

SZTUKA MANIPULACJI

---

**ATAKI Z WYKORZYSTANIEM  
SOCJOTECHNIKI**





SZTUKA MANIPULACJI

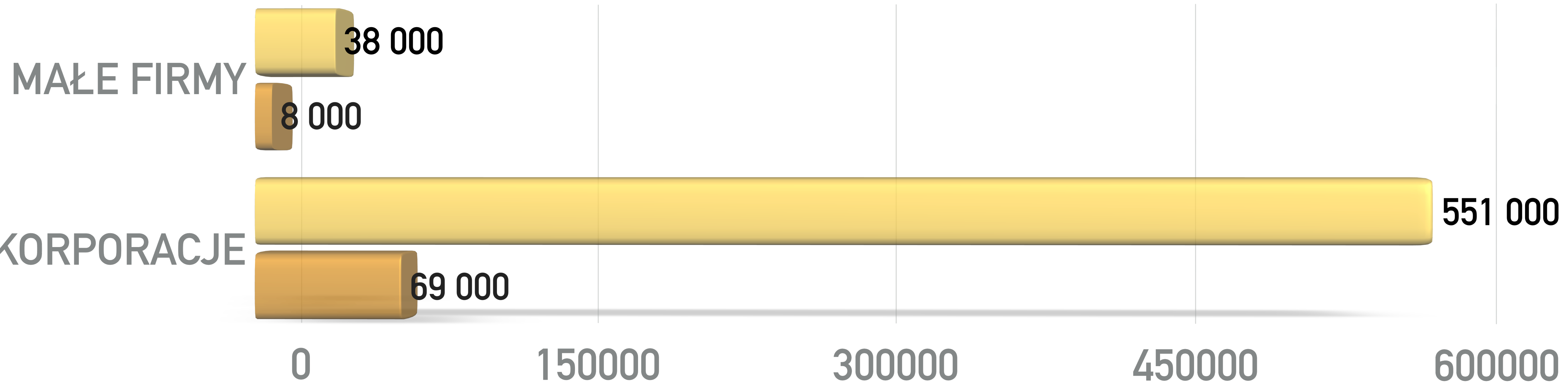
---

**DANE I STATYSTYKI**



## WYDATKI NA PRZECIWDZIAŁANIE CYBERATAKOM (\$)

Wydatki bezpośrednie      Koszty dodatkowe





☆ Preawizacja DHL

Do: [Redacted]

Preawizacja DHL



## Preawizacja DHL

Szanowni Państwo,

Otrzymaliśmy elektroniczne dane przesyłki nr 98626977650 z firmy [Redacted] Przesyłka nadal pozostaje w rękach nadawcy. Po przekazaniu jej Kurierowi DHL PARCEL prześlemy aktualny status wraz z planowanym terminem doręczenia.

Pozdrawiamy,  
DHL Parcel

[www.dhlparcel.com.pl](http://www.dhlparcel.com.pl)

Jeśli chcieliby Państwo otrzymywać drogą elektroniczną informacje o promocjach, nowych produktach i usługach, prosimy o wyrażenie zgody na stronie internetowej [DHL](http://DHL). Wypełnienie formularza zajmie tylko 2 minuty.

UWAGA: Wiadomość ta została wygenerowana automatycznie. Prosimy nie odpowiadać funkcją



Parcel\_Przesylka.18.12.  
2015.zip

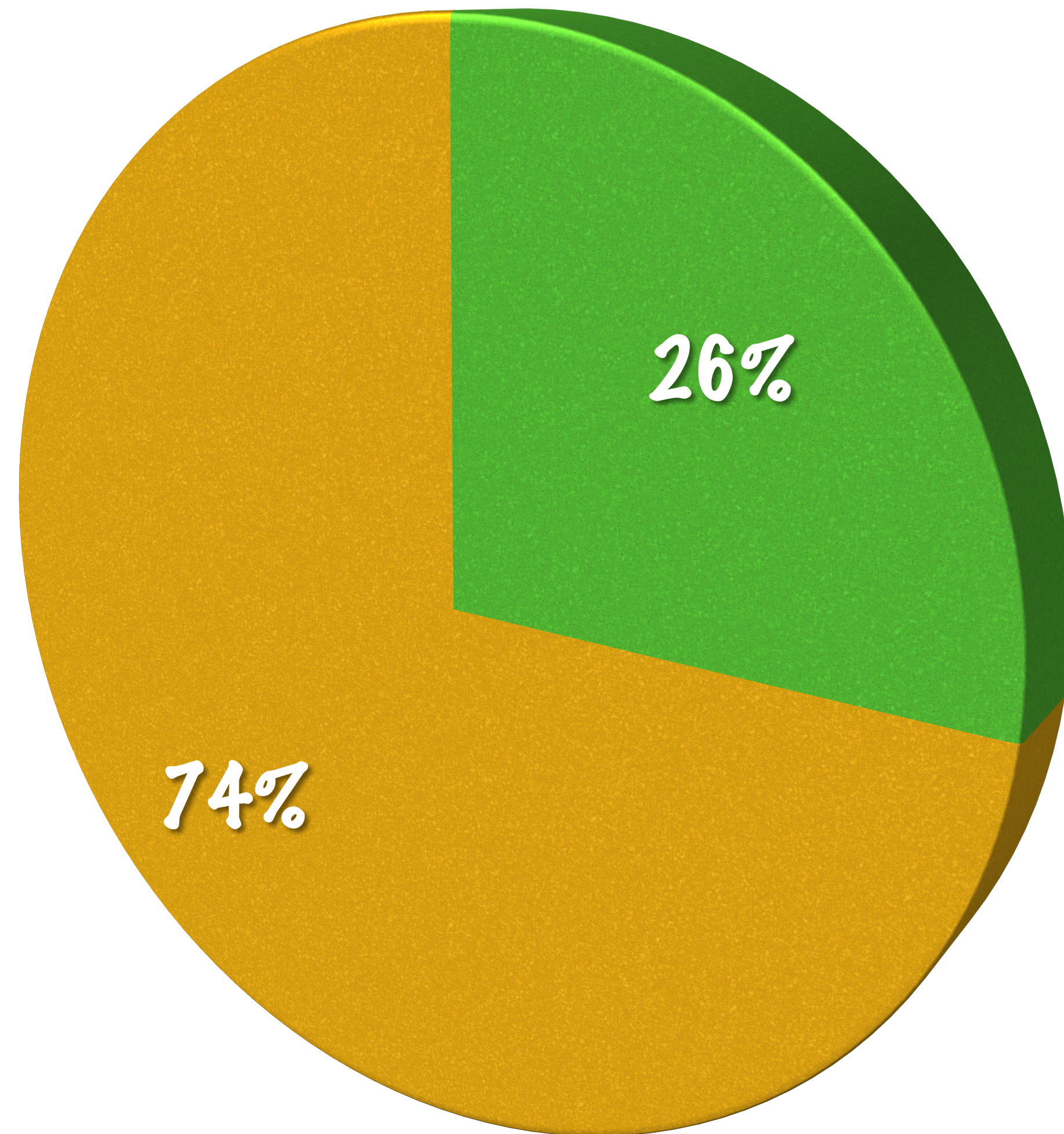
11 1111 1111 1111 1111 1111 1111

99 9999 9999 9999 9999 9999 9999

VBKlip



## ŚWIADOMOŚĆ UŻYTKOWNIKÓW



- Nie pobrano szkodliwego pliku
- Pobrano szkodliwy plik





SZTUKA MANIPULACJI

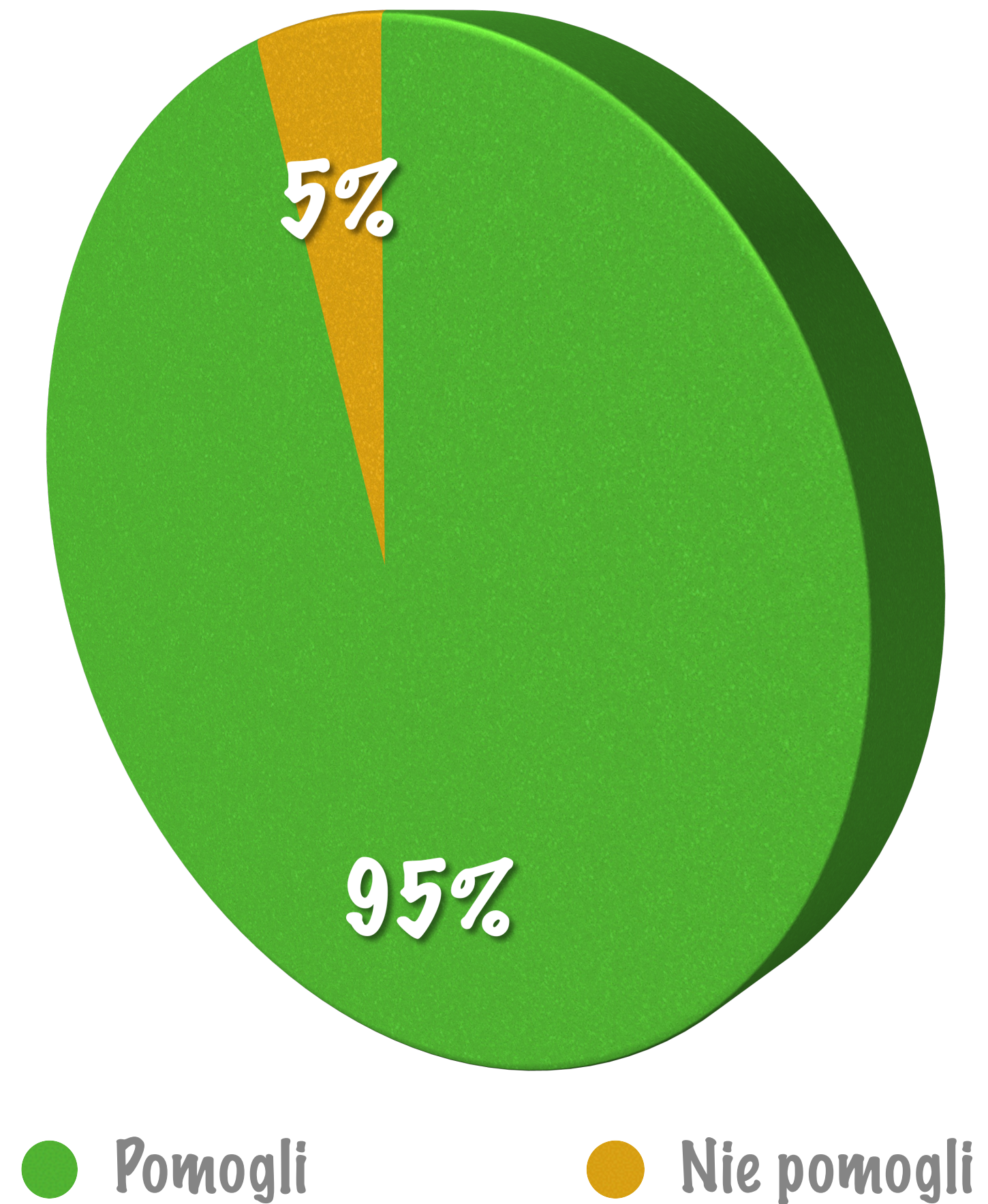
---

ATAK F2F



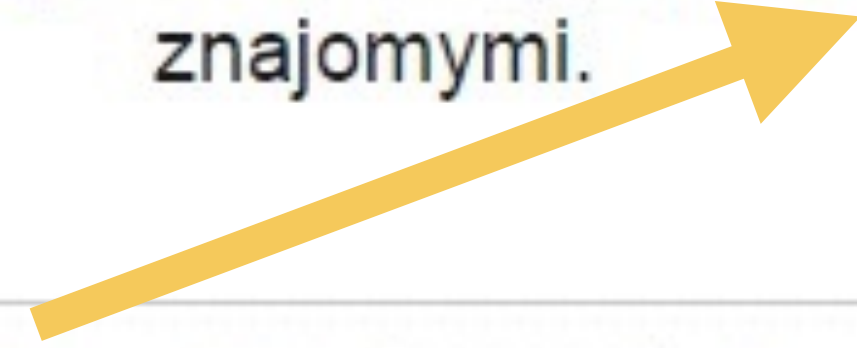
## METODY WPŁYWANIA NA DECYZJE

- ▶ Wzajemność
- ▶ Zaangażowanie i konsekwencja
- ▶ Współczucie





Adam [redacted] i Marcin [redacted] są teraz znajomymi.



Adam [redacted] i Magdalena [redacted] są

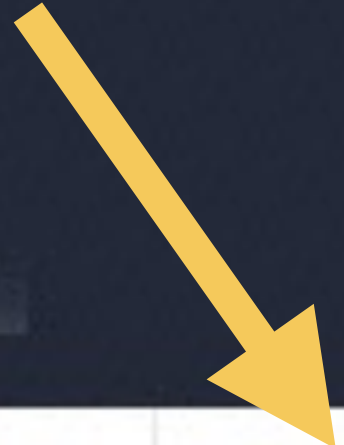
**Adam** [redacted]

Dodaj zdjęcie

Zaktualizuj informacje **3**

Zobacz dziennik aktywności **...**

**Adam** [redacted]



Oś czasu

Informacje

**Znajomi 91**

Zdjęcia

Więcej ▾

Marc  
już ta  
😊

Adam [redacted] i Paula [redacted] są teraz znajomymi.



13:54

swita



## PRZYKŁADOWY ATAK SOCJOTECHNICZNY

- ▶ Celem jest zainfekowanie sieci firmowej szkodliwym oprogramowaniem
- ▶ Wykorzystanie manipulacji poprzez współczucie i zaangażowanie
- ▶ Wykorzystanie informacji o pracowniku i stworzenie historii






SZTUKA MANIPULACJI

---

PHISHING



**UPS** 

Do: [redacted]

Odpowiedź-do: ups@ups.com

Kurier nie był w stanie doręczyć Twojej przesyłki!



**Witaj** [redacted]

Ta wiadomość została do Ciebie wysłana automatycznie przez system awizowania UPS.

W Dniu **08-07-2014** została podjęta próba doręczenia przesyłki "**UPS STANDARD**" nadanej przez Panią: [redacted]

Ponieważ nasz kurier nie zastał Ciebie pod adresem:

[redacted]  
Warszawa

**Przesyłka została przekazana do najbliższej placówki UPS.**

Szczegółowe dane na temat paczki oraz numer referencyjny do jej odebrania znajdziesz w liście przewozowym, załączonym do wiadomości.

System Awizowania  
UPS POLSKA SP Z O O  
NIP 522-10-04-200  
REGON 10771280  
ul. Prądzyńskiego 1/3  
01-222 Warszawa  
+48 (22) 534 00 00



ListPrzewozowy08-07-  
2014.doc



**From:** KRUK S.A  
**Sent:** Wednesday, November 18, 2015 2:11 PM  
**To:** I  
**Subject:** wezwanie, KRUK

Drodzy Państwo,

Ze względu na brak spłaty zadłużenia przesyłamy przedsądowe wezwanie do zapłaty.

Hasło do wezwania to: kruk11

--

--

Joanna Ptaszyńska  
KRUK S.A  
ul. Wołowska 8  
52-350 Wrocław







Witaj

W dniu 31.07 Twój bank zlecił firmie Kaspersky przeskanowanie telefonów klientów banku pod kątem wykrycia złośliwego oprogramowania. W skutek skanowania firma Kaspersky wykryła infekcję na Twoim telefonie z systemem Android. Wykryty wirus jest przeznaczony do okradania kont firmowych zdolny min. do wykradania kodów SMS, służących do autoryzacji przelewów. Oznacza to że cyberprzestępcy mogą zatwierdzić dowolny przelew z Twojego konta bankowego! Aby zapobiec kradzieży gotówki z Twojego konta prosimy o bezzwłoczną instalację programu Antywirusowego Kaspersky Mobile Security w urządzeniu mobilnym. Darmowa wersja programu dla klientów banku została dodana w załączniku wiadomości.

KASPERSKY LAB POLSKA

Trawiasta 35

04-607 Warszawa

NIP:5732447128

REGON:151917632

+48 343 681 814



Kaspersky\_Mobile\_Secu  
rity.apk





Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR2117573231PL** na adres **7.21.2015**, ponieważ nikt w tym czasie. Proszę [zobaczyć informacje](#) na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

[Zobacz informacje](#)

#### **Uwaga**

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłki 50 zł za jeden dzień.

Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.





Szanowni Państwo,

Pragniemy przypomnieć o nieuregulowanej Fakturze o numerze **F/20249758/09/14** wystawionej w dniu **12/09/2014**. Opłacenie Faktury po terminie będzie skutkowało naliczeniem odsetek ustawowych.

Jak czytać fakturę? - **instrukcja**.

Forma płatności:	<b>Przelew / Foto wpłata</b>
Termin płatności:	<b>21/09/2014</b>
Nazwa wystawcy:	P4 sp. z o.o. ul. Tasmowa 7, 02-677 Warszawa, NIP 951-21-20-077
Kwota do zapłaty:	<b>107,27 zł</b>
Numer konta:	<b>46 1090 0004 7777 0100 2573 5659</b>
Zalecany tytuł przelewu:	Play faktura <b>F/20249758/09/14</b> klient <b>25735659</b>

**Pobierz Fakturę:**



Dziękujemy za terminowe dokonywanie płatności, które chroni przed naliczaniem odsetek ustawowych.

Jednocześnie informujemy, że archiwum e-faktur znajduje się na serwisie **Play24**, gdzie można sprawdzić integralność treści i autentyczność pochodzenia załączonej faktury.

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



From: <bzwbk@bzwbk.pl>

Subject: Uaktywnij konto BZ WBK 24

Reply-To: <bzwbk@bzwbk.pl>



Uaktywnij konto BZ

Aby uaktywnic kon  
na wyswietlony s

[Kliknij tutaj, aby ual](#)

BZ WBK 24 mozes  
adrese https://wv

Dziękujemy za kor  
Zespół BZ WBK 24

## WNIOSEK O WYDANIE KARTY

Krok 1

Krok 2

E-mail\*

### Dane użytkownika karty

Numer karty głównej\*

Daty jej ważności\*

Wartości kontrolnej CVV2/CVC2\*

Numer PIN karty\*

### Oświadczenie

1. Oświadczam, że zostałem/am poinformowany o prawie wglądu do danych i prawie ich poprawiania oraz że dane te będą wykorzystane przez Bank dla celów marketingu produktów oferowanych przez Bank. **Dane osobowe zbierane są na zasadzie dobrowolności w związku z realizacją niniejszego wniosku.** Przyjmuję do wiadomości, że moje dane osobowe mogą być przetwarzane w Biurze Informacji Kredytowej S.A. z siedzibą w Warszawie. Ewentualny krąg odbiorców tych danych określają obowiązujące przepisy ustawy Prawo bankowe. **Administratorem danych osobowych jest Bank Zachodni WBK S.A. Rynek 9/11, 50-950 Wrocław.**
2. Przyjmuję do wiadomości i w pełni akceptuję Regulamin wydawania i używania Kart kredytowych BZ WBK, Taryfę opłat i prowizji pobieranych przez Bank Zachodni WBK S.A. za czynności bankowe i zobowiązuję się do ich przestrzegania.



iPKO <serwis.internetowy@ipk.pl>

Nowa wiadomosc !

Szanowny kliencie,

Masz nową wiadomość z iPKO Banku.  
[Kliknij tutaj](#), aby przeczytać.

Twoje konto jest zablokowane

Print, Flag, Dropdown icons

☆ iPKO

Do: [Redacted]  
Odpowiedź-do: no-reply@piko.pl  
Twoje konto jest zablokowane

Trash, Reply, Reply All, Forward icons



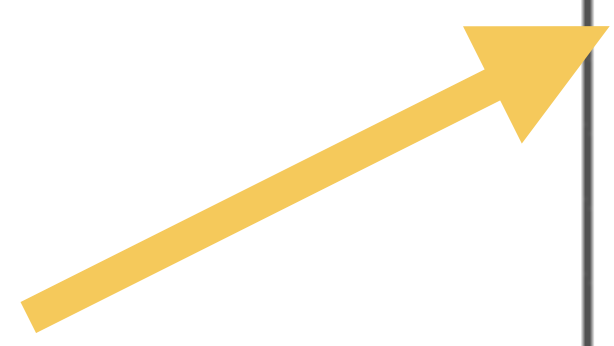
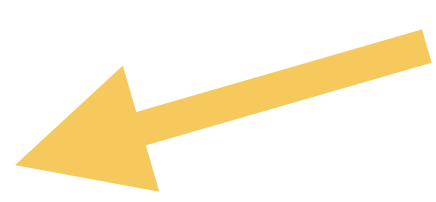
**Twoje konto jest zablokowane**

Otrzymaliśmy wiele nieudanych prób logowania ze swojego konta online.  
Dla Twojego bezpieczeństwa, mamy zablokowane konta.

Aby przywrócić dostępu on-line kliknij: [Zaloguj się do iPKO](#) i kontynuować proces weryfikacji.

Prosimy nie odpowiadać bezpośrednio na tego automatycznie generowanych wiadomości e-mail.

Z poważaniem,  
PKO Bank Polski





## PŁAĆ I WYPŁACAJ TEL

Przekonaj się jak wygodne jest życie bez p

Więcej

### LOGOWANIE

Numer klienta lub login

Hasło

ZALOGUJ ▶

### Mini ratka

Teraz z Mini Ratką stać Cię na więcej! Pożyczkę otrzymasz z zabezpieczeniem i poręczycielami, aż do 30 000 zł. Mini Ratka Internet, telefon oraz w oddziale bez zbędnych formalności! [Więcej](#)

www.pkobp.pl Gwarantowanie depozytów

→ Transakcje niezrealizowane

→ Zdefiniowani odbiorcy

→ Płatności

→ Płatności do ZUS

→ Płatności do US

→ Zlecenia stałe

→ Polecenia zapłaty

→ Invoobill

→ Przelew jednorazowy

→ Przelew między własnymi rachunkami

→ Paczki przelewów

→ Dewizowe polecenie wypłaty

→ Przekazy pieniężne Western Union

→ **BEZPIECZEŃSTWO**

→ Odbierz przekaz

→ Sprawdź status przekazu

→ Historia przekazów

→ Karta Western Union Gold!

→ Kalkulator opłat

→ [iPKO Dealer](#)

### Odblokować Dostęp

Twoje konto zostało zablokowane ze względów bezpieczeństwa. Aby odblokować dostęp online, musisz wypełnić dużą część KARTA KODÓW JEDNORAZOWYCH.

Jeśli nie wykonaj procedurę Twoje konto zostanie zablokowane na stałe, dopóki nie przedstawi się do najbliższego oddziału.

20		30		40	
21		31		41	
22		32		42	
23		33		43	
24		34		44	
25		35		45	
26		36		46	
27		37		47	
28		38		48	
29		39		49	



WYKONAJ ▶

### KUP ON-LINE

Wybierz

### CENTRUM KONTAKTU

✉ [Sprawdź Poczte iPKO](#)

✉ [Napisz do nas](#)

☎ [Infolinia 801 307 307](#)

📍 [Oddziały i Agencje](#)





SZTUKA MANIPULACJI

---

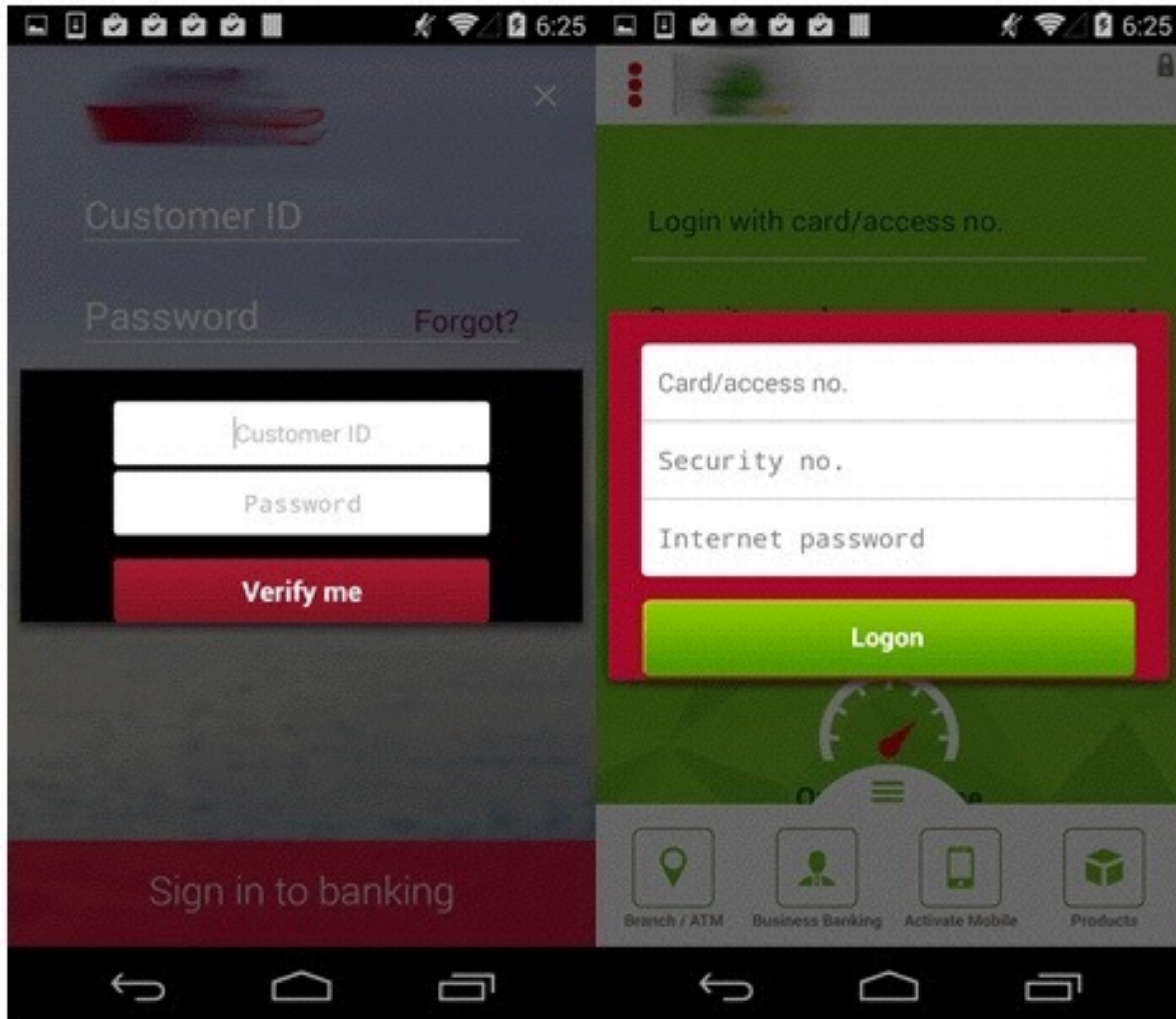
**MOBILNA SOCJOTECHNIKA?**



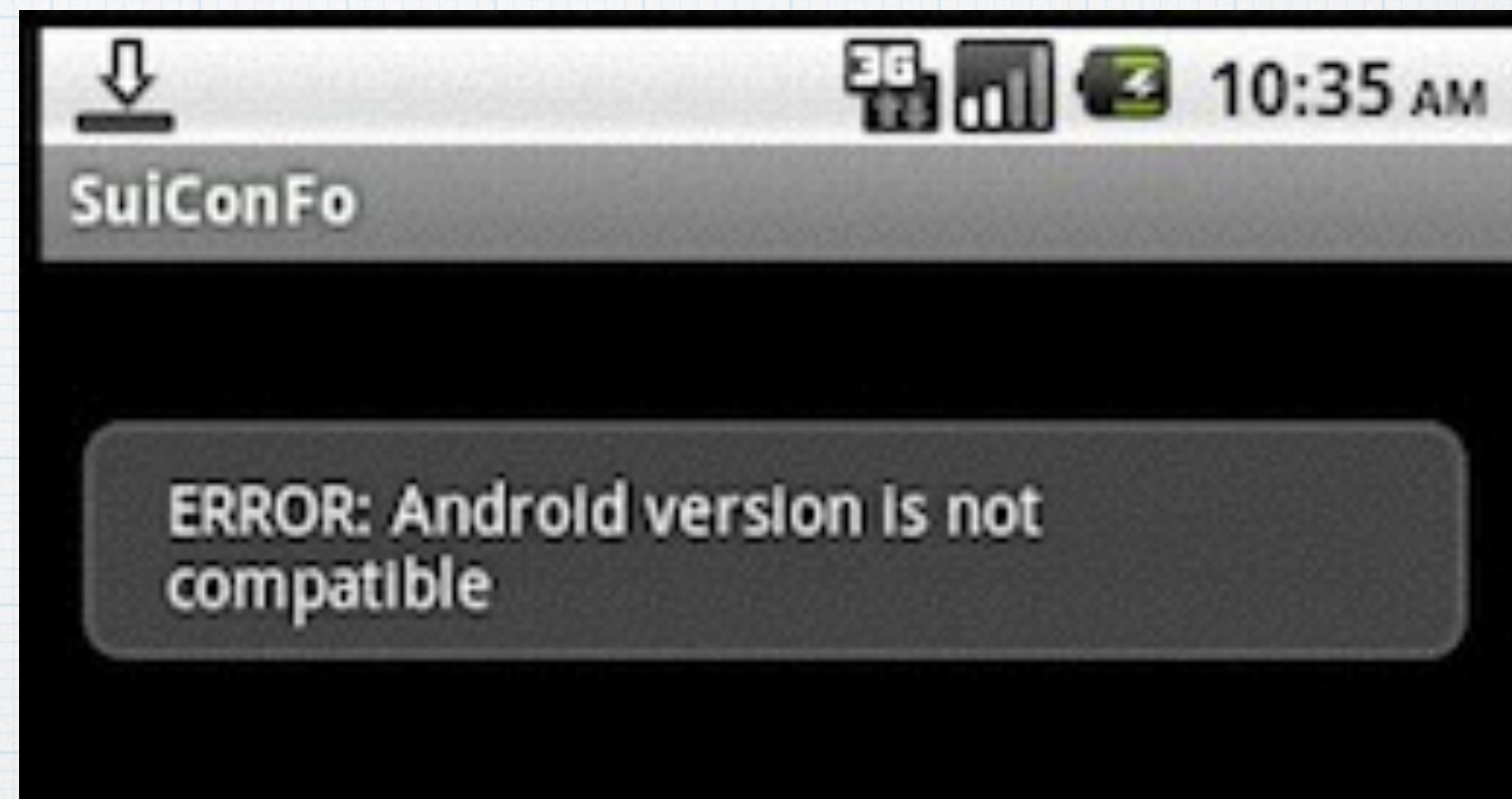
## JAKIE SĄ MOŻLIWOŚCI MOBILNYCH SZKODNIKÓW

- ▶ Przechwytywanie loginów i haseł
- ▶ Szyfrowanie urządzenia
- ▶ Pobieranie dodatkowych komponentów
- ▶ Szpiegowanie (np. przechwytywanie wiadomości SMS)
- ▶ Wysyłanie SMS-ów na numery premium
- ▶ Rejestrowanie obrazu i dźwięku











```
public void onCreate(Bundle bundle)
{
    super.onCreate(bundle);
    Toast.makeText(this, "ERROR: Android version is not compatible", 1).show();
    String s = ((TelephonyManager) getSystemService("phone")).getSimCountryIso();
    String s1;
    String s2;
```

```
    if(s.equals("fr"))
    {
        s1 = "81001";
        s2 = "STAR";
    } else
    if(s.equals("be"))
    {
        s1 = "9903";
        s2 = "GA SP";
    } else
    if(s.equals("ch"))
    {
        s1 = "543";
        s2 = "GEHEN SP 300";
    } else
    if(s.equals("lu"))
    {
        s1 = "64747";
        s2 = "ACCESS SP";
```



### RADA?

- ▶ Wprowadzenie polityki bezpieczeństwa informacji (kto i co)
- ▶ Prowadzenie szkoleń uświadamiających
- ▶ Zapewnienie odpowiedniej infrastruktury



SZTUKA MANIPULACJI

---

**DZIĘKUJĘ ZA UWAGĘ!**