

Senior Bezpieczny w Sieci 2.0

Rodzaje zagrożeń w sieci — jak nie dać się oszukać

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:

- Rodzaje zagrożeń w sieci
- Bezpieczne strony internetowe i rozpoznawanie oszustw
- Bezpieczne korzystanie z urządzeń mobilnych i komputerów
- Ochrona przed wirusami i zagrożeniami

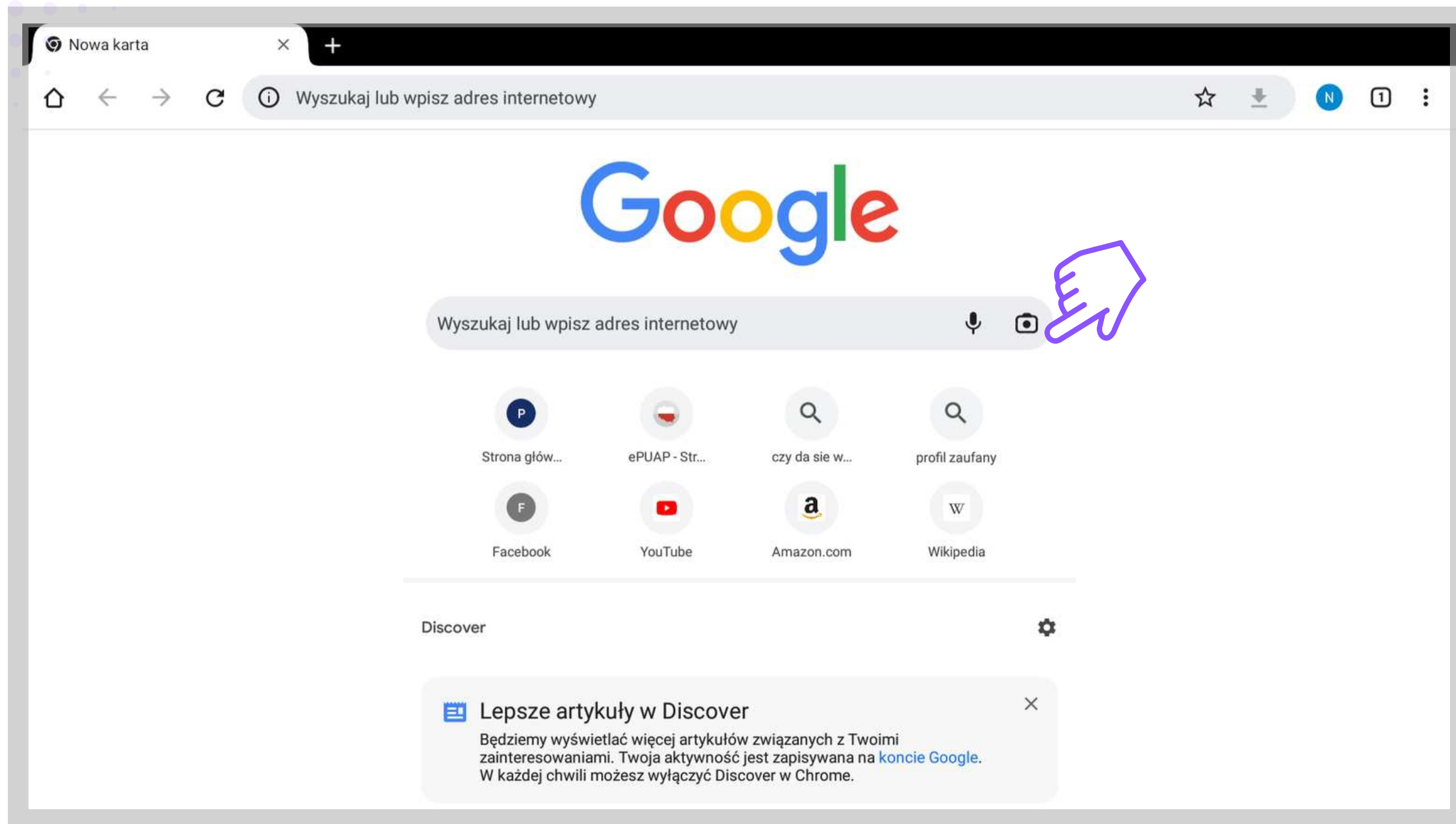


Obiektów Google



Jak uruchomić Obiektów Google?

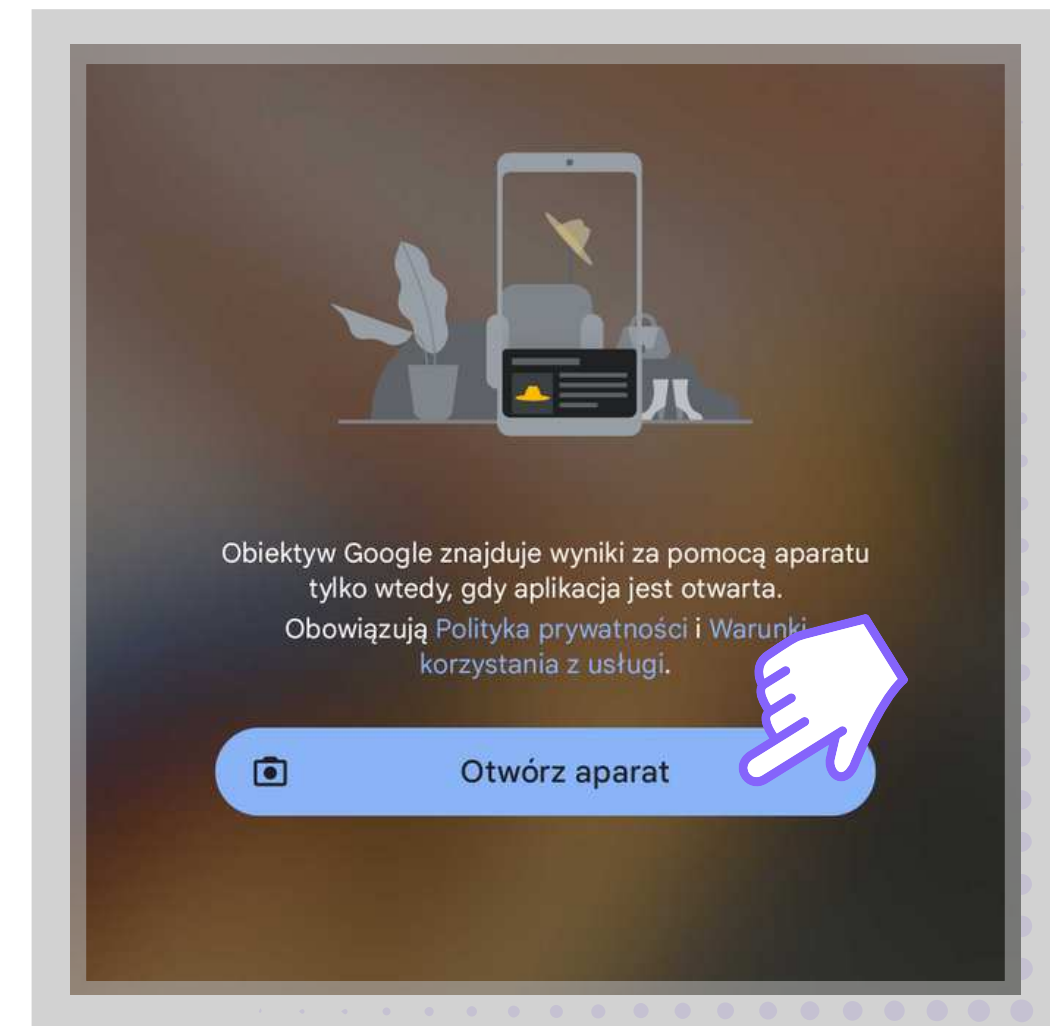
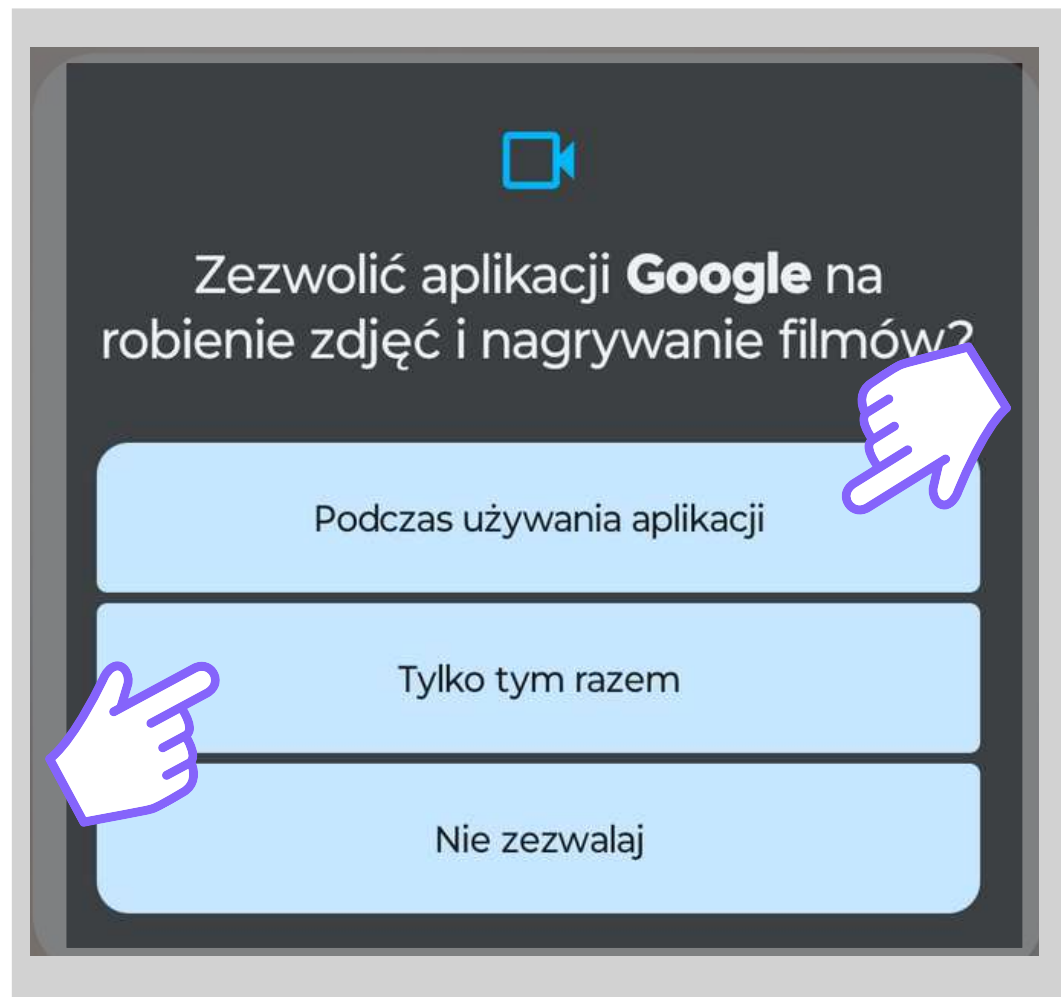
1. Kliknij ikonę małego obiektu w pasku wyszukiwania po prawej stronie, obok mikrofonu



Jak uruchomić Obiektów Google?

2. Jeżeli pojawi się komunikat dotyczący zezwolenia aplikacji Google na robienie zdjęć i nagrywanie wideo wybieramy opcję Podczas używania aplikacji lub Tylko tym razem

3. Następnie kliknij przycisk Otwórz aparat



Jak uruchomić Obiektyw Google?

4. Po włączeniu Obiektywu Google, skieruj aparat telefonu na kod QR. Gdy na ekranie pojawi się link, dotknij go – otworzy się formularz Google



Sprawdź swoją wiedzę!



Czym jest zagrożenie w sieci?



Zagrożenie w sieci to różnorodne formy oszustw i ataków, których celem jest wykorzystanie naszej nieuwagi lub nieznanomości zasad bezpiecznego korzystania z internetu. Ich głównym celem są pieniądze, dane osobowe lub infekowanie naszych urządzeń.

Rodzaje zagrożeń



PHISING

metoda, w której oszust podszywa się pod znaną firmę lub instytucję, próbując wyłudzić poufne informacje



RANSOMWARE

rodzaj złośliwego oprogramowania, infekującego oraz blokującego system komputerowy poprzez zaszyfrowanie wybranych plików. Często okno lub plik zawierający instrukcję odszyfrowania, sugeruje, że odzyskanie danych możliwe jest wyłącznie po wpłacie określonej kwoty na konto atakującego.

Rodzaje zagrożeń

NIEBEZPIECZNE LINKI I ZAŁĄCZNIKI



Niebezpieczne linki mogą prowadzić do stron zawierających wirusy lub złośliwe oprogramowanie, a załączniki mogą zainfekować nasze urządzenie po otwarciu

FAKE NEWS



Fake newsy to fałszywe informacje rozpowszechniane w sieci w celu manipulacji opinią publiczną, wywoływania paniki lub zysków finansowych.

Przykład ransomware



Przykład phishingu



Od: PUESC Polska <refundacja@puesc-pl.eu>

Data: 4 kwietnia 2023

Dw: PUESC Polska <refundacja@puesc-pl.eu>

Temat: Potwierdzenie zatwierdzonego wniosku o zwrot podatku za okres od stycznia 2023 do marca 2023

Drogi Obywatelu,

Mamy zaszczyt poinformować, że Pański wniosek o automatyczny zwrot podatku za okres od stycznia 2023 do marca 2023 został pomyślnie zatwierdzony.

Aby odebrać zwrot podatku, proszę odwiedzić najbliższe biuro administracji podatkowej i przedstawić swoje dane identyfikacyjne lub zalogować się na nasz portal internetowy poprzez skanowanie poniższego kodu QR:



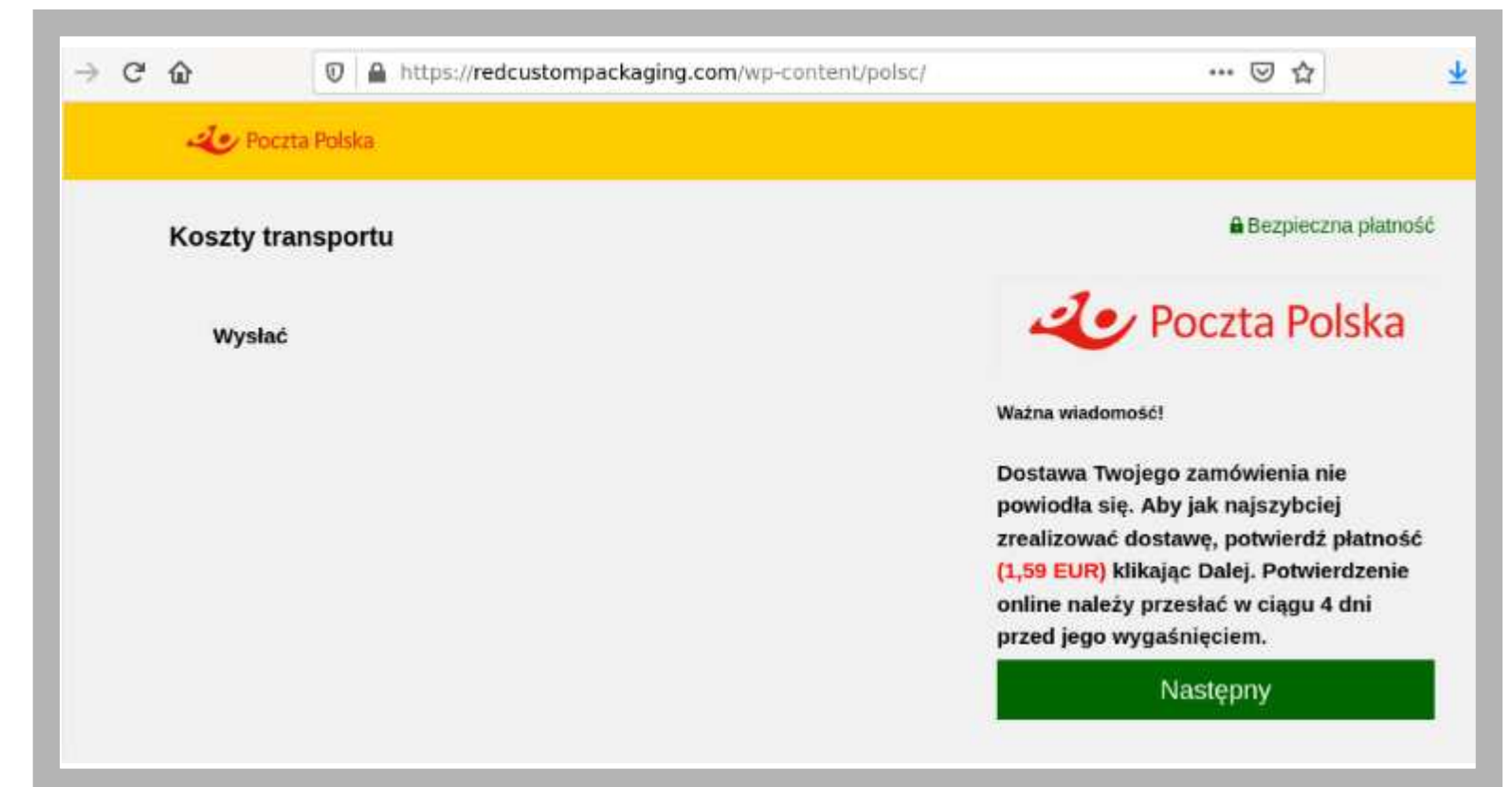
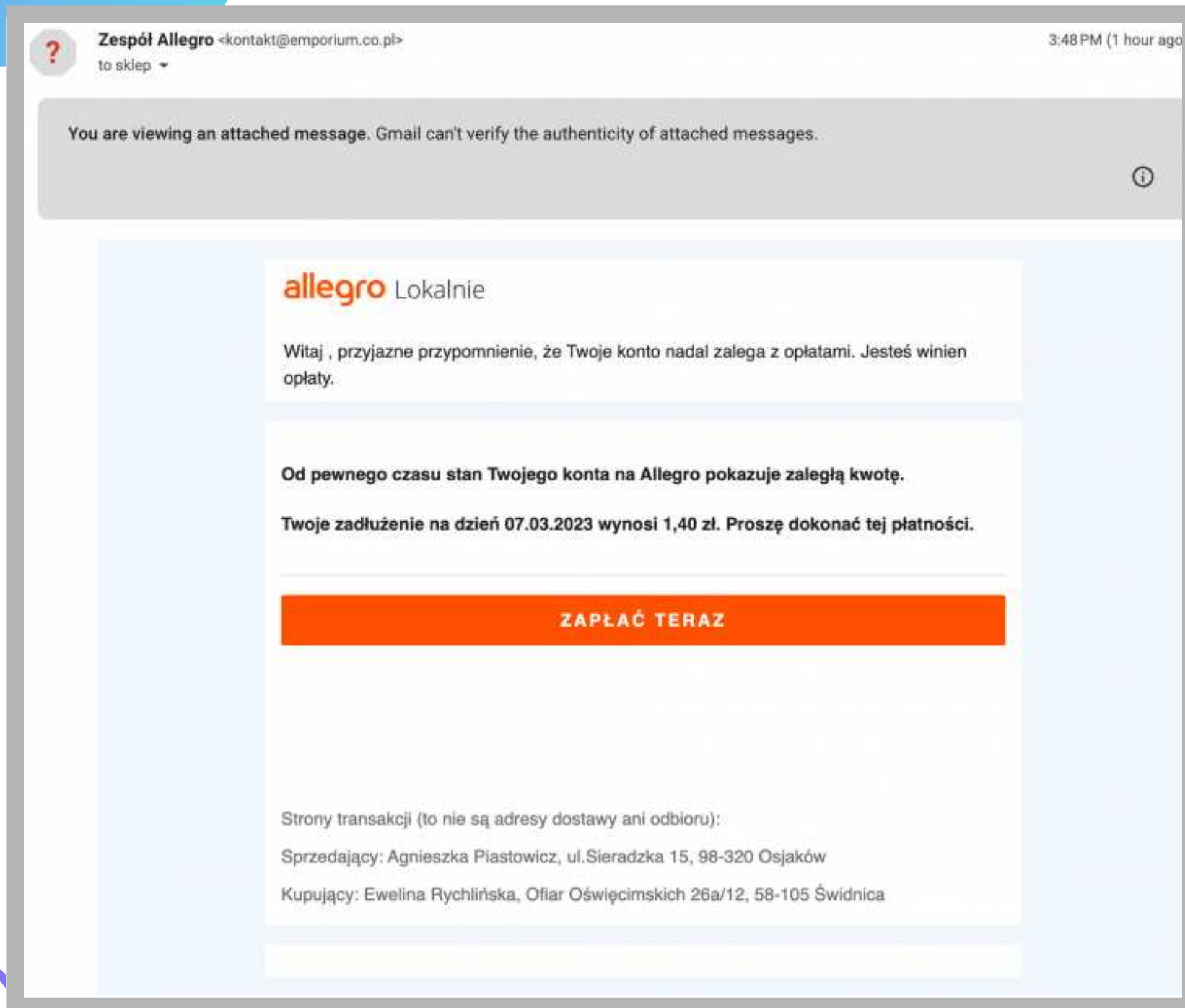
Prosimy o użycie tymczasowego hasła 6 [redacted] 9 podczas logowania.

Zwracamy uwagę, że tymczasowe hasło wygaśnie 24 godziny po otrzymaniu tej wiadomości, jako środek ostrożności mający na celu zapewnienie bezpieczeństwa transakcji.

Jeśli mają Państwo jakieś dodatkowe pytania lub potrzebują pomocy, prosimy o kontakt z nami.

Z poważaniem,
PUESC Polska

Przykład phishingu



Fałszywe kody QR



 **Kraków**

Strefa A

Opłata za miejsce parkingowe/Parking fee

Numer rejestracyjny/Registration number

Ilość godzin parkowania samochodu/Number of hours of car parking

Akceptujemy karty/We accept cards:  

Numer karty*/Card number*

Data wygaśnięcia*/Expiration date*

CVV*:

ZAPŁAĆ





Nie skanuj kodów QR umieszczonych na parkomatach!

Na niektórych krakowskich parkomatach pojawiły się naklejki zachęcające do płatności za parkowanie z wykorzystaniem kodów QR. Jest to oszustwo, które objęte zostało już policyjnym śledztwem.

Pracownicy ZDMK usuną naklejki, po zabezpieczeniu śladów przez policję. Do tego czasu prosimy o ich pozostawienie na urządzeniach i zgłoszenie pod numerem: 12 616 71 77 lub 12 616 75 55.

Przykład oszustwa sms-owego



← 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](https://aliorbank.pl)

← iga.swiatek



Iga Swiatek
iga.swiatek

1.7 followers · 116 posts

Today 23:25

Witaj rodaku tu Iga Swiatek pisze z drugiego konta i potrzebuje pomocy nie mam pieniędzy na samolot powrotny do Polski . Pozycz mi prosze swoja karte kredytowa Jest tu ze mna Robert Lewandowski



Cześć tu Robert Lewandowski

Double-tap to like



Message...



Text Message
Today 7:43 pm

Profil Zaufany - Twoje zlecenie pożyczki pienieznej w kwocie 20.000 PLN zostało przyjęte, pieniądze zostaną wypłacone w ciągu 60 minut. Możliwość anulowania zlecenia przez internet <https://profilzaufany.online/profil/>

iMessage
Dzisiaj, 16:02

Twoja faktura nie została w pełni opłacona. Prosimy o dopłatę 1 zł do dnia 22.11.2018 lub Twój numer zostanie zablokowany

ulink.pl



iMessage

9-5 12:29

Twoja paczka czeka w Paczkomacie WRO...
... . Kod odbioru ... QR kod <http://paczkomaty.pl> Do zobaczenia!

16:17

Wysyłka pod wskazany adres jest droższa. Prosimy dopłacić 1 PLN, brak dopłaty oznacza anulowanie zamówienia.
<http://in3post.tk/b6s5avv/1>



SMS



Przykład fake news



🚨 DRAMATYCZNE CHWILE 🚨

Cała Polska zmaga się teraz z ogromną powodzią 🤔. Sytuacja jest krytyczna - woda zalała w miejscowości, a mieszkańcy tracą nadzieję.

💔 DZIEWCZYNNKA WPADŁA DO RZEKI 💔

Właś... Wyświetl więcej



BLOGOWACBLOG.REST

Powódź w Warszawie. Dziewczynka wpadła do rwącej rzeki, trwa akcja ratunkowa
Tragedia

Aurelia [redacted]

13 godz. · 🌐

Śmiertelny wypadek w parku rozrywki "Energylandia" 8 osób zostało rannych!
Moment wypadku został nagrany przez świadków i opublikowany na stronie:
[WIDEO] <http://uwagatvn.waw.pl>



at/Julian Bellinger via Storyful

Przykład fake news



Wiadomości



Życie Omeny Mensah już nigdy nie będzie takie samo. Jej ostatnie słowa.

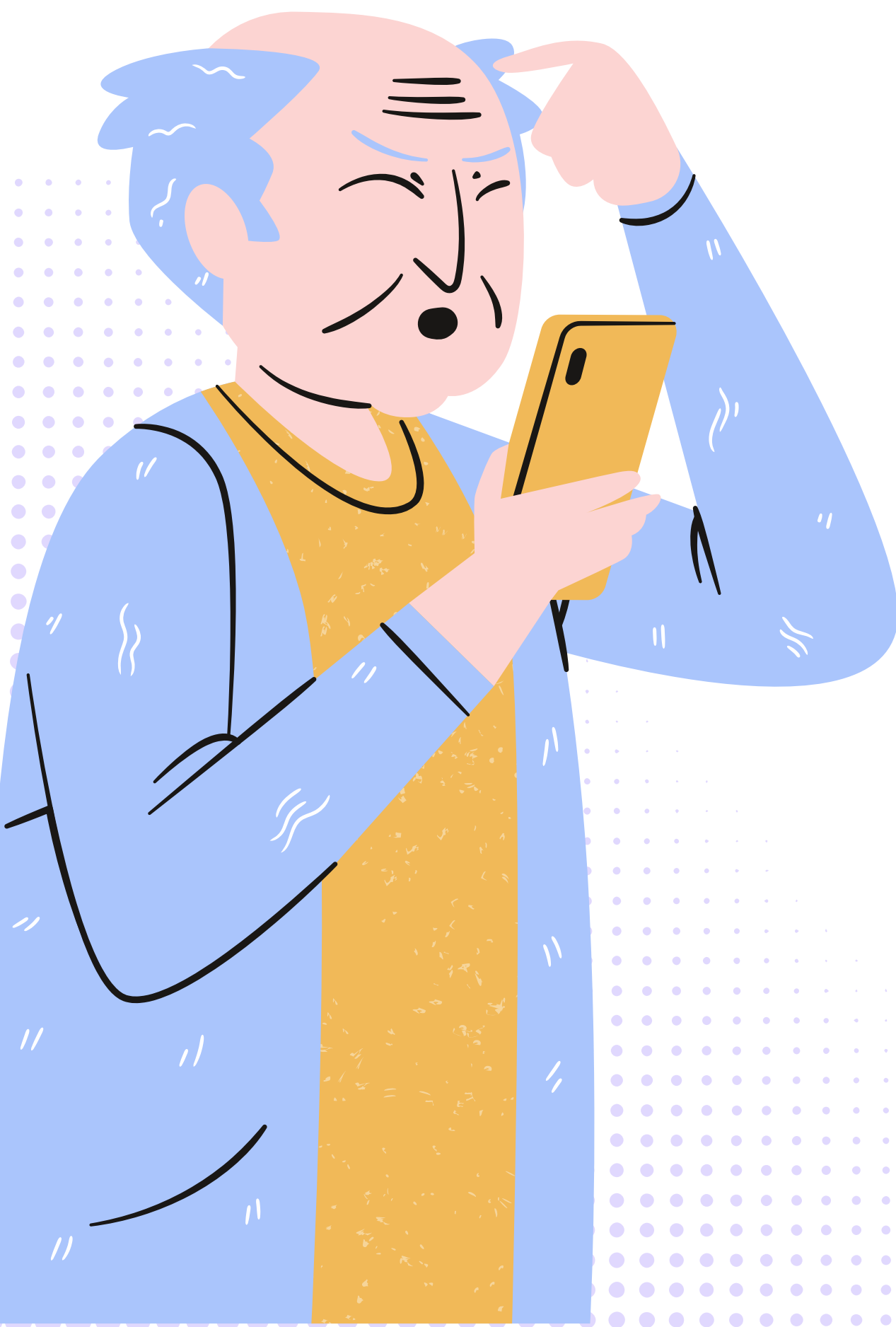
Magdalena [redacted]
10 lipca o 04:01 · 🌐

Magda Gessler Nie ŻYJE !
Prokuratura ze względu na bezpieczeństwo...
<http://kuchnia-gessler.waw.pl> [WIDEO +18]



😱👍🙄 41

56 udostępnień



Jak rozpoznać oszustwa internetowe?

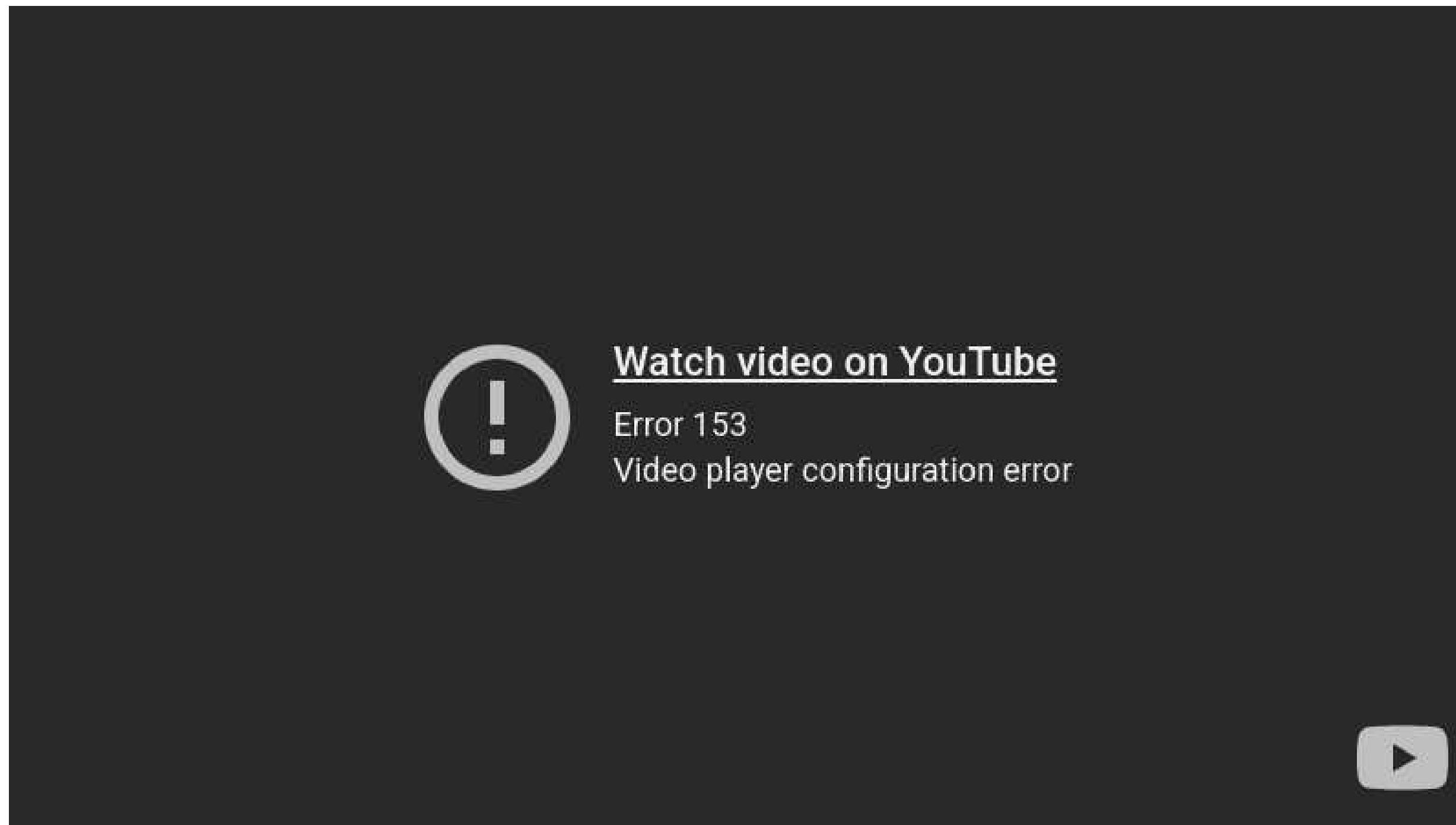
Jak rozpoznać oszustwa internetowe?

Zwracanie uwagi
na język i styl
wypowiedzi

Sprawdzanie
adresów e-mail i
linków

Nie podawanie
poufnych danych
przez e-mail lub
SMS.

Trzy mity bezpieczeństwa w sieci



Have I Been Pwned

Who's Been Pwned Passwords Notify Me API Pricing About ▾

Dashboard

Have I Been Pwned

Check if your email address is in a data breach

Check

Using Have I Been Pwned is subject to the [terms of use](#)





BEZPIECZNE STRONY INTERENTOWE



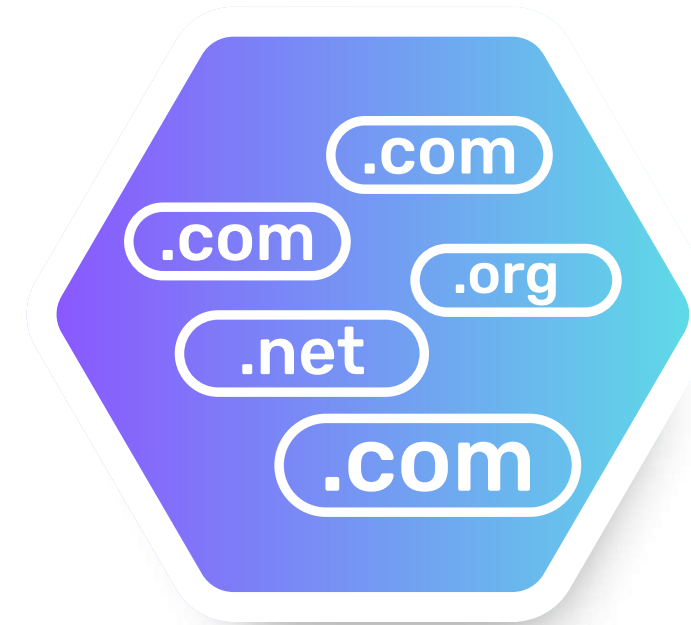
CECHY BEZPIECZNYCH STRON INTERNETOWYCH



**CERTYFIKAT
SSL**

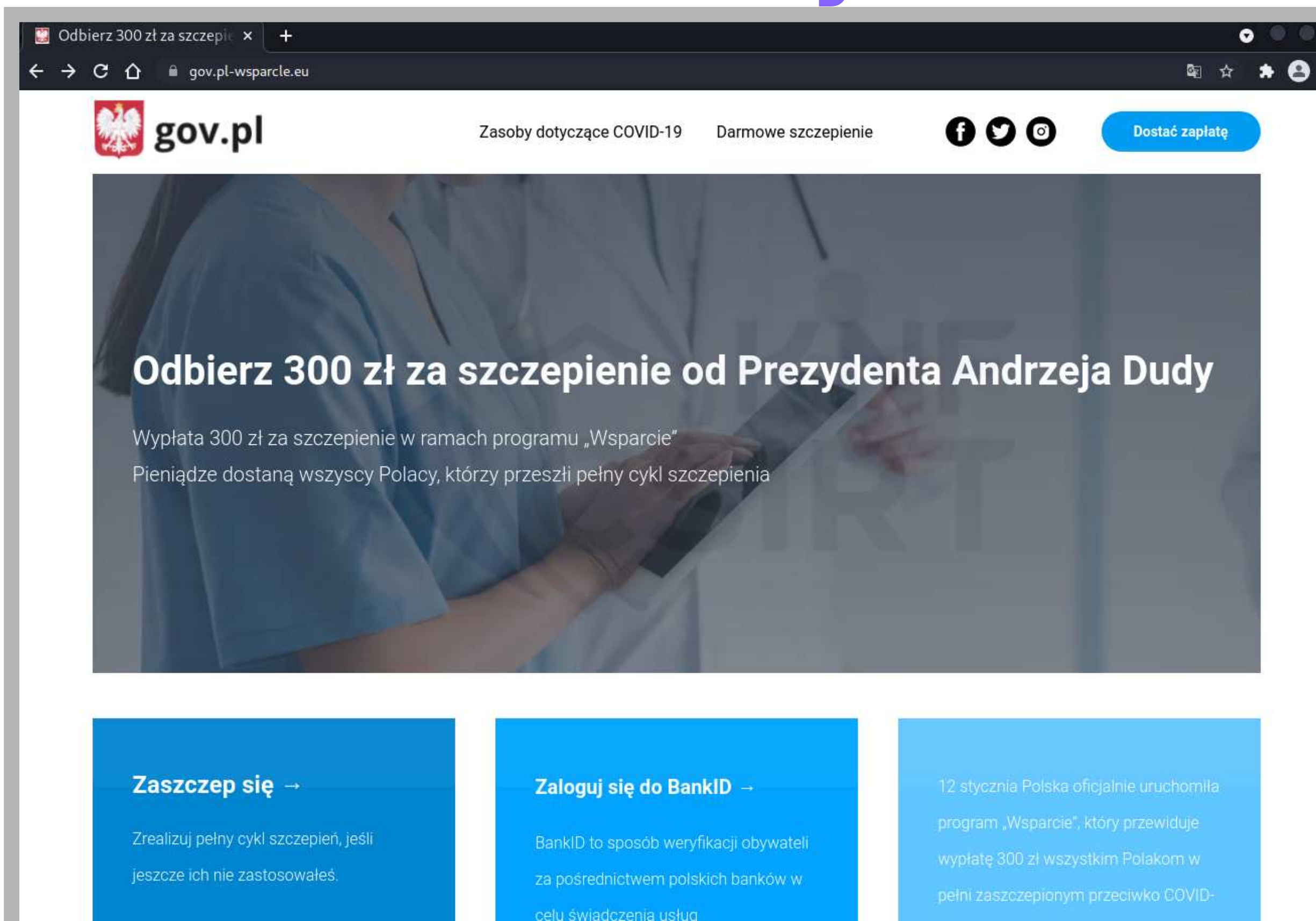


**ADRES STRONY
INTERNETOWEJ
BEZ LITERÓWEK**

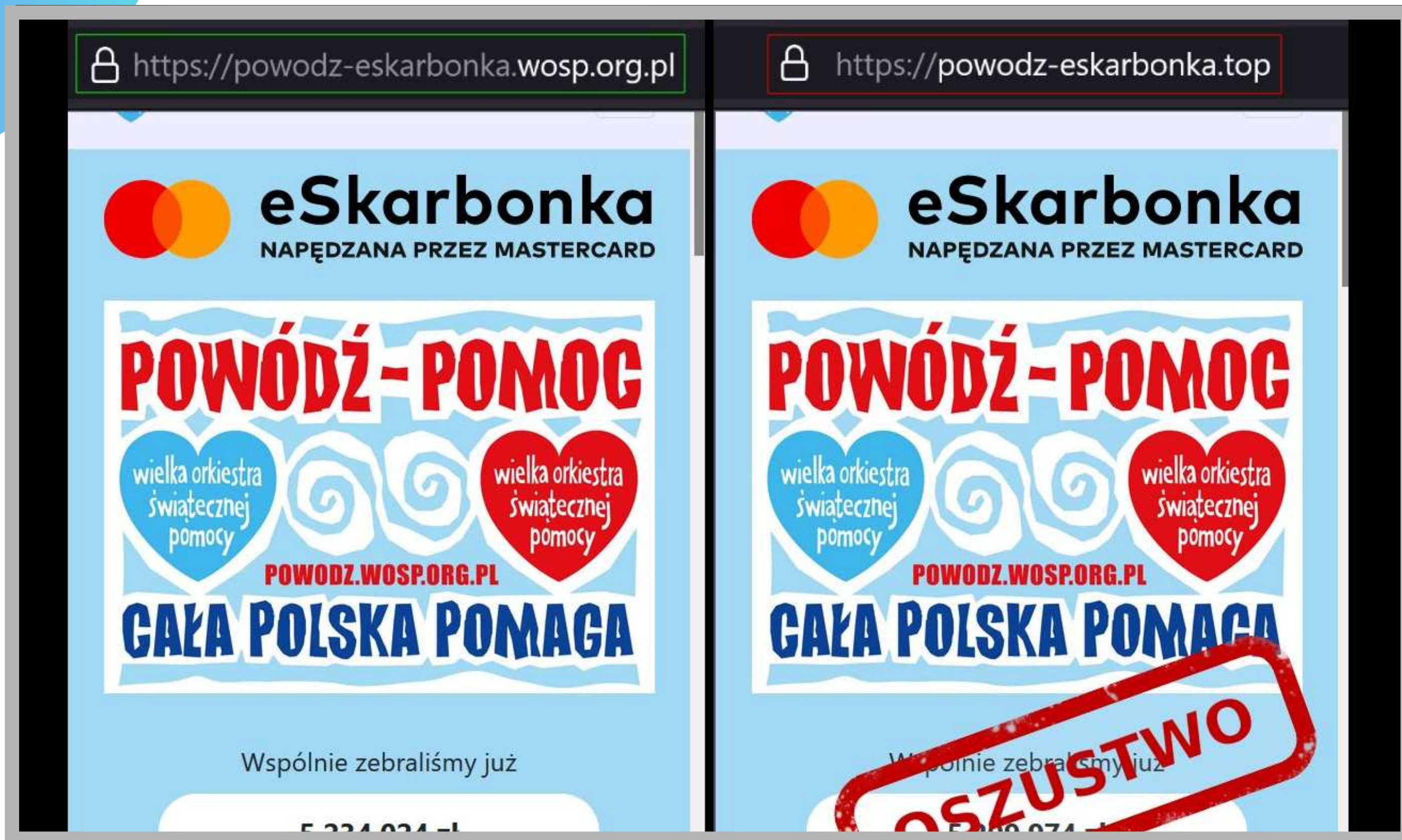


**NAZWA
DOMENY**

Przykład fałszywych stron internetowych



CERT.pl





Bezpieczne korzystanie z urządzeń mobilnych i komputerów

Jak unikać niebezpieczeństw w sieci?



**KORZYSTANIE Z
ZAUFANYCH
ŹRÓDEŁ
APLIKACJI**



**NIE KLIKAC W
LINKI
NIEZNANEGO
POCHODZENIA**



**NIEUDOSTĘPNIANIE
HASEŁ**



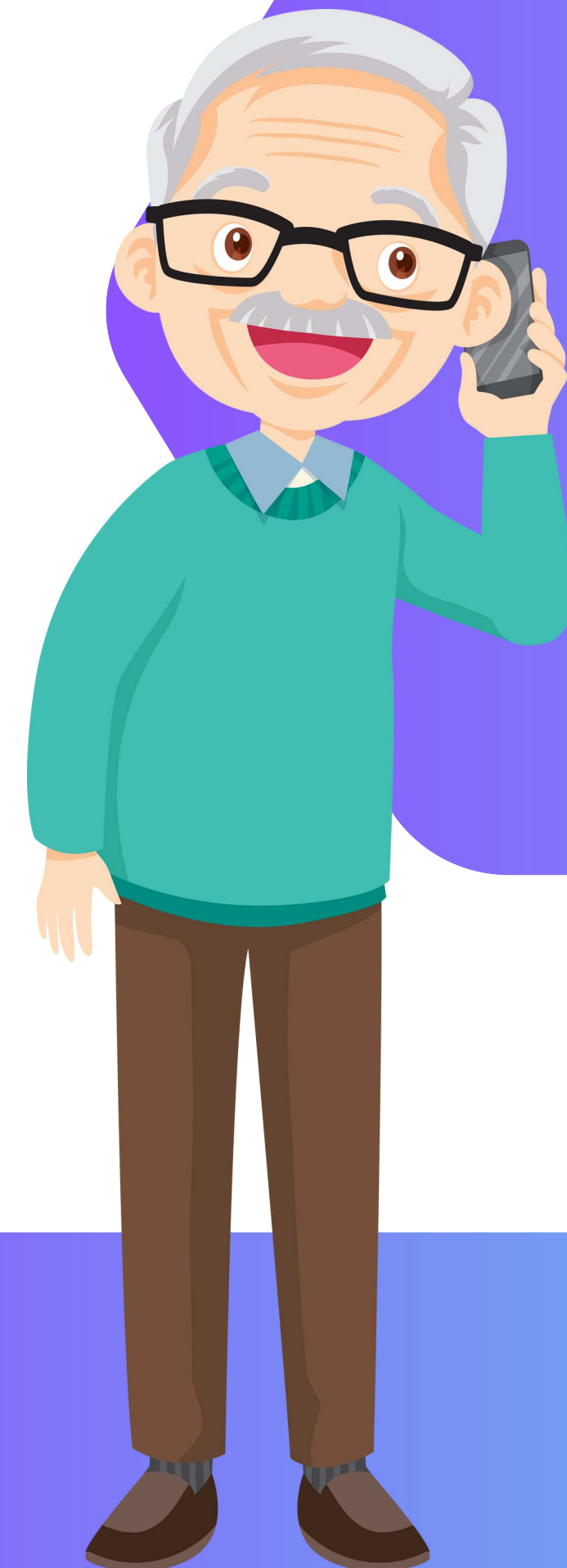
Aktualizacja oprogramowania

Aktualizacje oprogramowania są kluczowe dla bezpieczeństwa urządzeń. Każda nowa aktualizacja zawiera poprawki, które chroni przed nowymi zagrożeniami w sieci.

Warto co jakiś czas sprawdzić, czy nasze urządzenie jest aktualne. Starsze wersje oprogramowania mogą być podatne na ataki, dlatego regularne aktualizowanie to podstawa bezpieczeństwa.

Bezpieczne korzystanie z publicznych sieci WI-FI

- Korzystanie z VPN (Virtual Private Network) narzędzia, które szyfruje ruch internetowy i zapewnia większą prywatność oraz bezpieczeństwo, szczególnie w publicznych sieciach Wi-Fi





Ochrona przed wirusami i zagrożeniami





Programy antywirusowe

Programy antywirusowe są skuteczne w wykrywaniu i usuwaniu złośliwego oprogramowania. Regularne skanowanie pozwala na bieżąco monitorować stan bezpieczeństwa naszych urządzeń. Program antywirusowy powinien działać w tle i monitorować aktywność systemu w czasie rzeczywistym, blokując zagrożenia, zanim zainfekują urządzenie.

Przykłady programów antywirusowych



**AVASTFREE
ANTIVIRUS**



NORTON 360

Co zrobić gdy podejrzewamy, że nasze urządzenie zostało zainfekowane?



**ODŁĄCZ
URZĄDZENIE OD
INTERNETU**

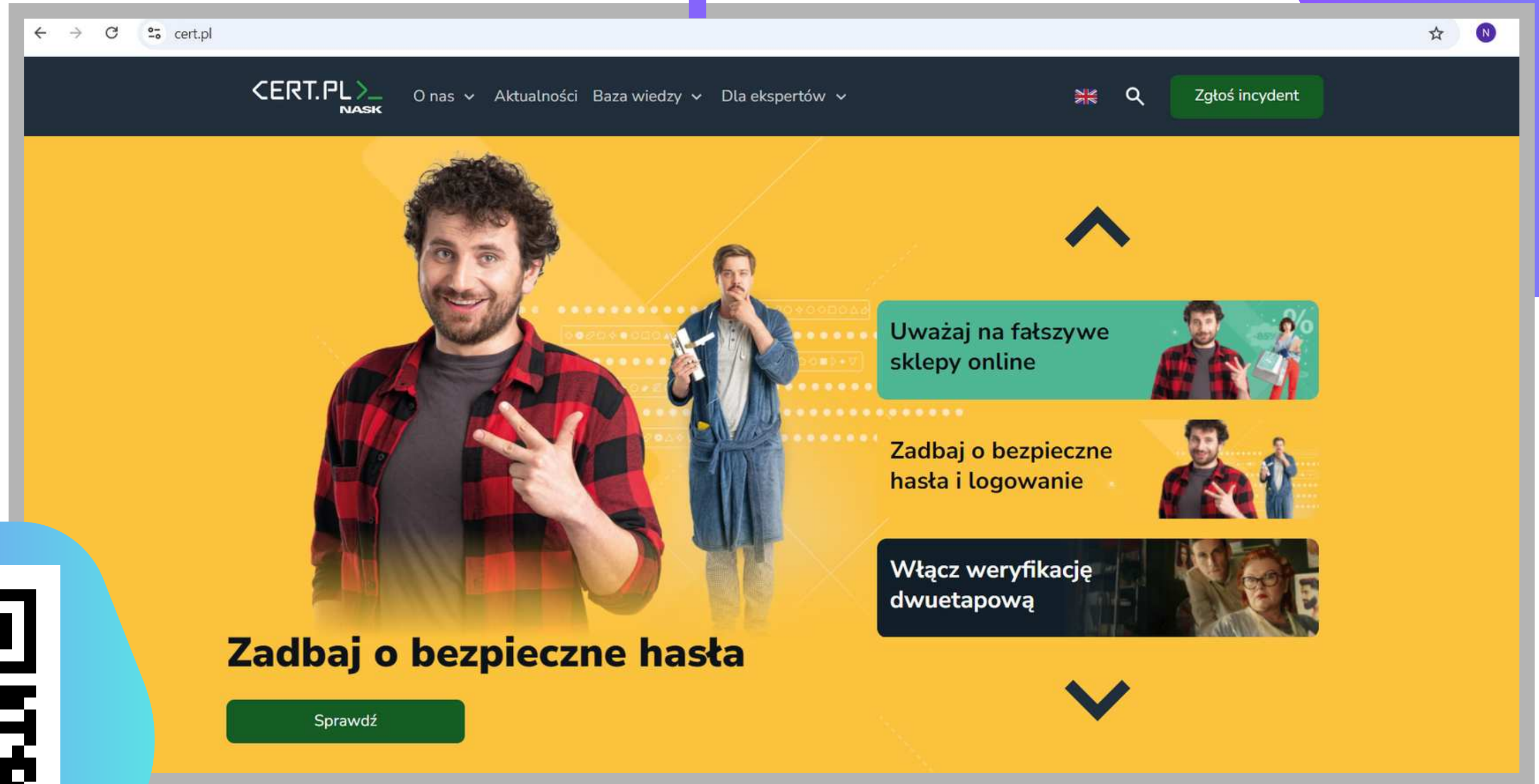


**PRZYWRÓĆ DO
USTAWIEŃ
FABRYCZNYCH**



**ZMIEŃ HASŁA
NA INNYM
URZĄDZENIU**

CERT.pl



Polub nas na Facebooku!



Skorzystaj z naszej CYBERLINII



Kiedy:

poniedziałek, środa i piątek

10:00–13:00

Tel: +48 579 519 688



KONTAKT

Spółeczna 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