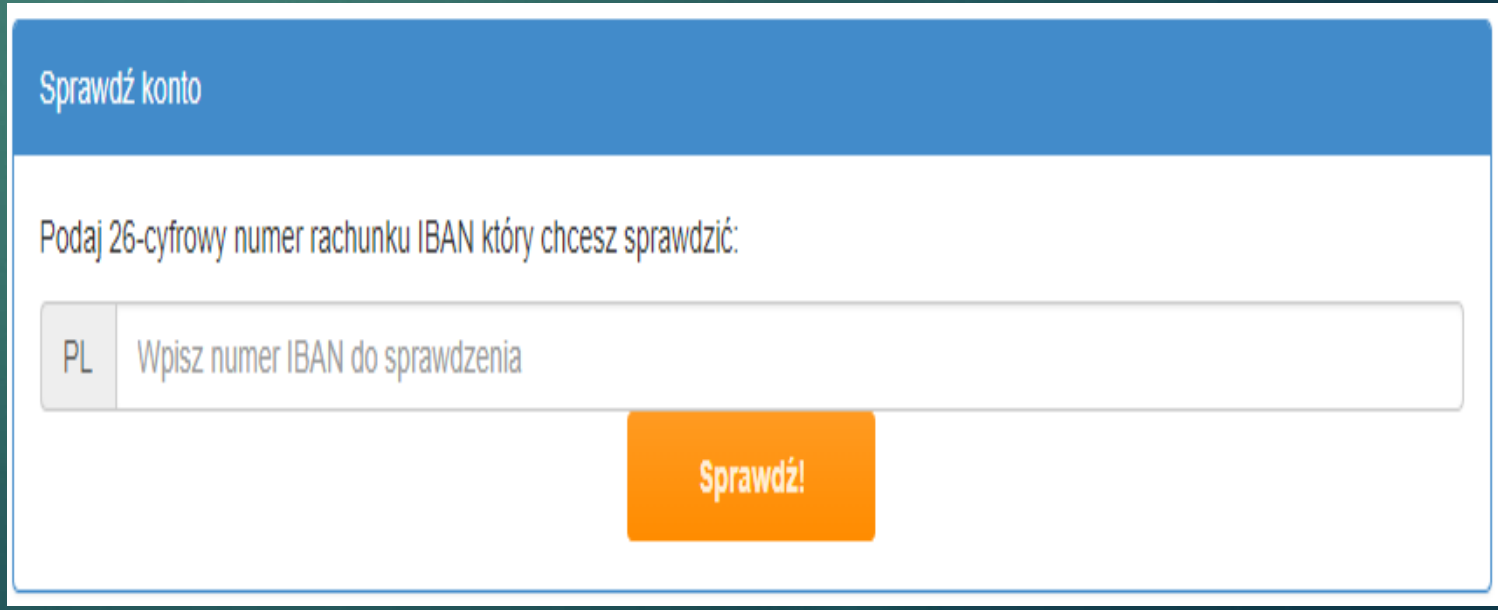
- Czy osoba o podanych danych w ogóle istnieje?
- Czy osoba miała kiedykolwiek konta na portalach społecznościowych?
- W jaki sposób inni internauci wyrażają się o tej osobie?

Niepokojące będzie również brak informacji o numerze rachunku bankowego

Link: http://jakitobank.pl/

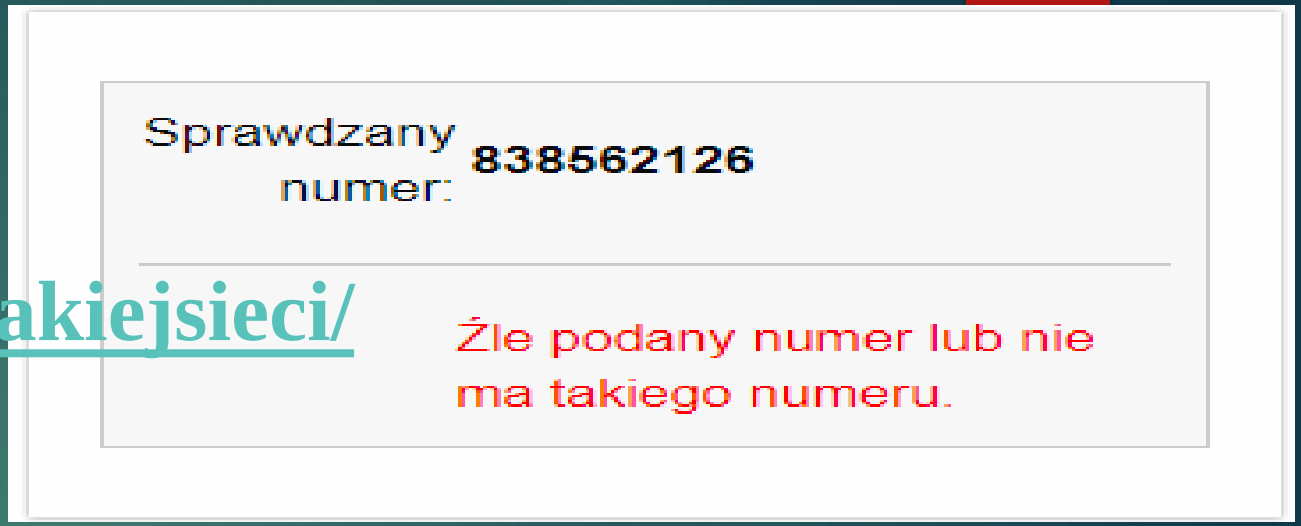
możemy sprawdzić każdy rachunek bankowy.

Uzyskamy informację, który bank go obsługuje oraz w której placówce został założony.
Pod tymi informacjami znajduje się sekcja komentarzy m.in., że rachunkiem posługuje się oszust



Numer telefonu komórkowego

Link: http://www.mgsm.pl/pl/wjakiejsieci/



Dzięki tej stronie sprawdzisz operatora numeru telefonu komórkowego, czy taki numer istnieje.

Warto sprawdzić telefony kontaktowe podane na stronie internetowej. Oszuści wiedzą, że umieszczenie ich w widocznym miejscu podnosi zaufanie. Wiedzą też, że mało który klient zdecyduje się skorzystać z tego telefonu i podają tam 9 przypadkowych cyfr.

Adres email

Należy zwracać uwagę na konstrukcję adresu e-mail, którym posługuje się pracodawca. Skoro ogłoszenie dotyczy pracy w poważnej, dobrze rozwijającej się firmie, to ich skrzynka pocztowa powinna znajdować się na własnym serwerze?

INNE OSZUSTWA i produkty finansowe związane są z pojęciem socjotechniki

Czym jest socjotechnika?

są to metody manipulacji człowiekiem,

mające na celu nakłonienie go do podjęcia określonych czynności

Ataki socjotechniczne - polegają na przekonaniu Użytkownika do otworzenia dokumentu z załącznika, pobrania pliku, podania poufnych danych na fałszywej stronie internetowej lub otworzenia linku do zainfekowanej strony www.

Użytkownik otrzymuje wiadomość, która skłania go do np.:

- kliknięcia w link oferujący ściągnięcie darmowej aplikacji na wybrany model telefonu,
- przesłaniu określonych informacji pod wskazany adres e-mail,
- wypełnienia fałszywego formularza z danymi osobowymi w celu wzięcia udziału w konkursie lub otrzymania nagrody.

Popularność transakcji kupna i sprzedaży przez Internet jest bardzo duża.

Można kupić lub sprzedać rzeczy już nie używanych w atrakcyjnej cenie.

Dostęp do takich ofert jest szybki i prosty, dlatego zyskuje na popularności, jednak niesie za sobą pewne ryzyko. Również oszuści działają w tej przestrzeni.

Działanie oszusta jest proste:
- podszywa się pod kupującego za pośrednictwem znanego komunikatora,
- na telefon komórkowy wysyła wiadomość z zapytaniem, czy ogłoszenie jest aktualne.
- W kolejnym sms, że zapłaci za towar i prosi o wysyłkę.
- W wiadomości załączony jest link do strony za pomocą, której sprzedający ma odebrać rzekomo przelane pieniądze, jednak wcześniej musi podać dane z karty płatniczej.
- Pokrzywdzony wpisuje dane swojej karty, pieniądze jednak nie wpływają na jego konto, **co więcej traci on swoje oszczędności, a kontakt z kupującym urywa się .**

Bądźmy ostrożni
podając w internecie
numer swojej karty kredytowej,
przestrzegajmy kilku zasad
ograniczając ryzyko:

- **nie klikaj żadnych odsyłaczy** w wiadomości przesłanej sms-em, za pośrednictwem komunikatora, czy e-maila: odsyłacze te, często prowadzą do sfałszowanych stron lub stron zainfekowanych szkodliwymi programami,
- kiedy kupujący lub sprzedający prosi cię o zainstalowanie nieznanego oprogramowania na telefon lub komputer, zastanów się – to może być program do szpiegowania twoich ruchów na klawiaturze, w ten sposób oszust widzi pulpit twojego laptopa i tak zdobywa twoje hasła do logowania,
- **nie otwieraj załączników** do wiadomości, jeżeli masz jakiekolwiek wątpliwości dotyczące nadawcy,

Kierujecie się opiniami robiąc zakupy?

TU TEŻ CZYHA NA NAS PUŁAPKA?

Opinie w sieci –

Według badań ponad 50 proc. Polaków wierzy we wszystko co przeczyta w sieci.

To zjawisko wykorzystują nieuczciwe sklepy internetowe by uwiarygodnić swoją sprzedaż. Zlecają np.: agencjom reklamowym pisanie pozytywnych, choć nieprawdziwych komentarzy, zamieszczanie ich na portalach i platformach internetowych zbierających i publikujących opinie o firmach działających w sieci.

- Problem w tym, że w praktyce prawdziwości fałszywek nikt nie weryfikuje i nikt nie jest odpowiedzialny za to, że wyprowadzają konsumentów w błąd.
- Konsekwencję takiego procederu ponoszą jedynie klienci nieuczciwych sklepów – bo tracą pieniądze.
- Klienci robili zamówienia, płacili, ale towar nie przychodził. Próbowali odzyskać pieniądze, ale wtedy okazało się, że sklep nie istnieje.

Portal eopiniowo nie tworzy sam opinii, a jedynie przechowują i upubliczniają komentarze klientów. Jeśli przedsiębiorca chce podjąć współpracę z serwisem, musi wykupić abonament na sześć miesięcy lub na rok. Koszt – od kilkudziesięciu złotych do ponad 600 zł. Potem sprzedawca instaluje u siebie udostępnione oprogramowanie i wchodzi do opiniowego systemu. Komentarze zbiera się za pomocą ankiet wysyłanych do klientów, którzy już zrealizowali transakcje. Opinie takie uznawane są przez portale – np.: Opineo.pl – za wiarygodne.

.

- Prawnicy skierowali zawiadomienia do UOKiK - Urzędu Ochrony Konkurencji i Konsumentów dotyczące podejrzenia stosowania praktyk naruszających zbiorowe interesy konsumentów
- Problem fałszowania opinii i manipulowania nimi zauważa też Unia Europejska. W 2019 r. przyjęto dyrektywę Parlamentu Europejskiego i Rady UE 2019/2161, która wyraźnie zakazuje zamieszczania fałszywych opinii i manipulowania opiniami.

Phishing

oszustwo mailowe.

Przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji np. danych logowania, danych karty kredytowej lub zainfekowania komputera szkodliwym oprogramowaniem. Zdecydowana większość wiadomości phishingowych jest dostarczana za pośrednictwem poczty elektronicznej, portali społecznościowych lub wiadomości sms.

przykłady fałszywych maili

Zwróć uwagę, czy adres nadawcy jest właściwy i czy nie ma w nim literówek.

Nie klikaj w linki, które zachęcają do logowania do banku. Jeśli wiadomość zawiera załącznik a nie jesteś pewien nadawcy, nie otwieraj załącznika.

Przeczytaj uważnie wiadomość. Cyberprzestępcy często piszą o problemach z logowaniem lub blokowaniem konta. Chcą na Tobie wymusić szybką reakcję. Dlatego zastanów się spokojnie nad sprawą, a gdy masz wątpliwości, zadzwoń do banku.

Szanowni Panstwo,

Pragniemy przypomniec o nieuregulowanej Fakturze o numerze **F/20249758/09/14** wystawionej w dniu **12/09/2014**. Oplacenie Faktury po terminie bedzie skutkowalo naliczeniem odsetek ustawowych.
Jak czytac fakture? - **instrukcja**.

Forma platnosci:	**Przelew / Foto wplata**
Termin platnosci:	**21/09/2014**
Nazwa wystawcy:	P4 sp. z o.o. ul. Tasmowa 7, 02-677 Warszawa, NIP 951-21-20-077
Kwota do zaplaty	**107,27 zl**
Numer konta:	**46 1090 0004 7777 0100 2573 5659**
Zalecany tytul przelewu:	Play faktura **F/20249758/09/14** klient **25735659**

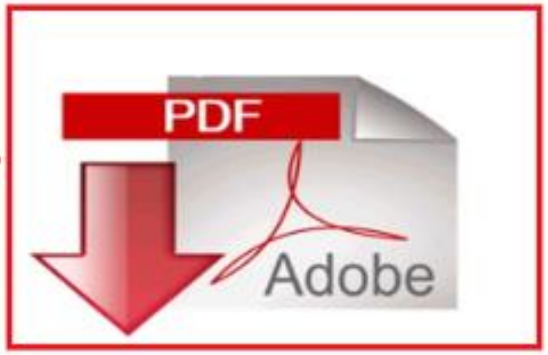
kwota powinna być zgodna z prognozą. Jeżeli do tej pory płaciliśmy abonament w wysokości np. 59 zł, a na nowej fakturze widzimy kwotę prawie dwukrotnie wyższą, to powinna nam się zapalić czerwona lampka.

fałszywy numer konta

numer klienta/abonenta. Fałszywe faktury wysyłane masowo mają przypisany na sztywno jeden numer, a niekiedy nie posiadają go wcale. Dzięki temu możemy sprawdzić czy faktycznie faktura jest adresowana do nas

Pobierz Fakture:

załącznik, który zawiera szkodliwe oprogramowanie. Współczesny malware potrafi rezydować na komputerze w sposób niezauważony i przez wiele tygodni wykradać dane użytkownika, a nawet zaszyfrować wszystkie pliki i żądać za to okupu (ransomware).



Dziekujemy za terminowe dokonywanie platnosci, które chroni przed naliczaniem odsetek ustawowych.

Jednoczesnie informujemy, ze archiwum e-faktur znajduje sie na serwisie **Play24**, gdzie mozna sprawdzic integralnosc tresci i autentycznosc pochodzenia zalaczonej faktury.

Zachecamy do wypelnienia ankiety na temat e-faktury. Ankieta dostepna jest po zalogowaniu do Play24, w zakładce Faktury. Państwa opinia jest dla nas bardzo ważna. Dziękujemy!

Od: Facebook
Do: mnie [redacted]@wp.pl
Temat: Podejrzana aktywność na Twoim koncie

24 cze 2020 21:38 (2 dni temu)

Facebook
gmai5@int.pl

zwróć uwagę na dziwny adres e-mail

Facebook

Wykryliśmy podejrzaną aktywność na Twoim koncie Facebook związaną z zamówieniem reklamy za kwotę 375 zł. Ze względów bezpieczeństwa wymagamy potwierdzenia, że zamówienie zostało złożone przez Ciebie.
Potwierdzam zamówienie.

Potwierdzam zamówienie

Jeśli sądzisz, że Twoje osobiste konto na Facebooku mogło zostać przejęte przez osoby nieuprawnione prosimy o anulowanie zamówienia, zaktualizowanie aplikacji Facebook, zmianę hasła i wylogowanie się z innych urządzeń..

Anuluj zamówienie

wiesz, że nic nie zamawiałeś, więc na 90% klikniesz "Anuluj zamówienie"

Potrzebujesz dodatkowej pomocy? Dowiedz się więcej na temat zabezpieczania konta.

Ta wiadomość została wysłana na adres[redacted]@wp.pl. Aby zapewnić bezpieczeństwo swojego konta, nie przekazuj dalej tego e-maila.

Najczęściej spotykane kampanie spamerskie, które zawierały zainfekowane pliki lub linki kierujące na fałszywe strony:

- „Faktura Orange”
- „Potwierdzenie otrzymania paczki”
- „Wezwanie do zapłaty”
- „eFaktura za energię elektryczną”
- „Twoje konto zostało zablokowane”
- „Ważne! Dotyczy Państwa firmy”
- „Korekta rocznego zeznania podatkowego”

Najnowszy atak phishingowy kierowany do klientów nazwa.pl home.pl

Od: **nazwa.pl** <nazwa@[redacted].eu>
Date: sob., 26 wrz 2020 o 15:35
Subject: [redacted].eu - dobiega konca w dniu 2020-09-28
To: <contact@[redacted].eu>

Dzień dobry,

pragnę przypomnieć, że abonament usługi "[redacted].eu" dobiega końca w dniu **2020-09-28**

Informacje dotyczące kontynuacji dostępne są w Panelu, w sekcji Płatności:

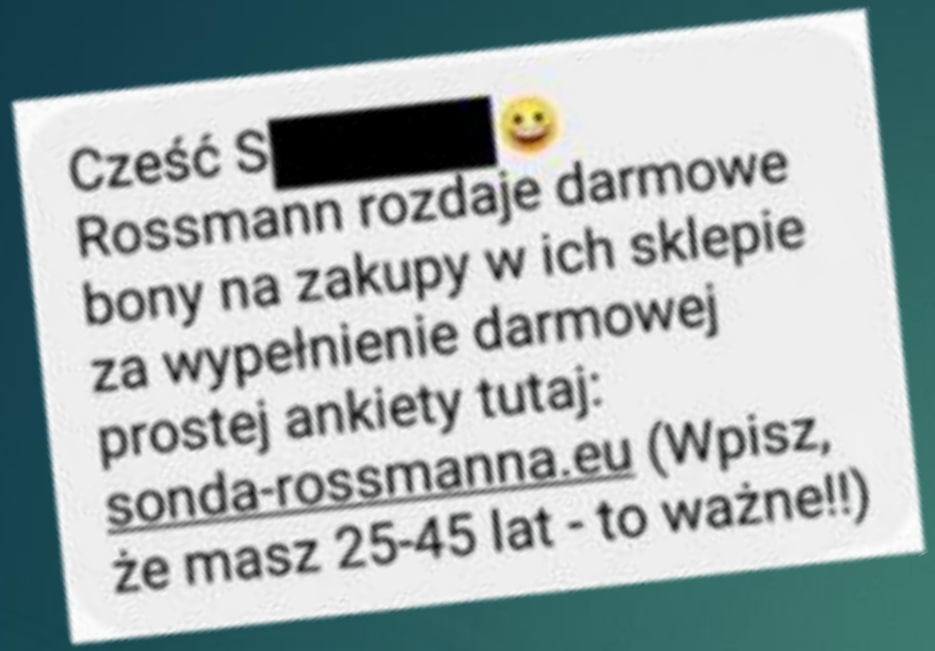
https//panel.nazwa.pl/cgi-bin/order/bill.cgi?reference=[redacted].eu

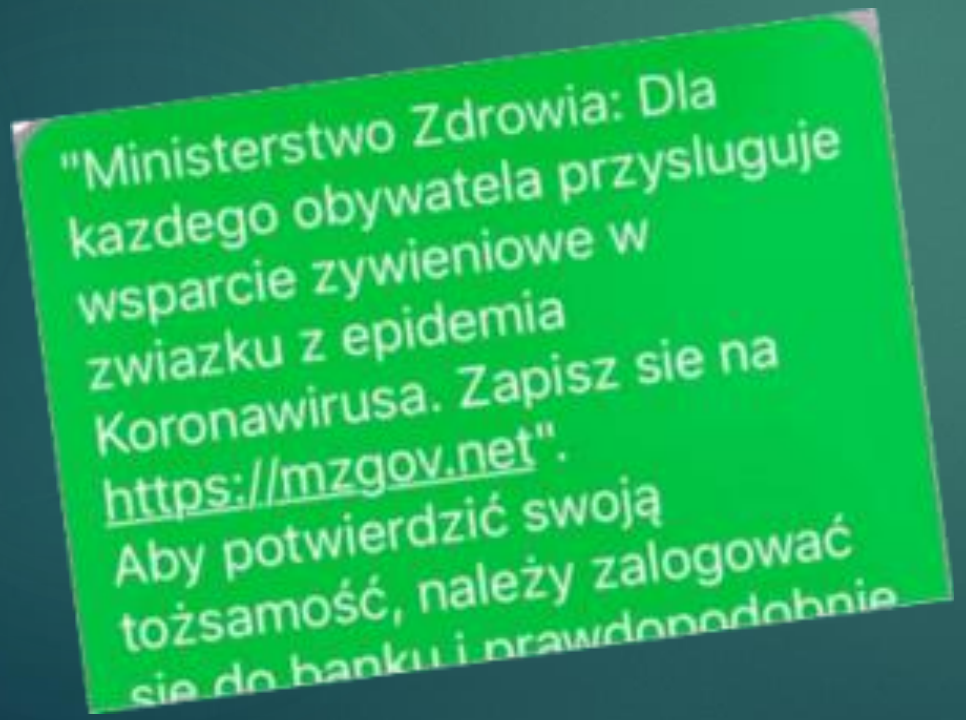
Przedłużenie usługi we wskazanym terminie zapewni ciągłość jej działania.

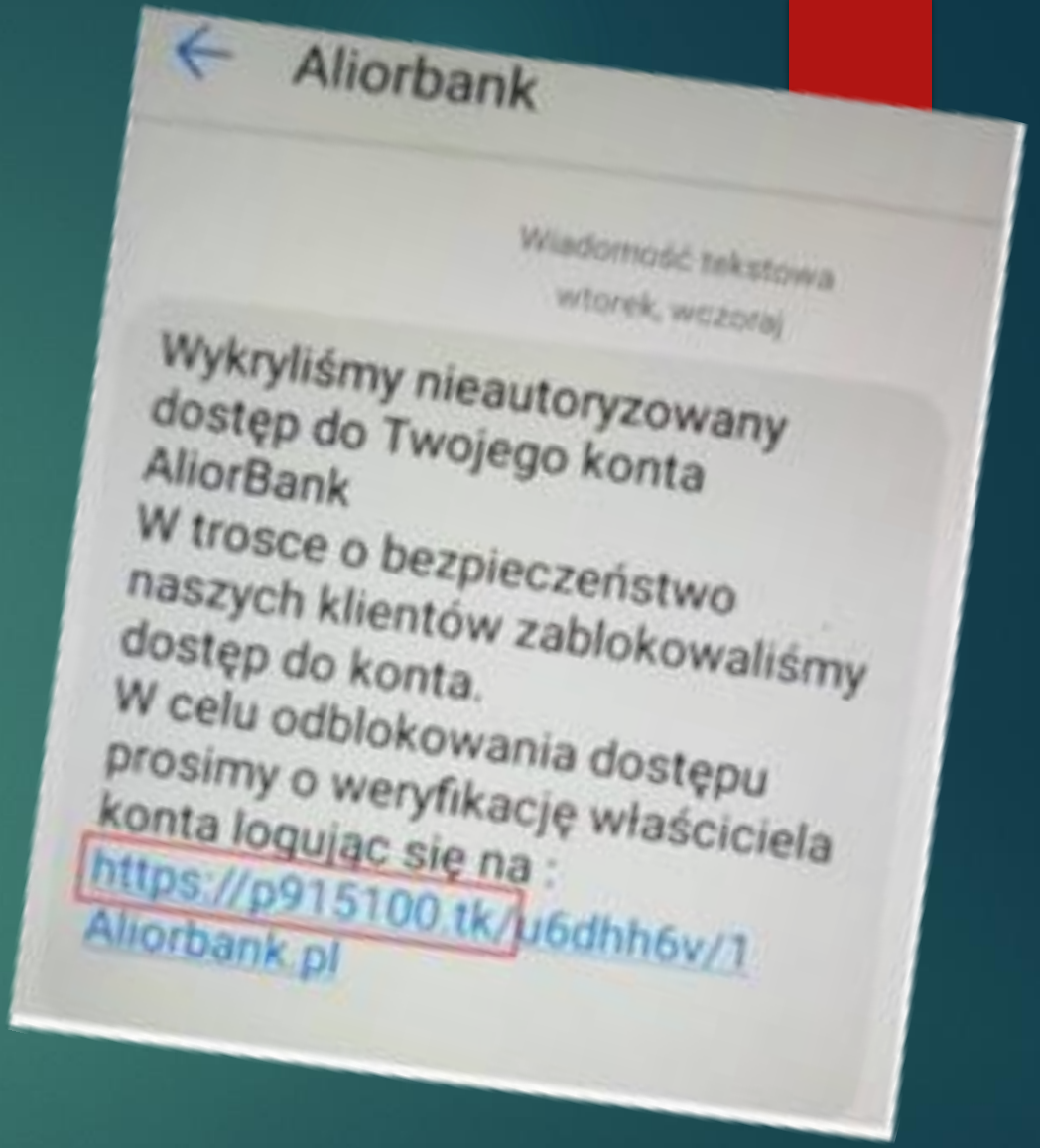
Aby uniknąć zawieszenia usługi i dodatkowych kosztów przywrócenia, konieczne jest dokonanie opłaty za przedłużenie teraz.

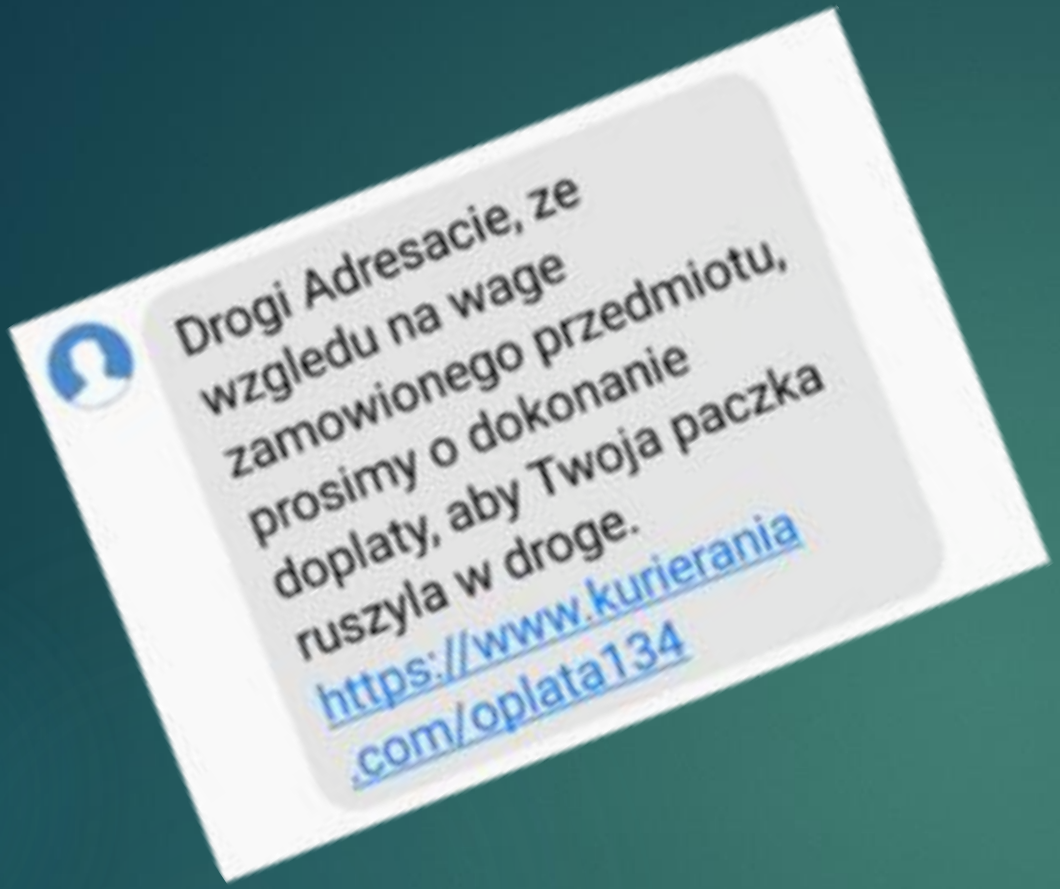
--
Pozdrawiam
Szturmaj Magdalena
Dział Obsługi Klienta nazwa.pl

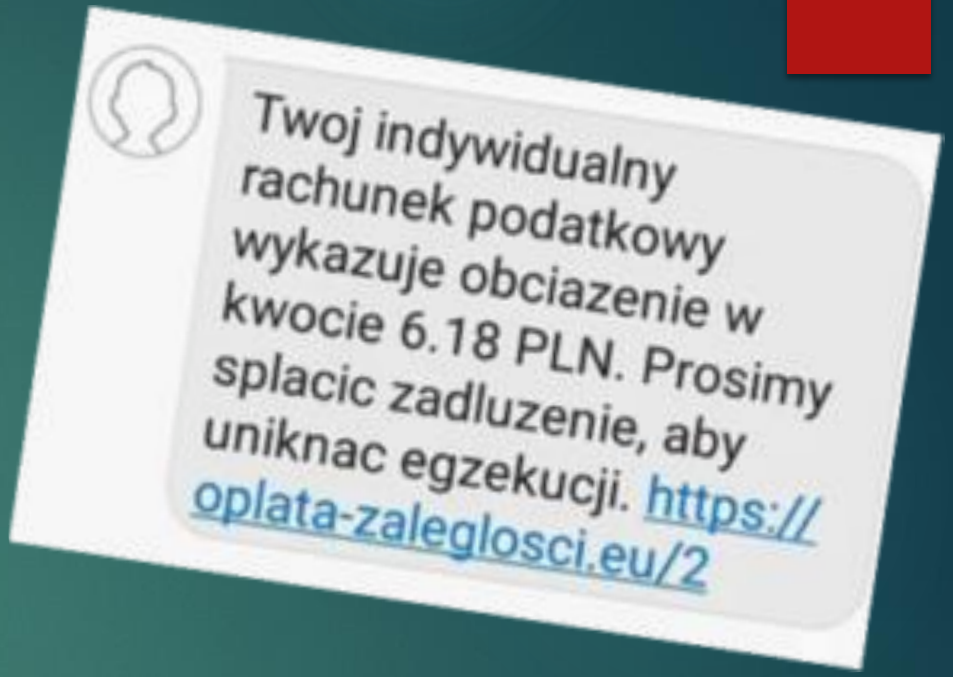
Przykłady fałszywych smsów


Cześć S[redacted]
Rossmann rozdaje darmowe bony na zakupy w ich sklepie za wypełnienie darmowej prostej ankiety tutaj: sonda-rossmanna.eu (Wpisz, że masz 25-45 lat - to ważne!!)


"Ministerstwo Zdrowia: Dla kazdego obywatela przysluguje wsparcie zywieniowe w zwiazku z epidemia Koronawirusa. Zapisz sie na https://mzgov.net".
Aby potwierdzić swoją tożsamość, należy zalogować


Aliorbank
Wiadomość tekstowa
wtorek, wczoraj
Wykryliśmy nieautoryzowany dostęp do Twojego konta AliorBank
W trosce o bezpieczeństwo naszych klientów zablokowaliśmy dostęp do konta.
W celu odblokowania dostępu prosimy o weryfikację właściciela konta logując się na :
https://p915100.tk/u6dhh6v/1
Aliorbank.pl


Drogi Adresacie, ze wzgledu na wage zamowionego przedmiotu, prosimy o dokonanie doplaty, aby Twoja paczka ruszyla w droge. https://www.kurierania.com/oplata134


Twoj indywidualny rachunek podatkowy wykazuje obciazenie w kwocie 6.18 PLN. Prosimy splacic zadluzenie, aby uniknac egzekucji. https://oplata-zaleglosci.eu/2

Co może świadczyć o ataku phishingowym?

„Drogi kliencie”.

Napastnicy często stosują ogólne zwroty okolicznościowe, tymczasem większość organizacji komunikujących się za pośrednictwem e-maila zna dane adresatów i zwraca się do nich po imieniu lub nazwisku.

Większość fałszywych wiadomości zawiera różnego rodzaju groźby, ostrzeżenia.

„Jeśli nie odpowiesz na powyższą wiadomość, Twoje konto bankowe zostanie wkrótce zablokowane”.

Ich autorzy ostrzegają adresata, że brak reakcji może przyczynić się do zamknięcia konta, zerwania umowy, utraty danych, awarii itp.

Prośba o udostępnienie informacji wrażliwych

Cyberprzestępcy zazwyczaj proszą o podanie haseł dostępowych, PIN, numerów kart kredytowych itp.

Błędy językowe

Cyberprzestępcy pochodzą z różnych części globu, dlatego list napisany przez obcokrajowca w języku polskim, może zawierać liczne błędy ortograficzne i gramatyczne.

Niewłaściwe adresy

Należy sprawdzić czy po kliknięciu na link strony, zostaniemy przekierowani na adres witryny prawdziwego serwisu internetowego.

VISHING

Na czym polega vishing?

to wyłudzanie danych lecz w wersji głosowej, a dokładnie w trakcie rozmowy telefonicznej.

Zręczni rozmówcy podający się za np. bankowców, doradców inwestycyjnych są w stanie tak zmanipulować rozmówcę, że ten ujawni swoje szczegółowe dane. Chwilę później giną środki z jego konta bankowego. Vishing, nie wymaga od przestępców zaawansowanej wiedzy informatycznej. Wyłudzają dokładnie te same dane, używając do tego celu wyłącznie telefonu.

Jak się chronić przed vishingiem?

Najlepszą radą może być ta, którą wielokrotnie słyszeliśmy jako dzieci — **„nie rozmawiaj z nieznajomymi”.**

Należy tę radę uzupełnić prostym przesłaniem — nie podawaj rozmówcy szczegółowych danych na swój temat, a już na pewno nie rób tego w przypadku **loginów, haseł, kodów PIN** oraz innych informacji, które mogą być kluczem dostępu do naszych kont bankowych, czy usług cyfrowych, jak np. media społecznościowe, portale pracownicze.

Jak rozpoznać oszustwo vishingu?

- Każdorazowo, kiedy rozmówca prosi nas o jakiekolwiek informacje szczegółowe na nasz temat, powinna w naszej głowie zapalić się lampka ostrzegawcza.
- Szczególnie powinniśmy uważać, gdy w rozmowie pojawiają się wyrażenia wywierające na nas presję np „ostatnia szansa", „mamy niewiele czasu", „musimy szybko działać", „to absolutnie bezpieczne, proszę się nie obawiać". Jeżeli do tego dochodzą pytania o dane wrażliwe, najlepiej od razu przerwać takie połączenie.
- Jeżeli rozmówca pyta nas, czy jesteśmy przy komputerze i proponuje zainstalowanie oprogramowania ułatwiającego „szkolenie" z obsługi narzędzi inwestycyjnych, lub przekieruje nas do „obsługi technicznej", to stuprocentowa próba oszustwa!

Jak zareagować jeśli podejrzewamy vishing?

- Jeżeli podejrzewamy, że rozmówca ma nieuczciwe intencje, powinniśmy przerwać połączenie i zagrozić zgłoszeniem sprawy na policję. Można poprosić o telefon za chwilę i zweryfikować prawdziwość oferty np. dzwoniąc na bankową infolinię.
- Oszuści specjalizujący się w vishingu są sprawnymi socjotechnikami i będą robić wszystko, żeby podtrzymać rozmowę i nie dopuścić do jakiejkolwiek próby weryfikacji prawdziwości „oferty". Nasza przewaga polega na tym, że w każdym momencie możemy nacisnąć czerwony przycisk kończący połączenie lub zwyczajnie odłożyć słuchawkę.

- fałszywe inwestycje internetowe oferowane na portalach społecznościowych prowadzące do kradzieży danych wrażliwych
- wyłudzenia:
  - pokazy z „prezentami”
  - „Na wnuczka”
  - „Na policjanta”
  - „Na inkasenta”…

Im większe „**obiecane zyski**”, tym większe ryzyko inwestycyjne.

Nie ma szybkich pieniędzy nie obarczonych żadnym ryzykiem.