Senior Bezpieczny w Sieci 2.0

Phishing i inne metody oszustw w internecie– nie daj się złapać

Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Kancelarii Prezesa Rady Ministrów

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021–2025. Edycja 2025

W tej prezentacji znajdziesz:

- Wprowadzenie do phishingu i oszustw internetowych
- Rodzaje oszustw internetowych
- Rozpoznawanie podejrzanych wiadomości i stron internetowych
- Metody unikania oszustw i praktyczne ćwiczenia

Co to jest phising?

Jest to rodzaj oszustwa internetowego, w którym oszuści podszywają się pod zaufane instytucje lub osoby, aby wyłudzić poufne informacje, takie jak hasła, numery kart kredytowych, czy inne dane osobowe.

Jak działa phishing?

Phishing działa na zasadzie wykorzystania naszego zaufania do znanych instytucji oraz presji czasu. Możecie otrzymać e-mail, który twierdzi, że Wasze konto zostanie zablokowane, jeśli natychmiast nie wprowadzicie pewnych danych. W rzeczywistości jest to tylko próba wyłudzenia informacji.

Najczęstsze formy phishingu

E-mail phishing

To oszustwo przez fałszywe e-maile. Wyglądają jak wiadomości od banku, sklepu, firm kurierskich czy urzędu. Zwykle proszą o podanie danych osobowych, kliknięcie w link lub zalogowanie się do konta.

Smishing

Oszustwo przez SMS – wiadomości podszywają się pod bank, firmę kurierską lub znajomego. Często proszą o kliknięcie w link lub podanie danych.

Najczęstsze formy phishingu

Spear phishing

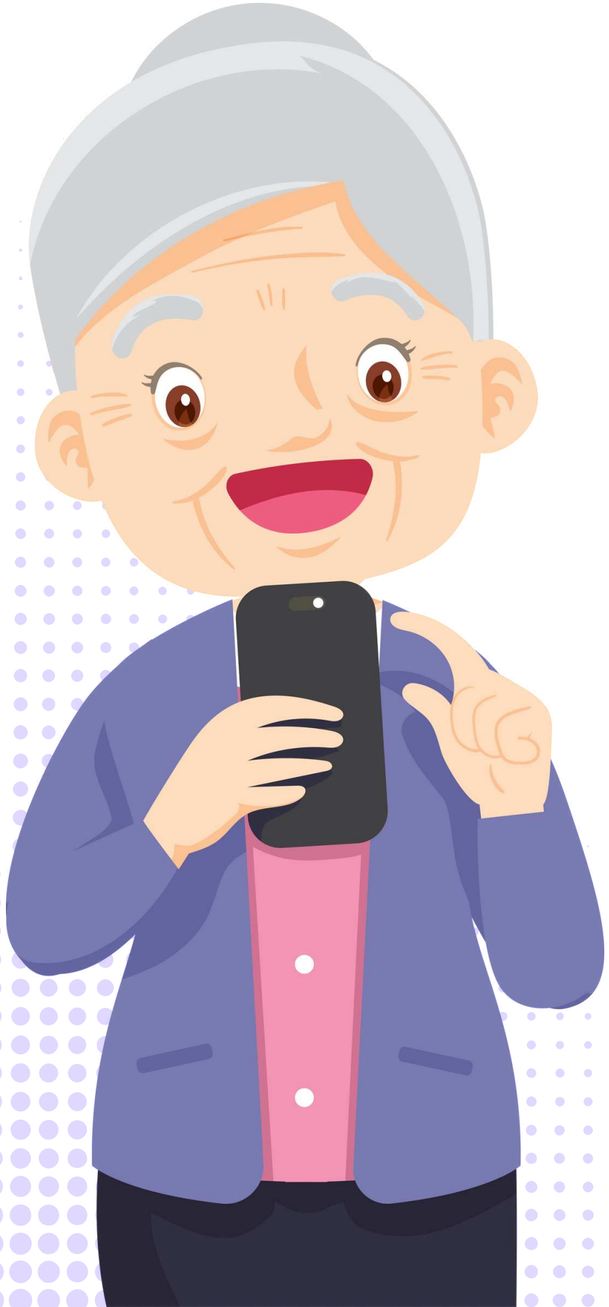
To bardziej osobiste oszustwo – e-mail lub wiadomość wygląda, jakby przyszła od znajomego, ale to podszyty oszust.

Vishing

Oszuści dzwonią i udają np. pracownika banku lub policjanta. Chcą wyłudzić hasła, numery kont lub inne dane.

Fałszywe strony internetowe

Otwierasz link, który wygląda jak strona Twojego banku lub sklepu. W rzeczywistości to strona oszusta, która kradnie Twoje dane.



Rodzaje oszustw internetowych

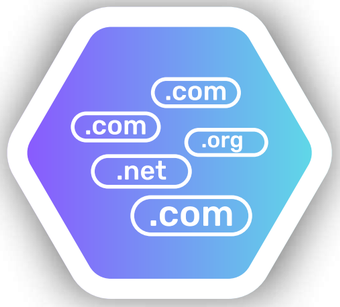
Metoda oszustw– Linki

Oszust wysyła do Ciebie wiadomość – może to być e-mail, SMS, wiadomość na Facebooku lub WhatsApp. W tej wiadomości znajduje się link, który wygląda jak coś ważnego albo ciekawego.

Metoda oszustw- Linki

Instalacja złośliwego oprogramowania

Fałszywe reklamy



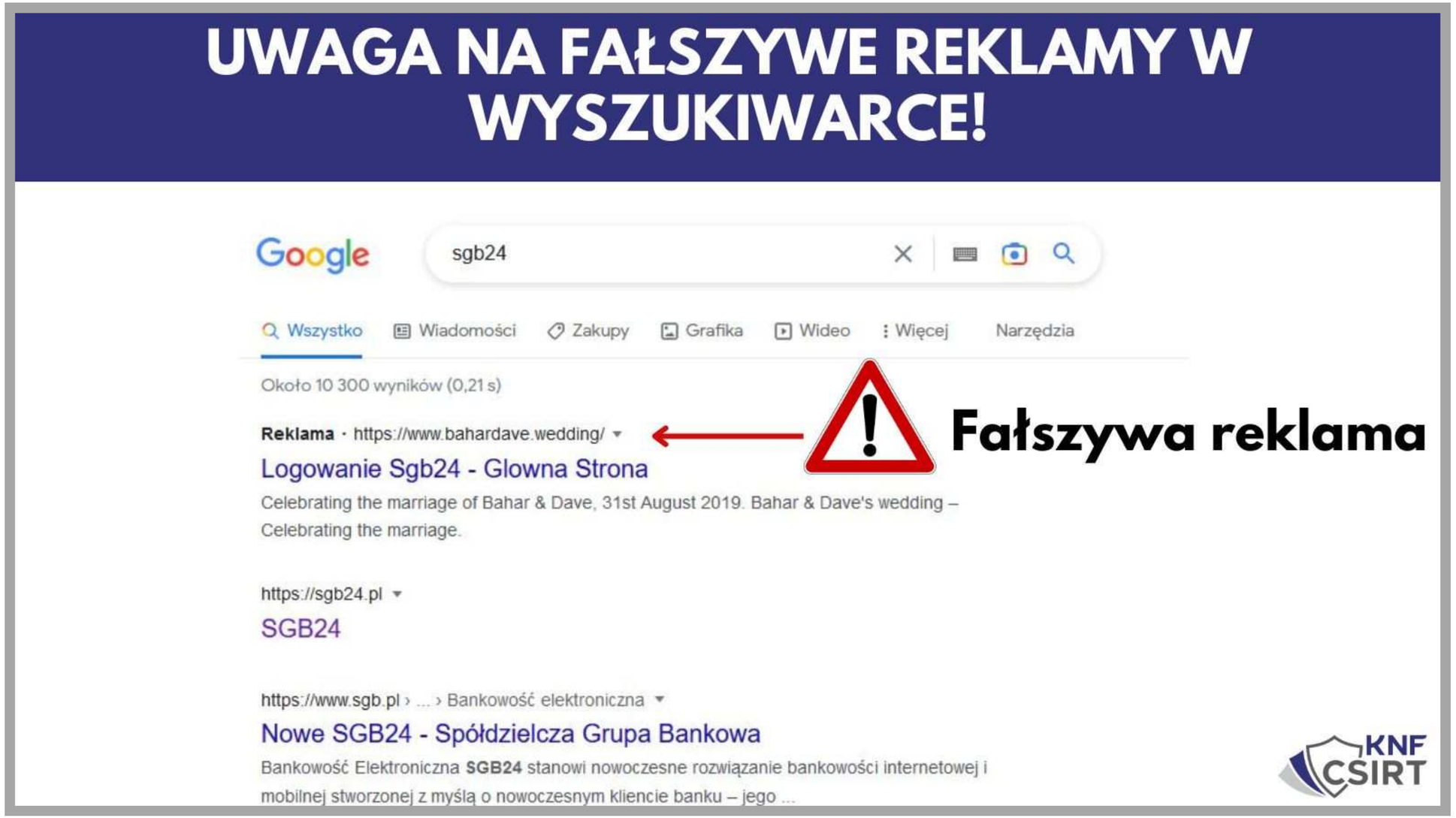
Fałszywe strony internetowe

Fałszywe strony banków i firm kurierskich

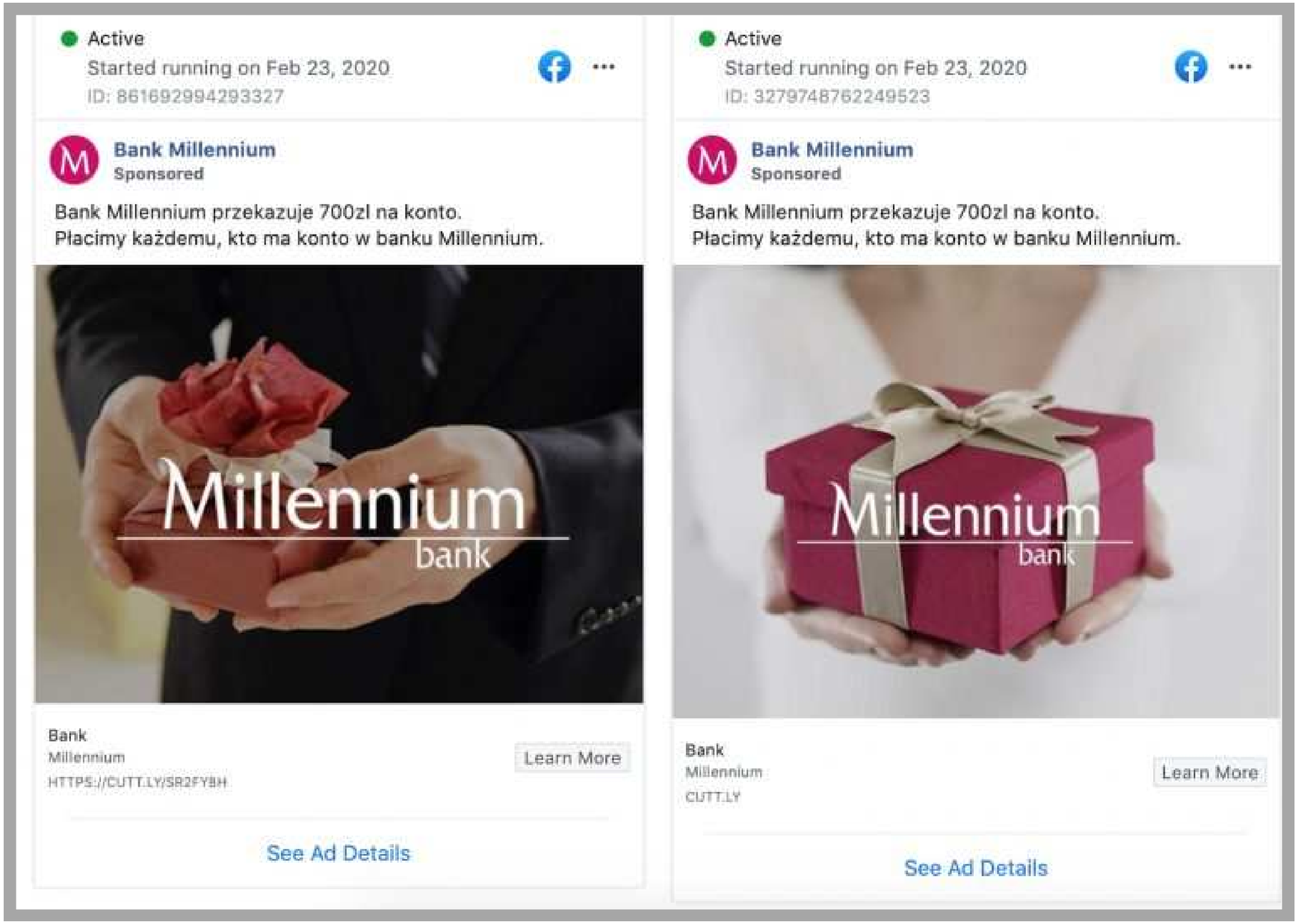
Jak się chronić?

- Nigdy nie klikaj w link, którego nie jesteś pewien
- Nie otwieraj linków z wiadomości od nieznajomych
- Sprawdzaj dokładnie adres strony
- Gdy masz wątpliwość – zapytaj kogoś z rodziny lub zadzwoń do firmy, której rzekomo dotyczy wiadomość.

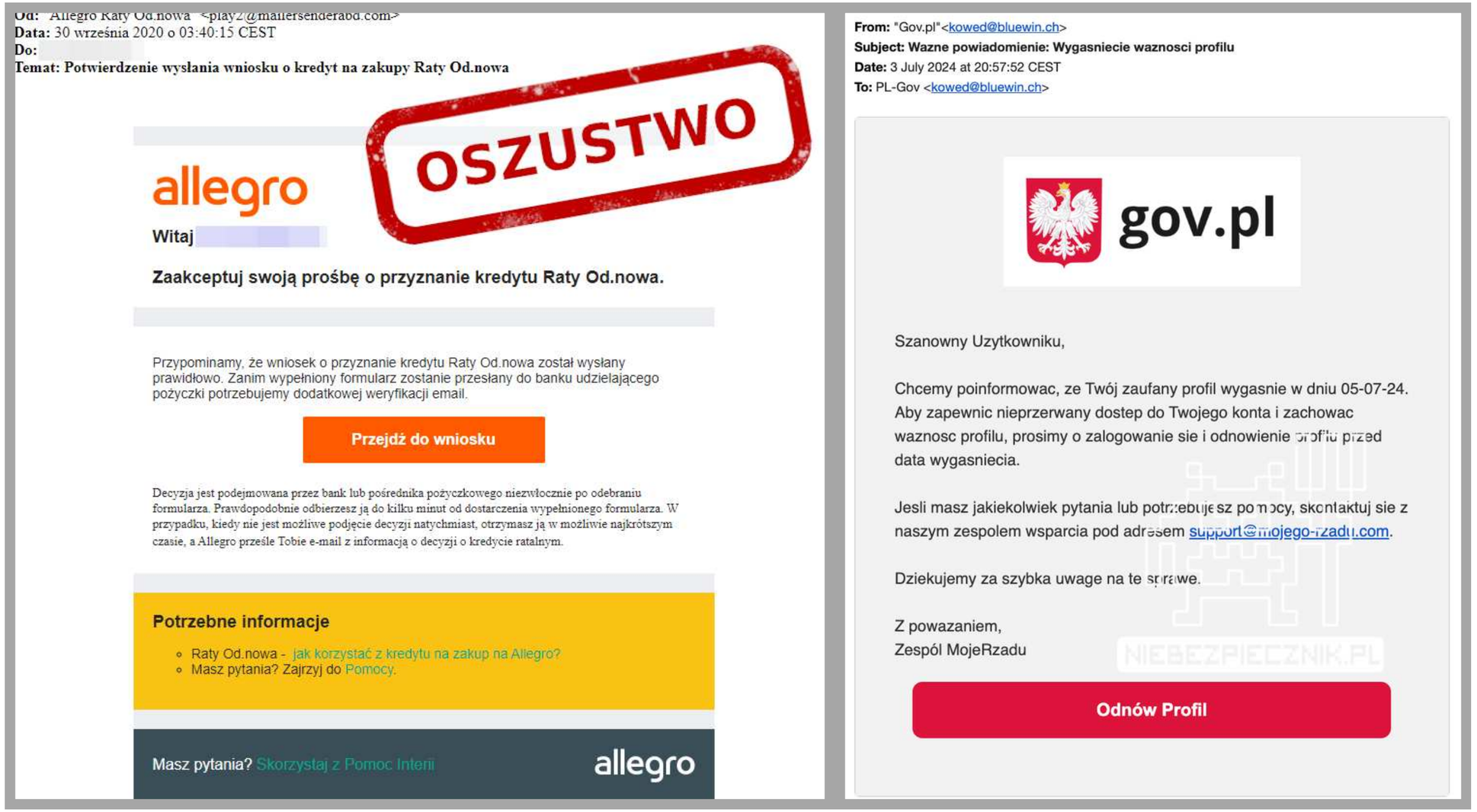
Fałszywe reklamy



Fałszywe reklamy na Facebooku



Fałszywa wiadomości mailowe



Od: "Allegro Raty Od.nowa" <play2@mailersenderabd.com>
Data: 30 września 2020 o 03:40:15 CEST
Do:
Temat: Potwierdzenie wysłania wniosku o kredyt na zakupy Raty Od.nowa

OSZUSTWO

allegro

Witaj

Zaakceptuj swoją prośbę o przyznanie kredytu Raty Od.nowa.

Przypominamy, że wniosek o przyznanie kredytu Raty Od.nowa został wysłany prawidłowo. Zanim wypełniony formularz zostanie przesłany do banku udzielającego pożyczki potrzebujemy dodatkowej weryfikacji email.

Przejdź do wniosku

Decyzja jest podejmowana przez bank lub pośrednika pożyczkowego niezwłocznie po odebraniu formularza. Prawdopodobnie odbierzesz ją do kilku minut od dostarczenia wypełnionego formularza. W przypadku, kiedy nie jest możliwe podjęcie decyzji natychmiast, otrzymasz ją w możliwie najkrótszym czasie, a Allegro prześle Tobie e-mail z informacją o decyzji o kredycie ratalnym.

Potrzebne informacje

- Raty Od.nowa - jak korzystać z kredytu na zakup na Allegro?
- Masz pytania? Zajrzyj do Pomocy.

Masz pytania? Skorzystaj z Pomoc Interii allegro

From: "Gov.pl"<kowed@bluewin.ch>
Subject: Wazne powiadomienie: Wygasniecie waznosci profilu
Date: 3 July 2024 at 20:57:52 CEST
To: PL-Gov <kowed@bluewin.ch>

gov.pl

Szanowny Uzytkowniku,

Chcemy poinformowac, ze Twój zaufany profil wygasnie w dniu 05-07-24. Aby zapewnic nieprzerwany dostep do Twojego konta i zachowac waznosc profilu, prosimy o zalogowanie sie i odnowienie profilu przed data wygasniecia.

Jesli masz jakiekolwiek pytania lub potrzebujesz pomocy, skontaktuj sie z naszym zespolem wsparcia pod adresem support@mojego-rzadu.com.

Dziekujemy za szybka uwage na te sprawe.

Z powazaniem,
Zespól MojeRzadu

Odnów Profil

Fałszywa wiadomości mailowe

AB

Administrator biznes.gov.pl <administrator@biznes.gov.pl>
To undisclosed-recipients:

Reply | Reply All

If there are problems with how this message is displayed, click here to view it in a web browser.

Biznes.gov.pl - NOWE POWIADOMIENIE.rar
68 KB

Biznes.gov.pl

Serwis informacyjno-usługowy dla przedsiębiorcy

Drogi Użytkowniku!

Załącznik to oficjalne powiadomienie elektroniczne od Biznes.gov.pl

Powiadomienie będzie dostępne na Twoim Autoryzowanym Koncie od 09-08-2022 do 09-17-2022. Jeżeli nie przystąpisz do jej lektury we wskazanym terminie, wywołane zostaną odpowiednie skutki, zgodnie z obowiązującymi przepisami.[Art. 46 Kodeksu postępowania administracyjnego.]

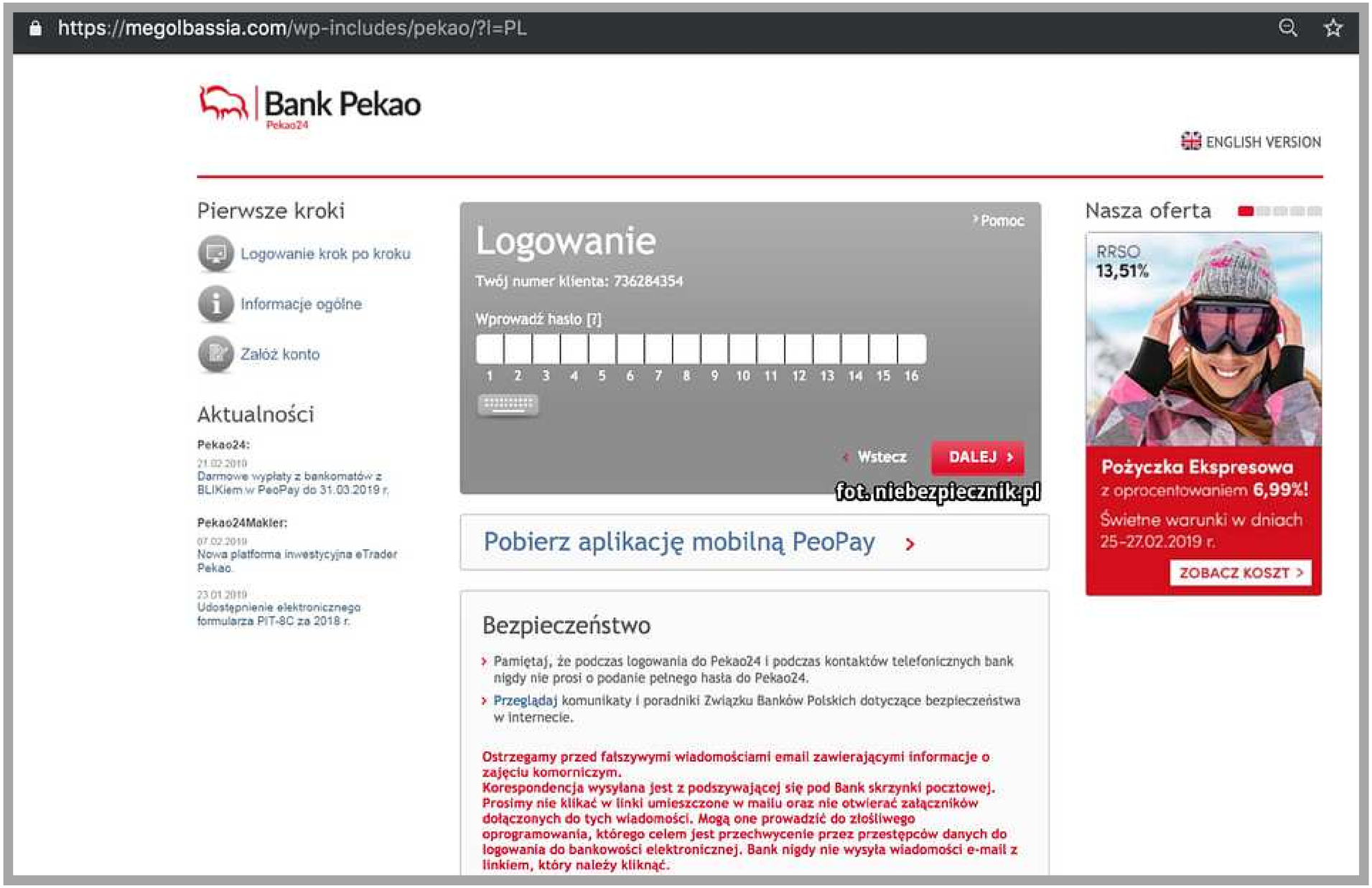
Wiadomość została wygenerowana automatycznie przez serwis biznes.gov.pl (prosimy na tę wiadomość nie odpowiadać).

Pozdrawiamy,
Zespół Biznes.gov.pl

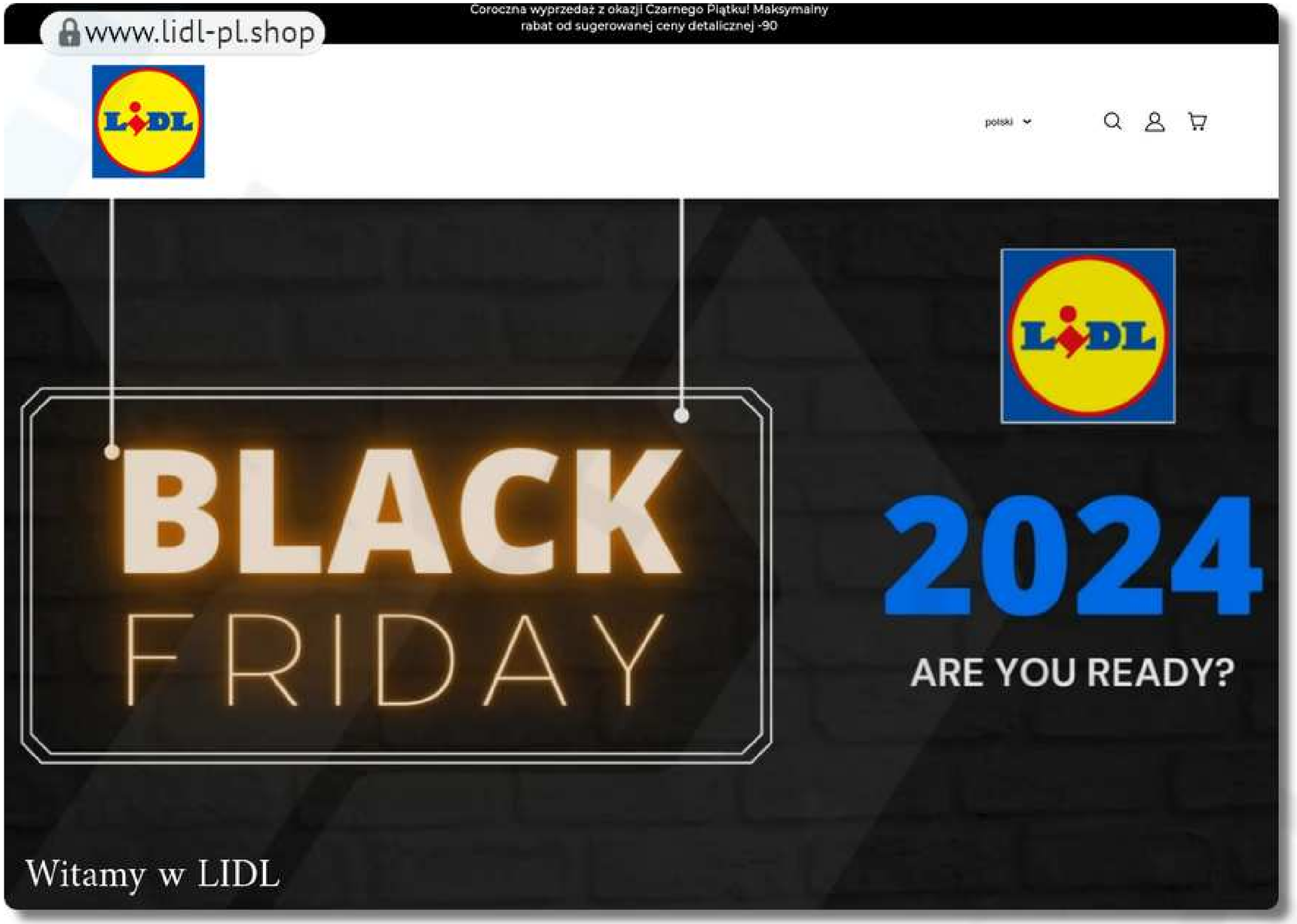
gov.pl / Biznes.gov.pl

Portal Biznes.gov.pl to źródło informacji o usługach, które administracja świadczy dla osób prowadzących i planujących rozpocząć działalność gospodarczą. W razie pytań możesz skorzystać z Centrum Pomocy.

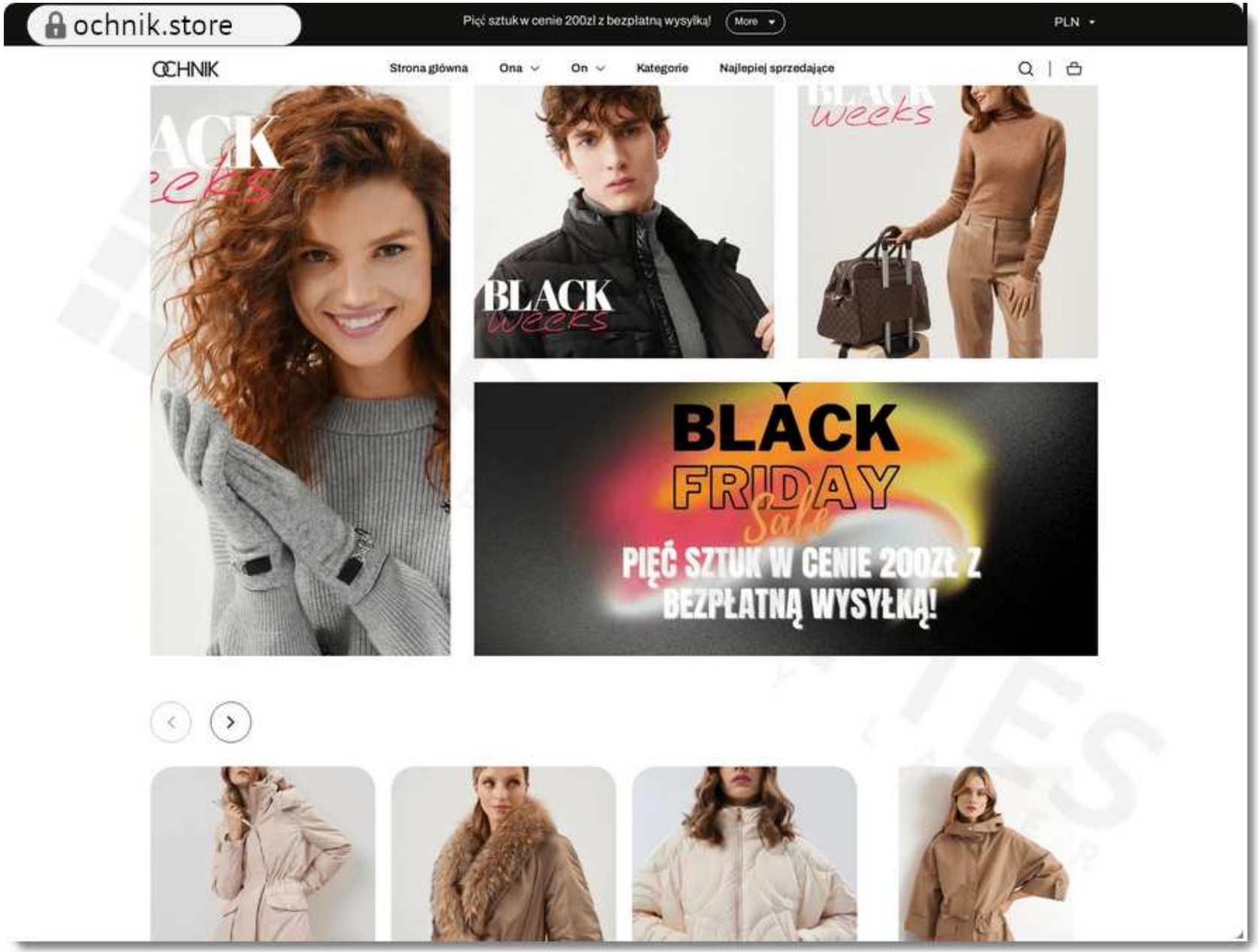
Fałszywa strona banku



Fałszywe strony internetowe



Fałszywe strony internetowe



Metoda na “wnuczka”

Oszustwo metodą "na wnuczka" to popularny schemat przestępczy, w którym oszuści wykorzystują zaufanie osób starszych, podszywając się pod członków rodziny lub funkcjonariuszy policji.

Schemat działania– Metoda na “wnuczka”

Krok 1:
Przedstawienie się rozmówcy jako bliska osoba, informująca o sytuacji wymagającej natychmiastowej pomocy finansowej

Krok 2:
W trakcie rozmowy oszust stara się zmanipulować emocjonalnie ofiarą , aby działała bez zastanowienia

Krok 3:
Po zdobyciu zaufania, oszust informuje że nie może odebrać pieniędzy osobiście i prosi o przekazanie pieniędzy wydelegowanej osobie

Metoda oszustwa– “nigeryjski przekręt”

Nigeryjski przekręt to rodzaj oszustwa internetowego, które polega na wciągnięciu ofiary w fikcyjny transfer dużej sumy pieniędzy. Przestępcy często kontaktują się z ofiarami za pośrednictwem e-maila, oferując udział w rzekomym transferze ogromnych kwot, co zazwyczaj kończy się wyłudzeniem pieniędzy

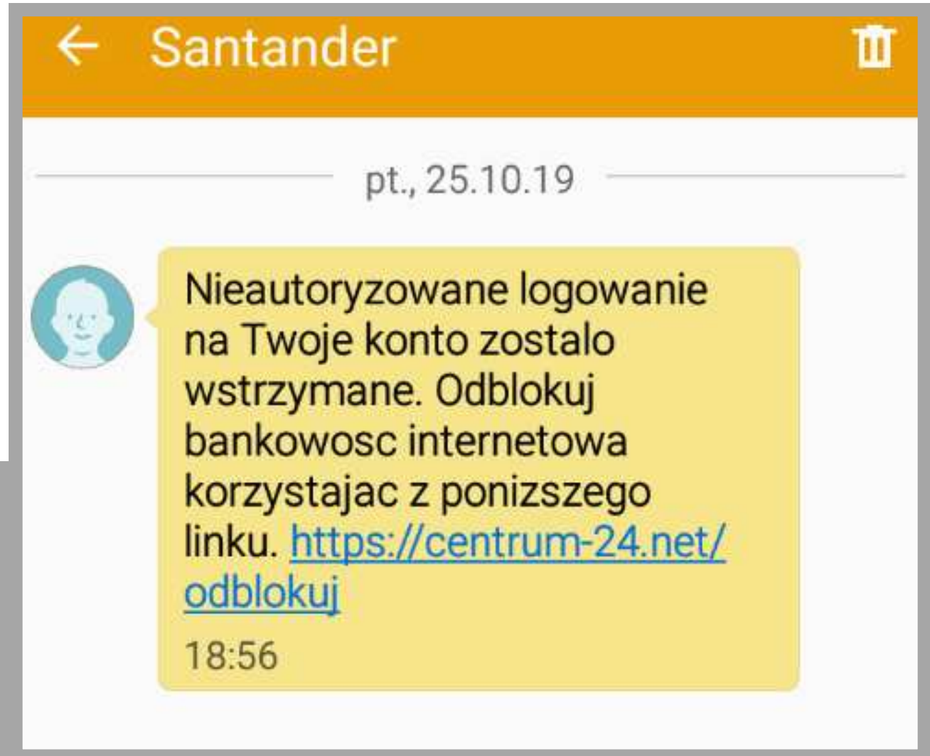
Rodzaje “nigeryjskich przekrętów”

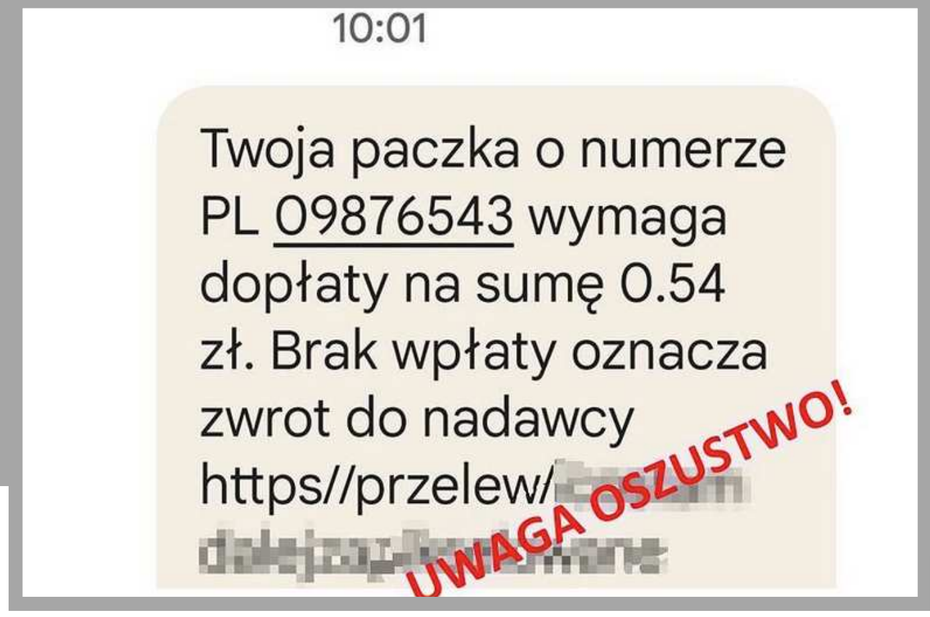
- Na uchodźcę politycznego
- Na inwestora
- Na wygraną na loterii
- Na konta bez właściciela
- Na spadek

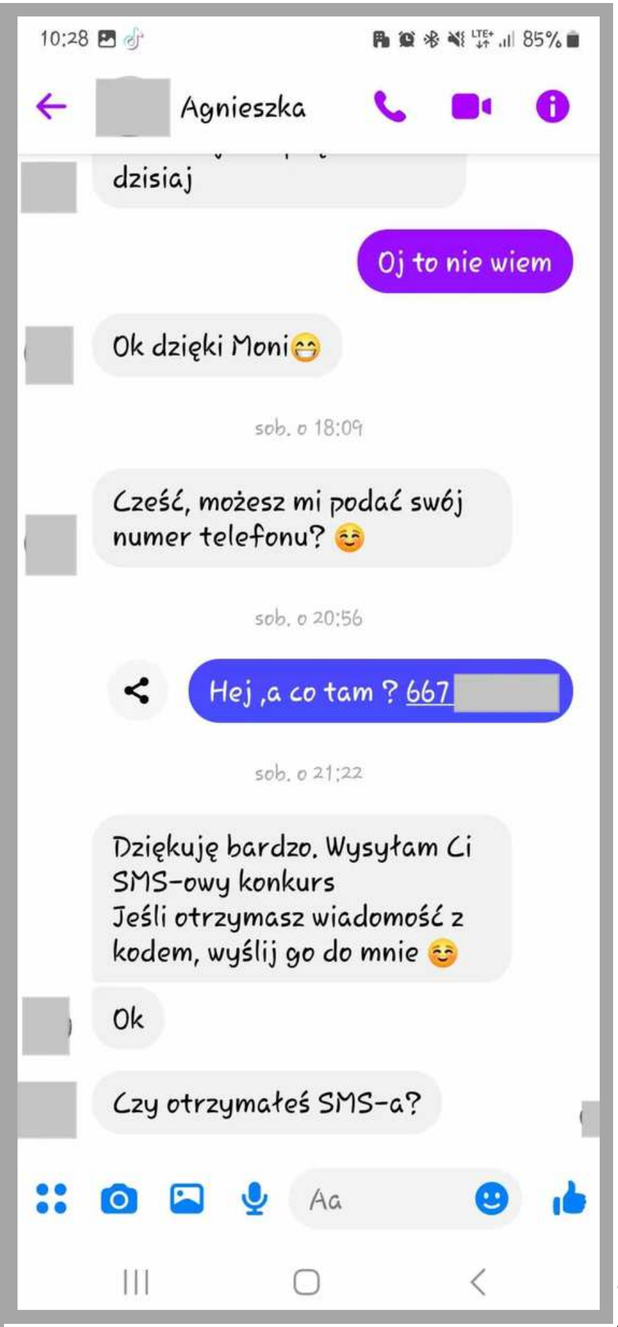
Jak rozpoznać fałszywe SMS-y z linkami

- **Podejrzane linki**: Linki z literówkami lub dziwnymi domenami.
- **Presja czasu**: Wiadomości, które zmuszają do natychmiastowego działania.
- **Prośby o pieniądze**: Wiadomości proszące o szybkie przelewy lub pożyczki.
- **Informacje o nagłych sytuacjach**: Wiadomości dotyczące rzekomych problemów z paczkami czy płatnościami

Fałszywe SMS-y





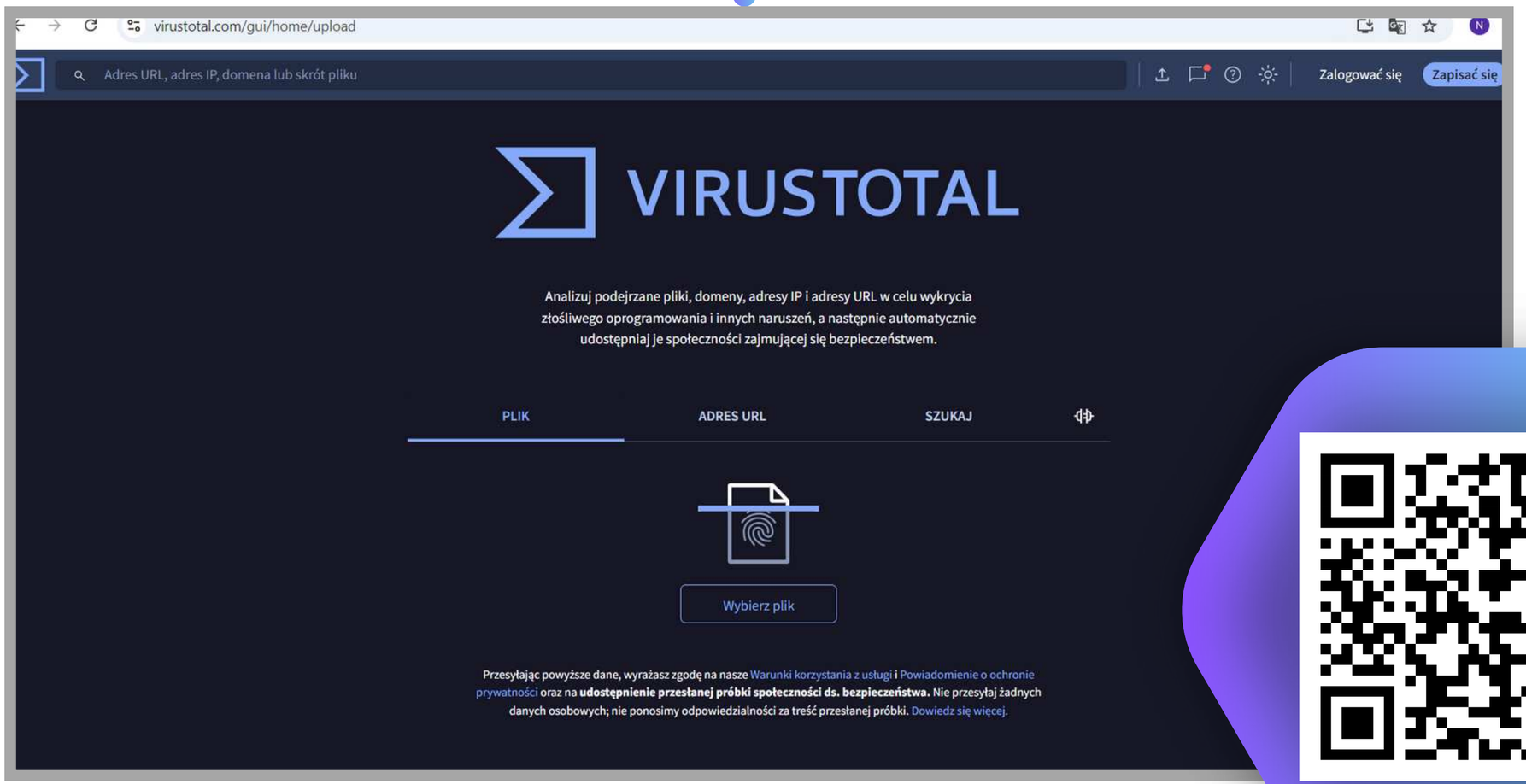


Narzędzia do sprawdzania linków

Narzędzia do sprawdzania linków

- Dostępne są serwisy internetowe takie jak: VirusTotal, PhishTank lub Google Transparency Report, które skanują linki pod kątem potencjalnych zagrożeń
- Narzędzia te analizują linki przy użyciu wielu silników antywirusowych i baz danych, dostarczając informacji o złośliwych oprogramowaniach

Virus Total


virustotal.com/gui/home/upload
Adres URL, adres IP, domena lub skrót pliku
Zalogować się
Zapisać się
VIRUSTOTAL
Analizuj podejrzane pliki, domeny, adresy IP i adresy URL w celu wykrycia złośliwego oprogramowania i innych naruszeń, a następnie automatycznie udostępniaj je społeczności zajmującej się bezpieczeństwem.
PLIK
ADRES URL
SZUKAJ
Wybierz plik
Przesyłając powyższe dane, wyrażasz zgodę na nasze Warunki korzystania z usługi i Powiadomienie o ochronie prywatności oraz na udostępnienie przesłanej próbki społeczności ds. bezpieczeństwa. Nie przesyłaj żadnych danych osobowych; nie ponosimy odpowiedzialności za treść przesłanej próbki. Dowiedz się więcej.

Cechy charakterystyczne podejrzanych wiadomości

Błędy językowe

Wiele wiadomości phishingowych zawiera błędy gramatyczne, interpunkcyjne oraz ortograficzne

Nieznany nadawca

Często oszuści używają adresów, które przypominają prawdziwe, ale mają subtelne różnice

Bezosobowe powitanie

Wiadomości zaczynające się od "Drogi Kliencie" zamiast imienia i nazwiska powinny wzbudzić Twoją czujność

Pilność i presja czasu

Wiadomości, które nakłaniają do szybkiego działania są często próbą wyłudzenia informacji

Jak postępować w przypadku podejrzanych wiadomości

Nie klikaj w link

Zweryfikuj informacje

Zgłoś oszustwo

Polub nas na Facebooku!

Skorzystaj z naszej CYBERLINII

Kiedy:

poniedziałek, środa i piątek
10:00–13:00
Tel: +48 579 519 688

KONTAKT

Społeczna Grupa Medialna

tel. +48 579 519 688

e-mail seniorzy@mediagroup.org.pl

mediagroup.org.pl

Ul. Marszałkowska 31, 42-400 Zawiercie

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021–2025. Edycja 2025