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

AKTYWNI+

Społeczna Grupa Medialna

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

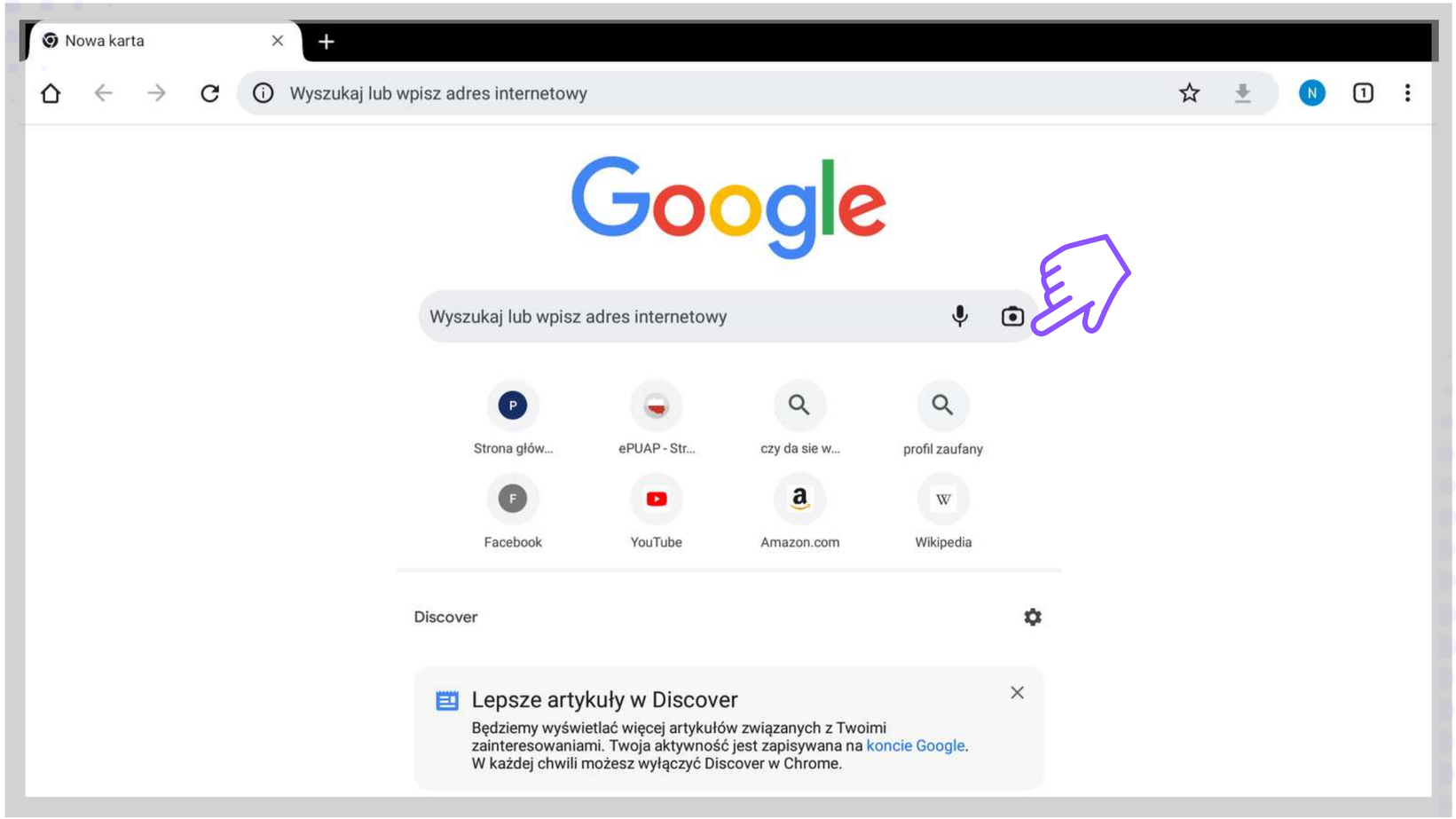
W tej prezentacji znajdziesz:

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

Obiektyw Google

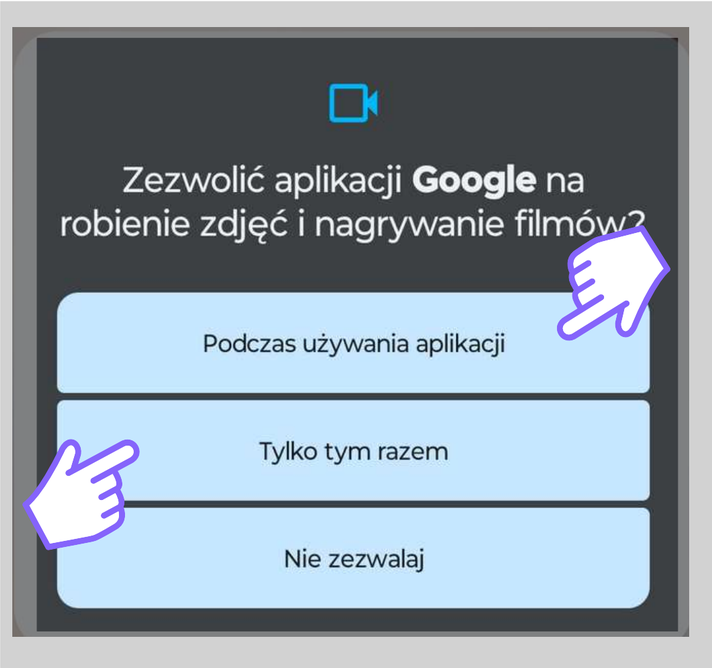
Jak uruchomić Obiektyw Google?

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

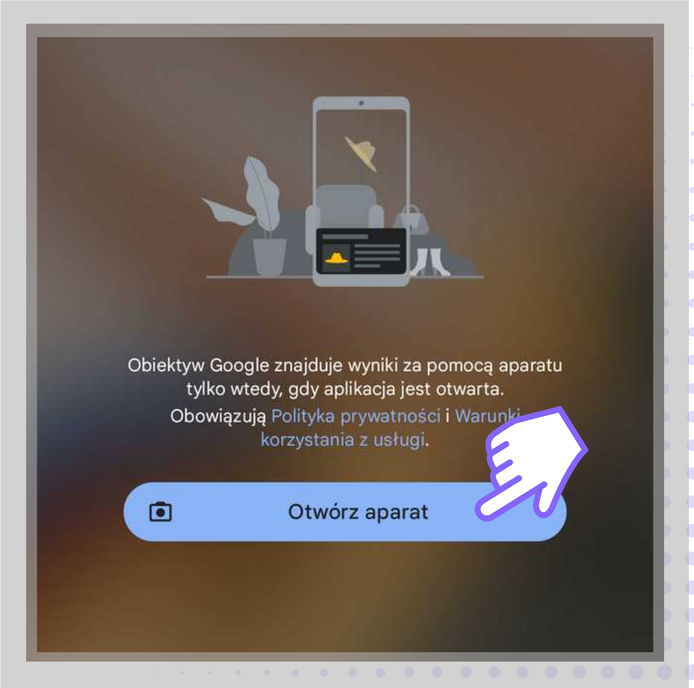


Jak uruchomić Obiektyw Google?

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 nieznajomości 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 oprogra – mowania, infekującego oraz blokującego system komputerowy poprzez zaszyfrowanie wybranych plików. Często okno lub plik zawie – rający 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 phisingu

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:

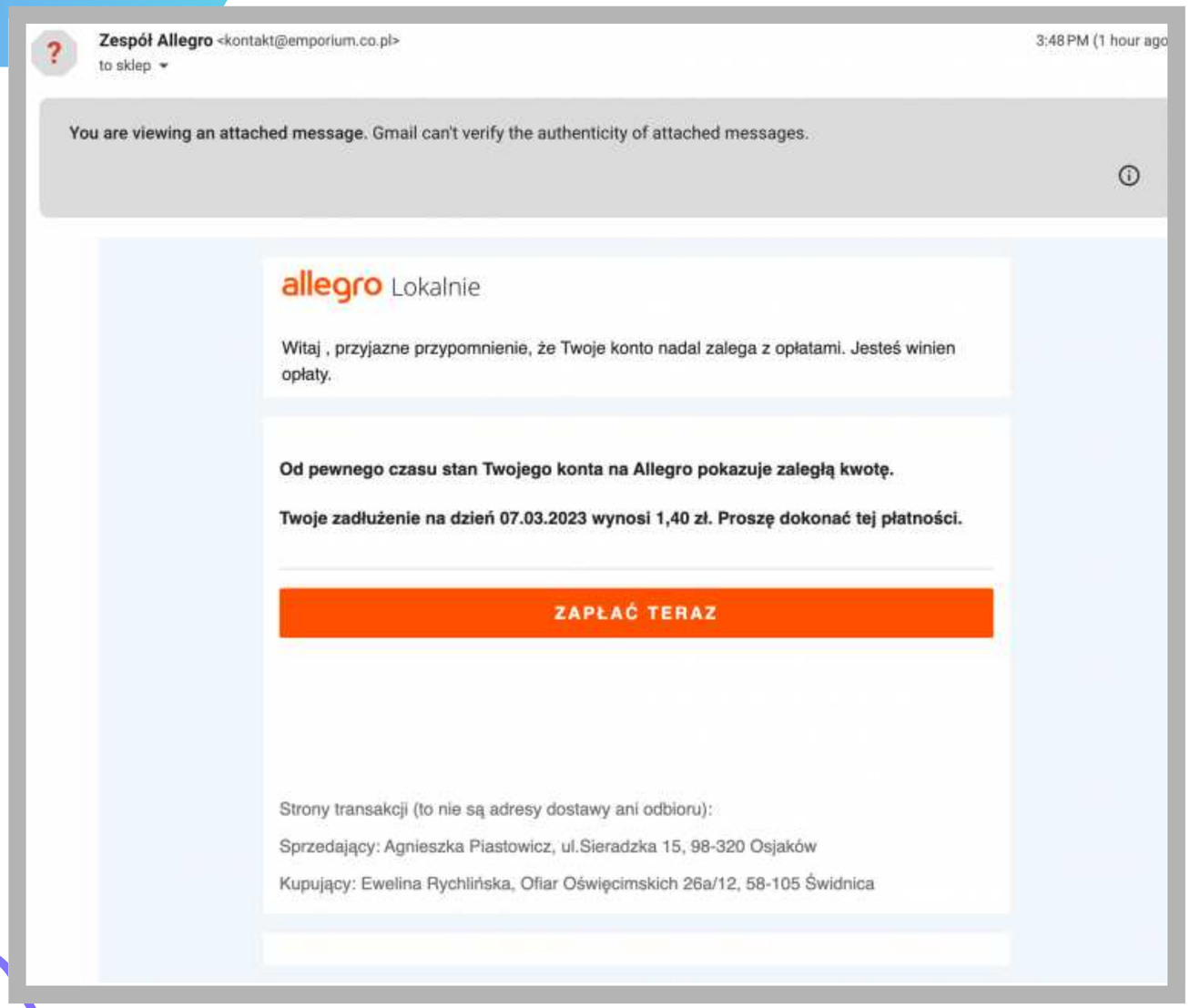
Prosimy o użycie tymczasowego hasła **6 9** podczas logowania.

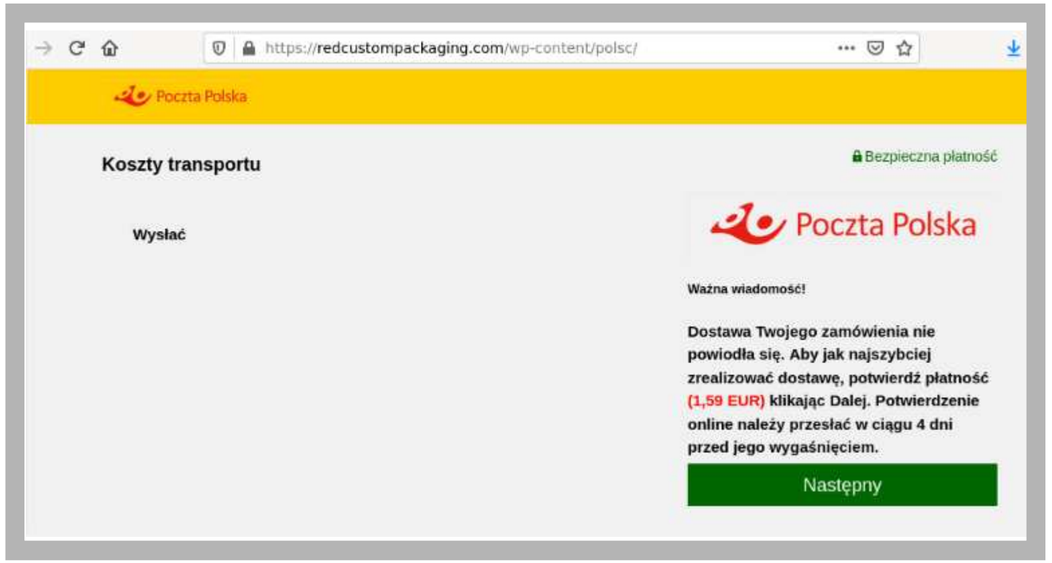
Zwracamy uwagę, że tymczasowe hasło wygaśnie 24 godziny po otrzymaniu tej wiadomości, jako środek ostrożności mający na celu zapewnienie bezpieczeństwa transakcji.

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

Z poważaniem,
PUESC Polska

Przykład phisingu





Fałszywe kody QR

Kraków PL
Przed chwilą ·

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.

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*

MM/YY

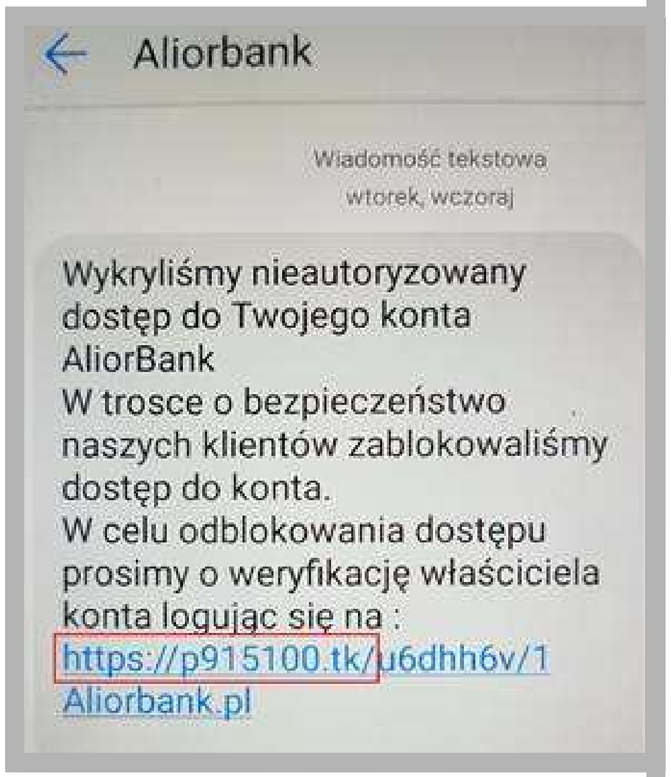
CVV*:

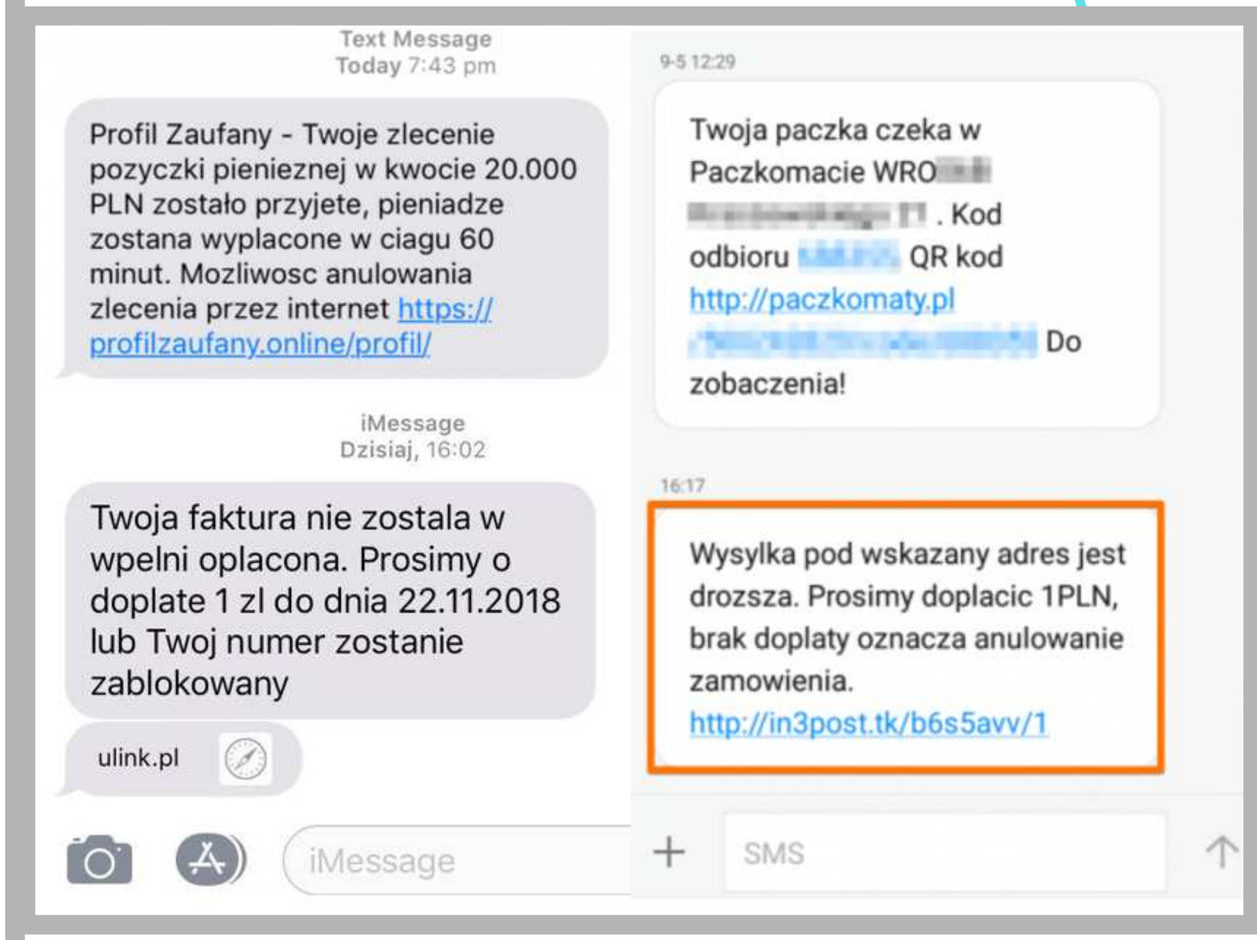
ZAPŁAĆ

OSZUSTWO

NIEBEZPIECZNIK.PL

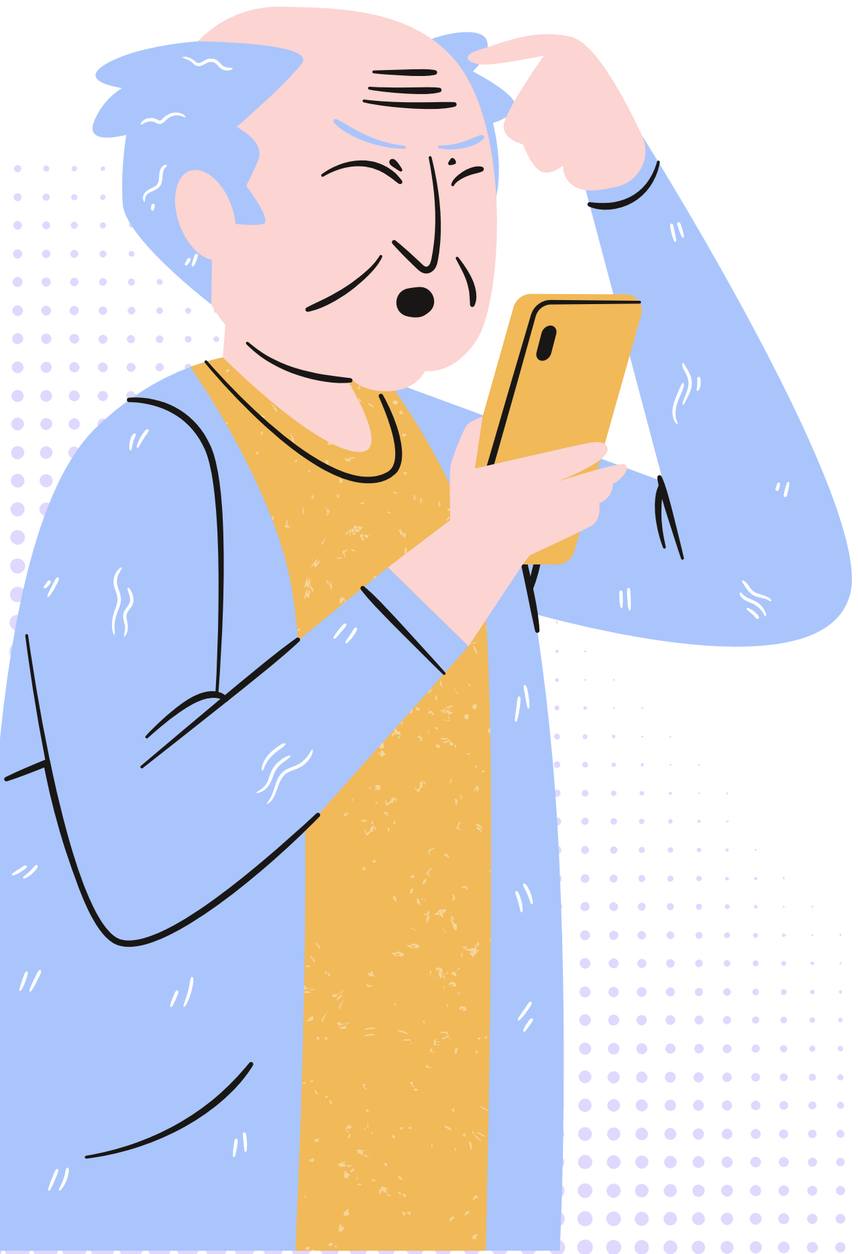
Przykład oszustwa sms-owego





Przykład fake news

Przykład fake news



Jak rozpoznać oszustwa internetowe?

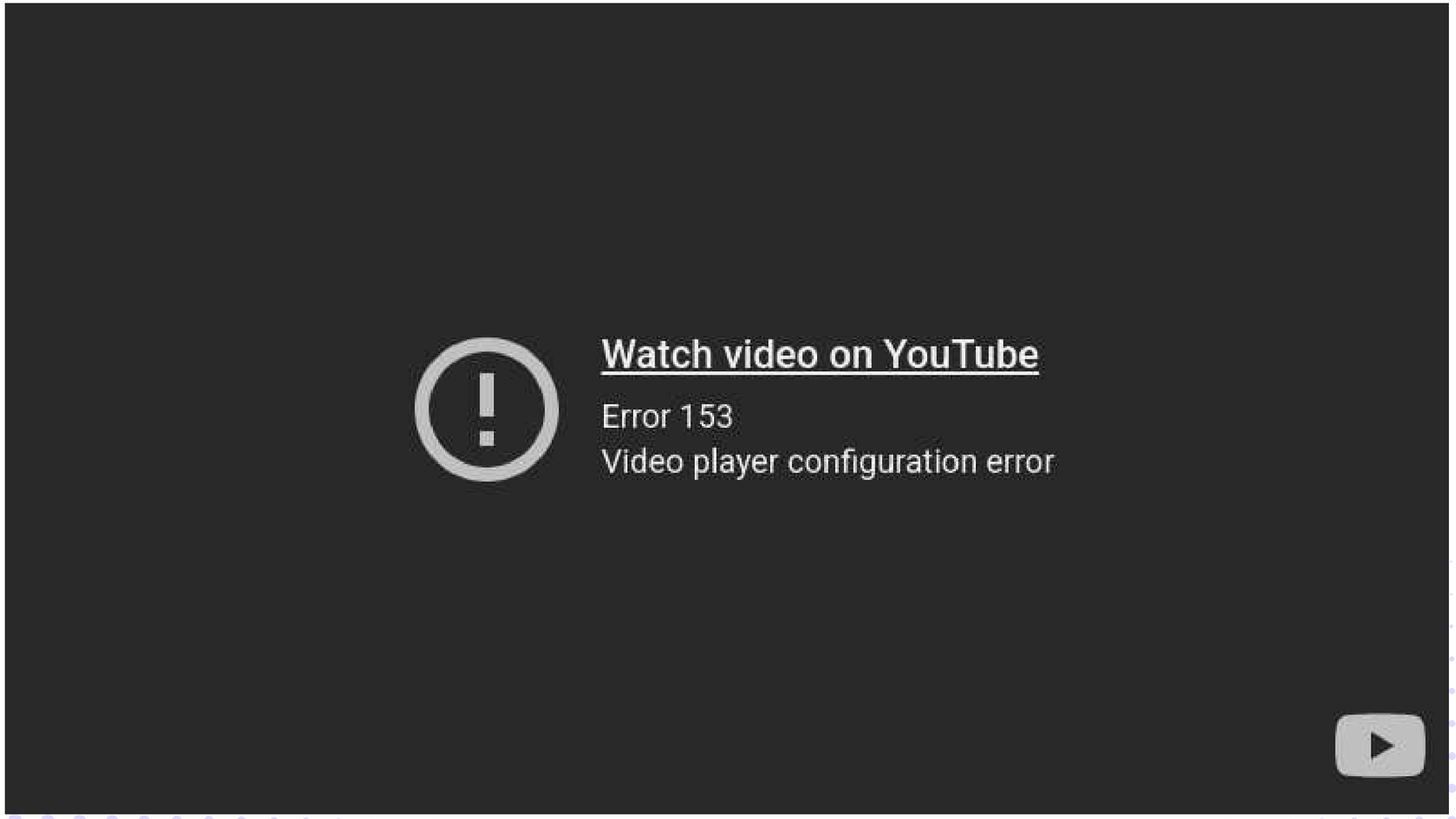
Jak rozpoznać oszustwa internetowe?

Zwracanie uwagi na język i styl wypowiedzi

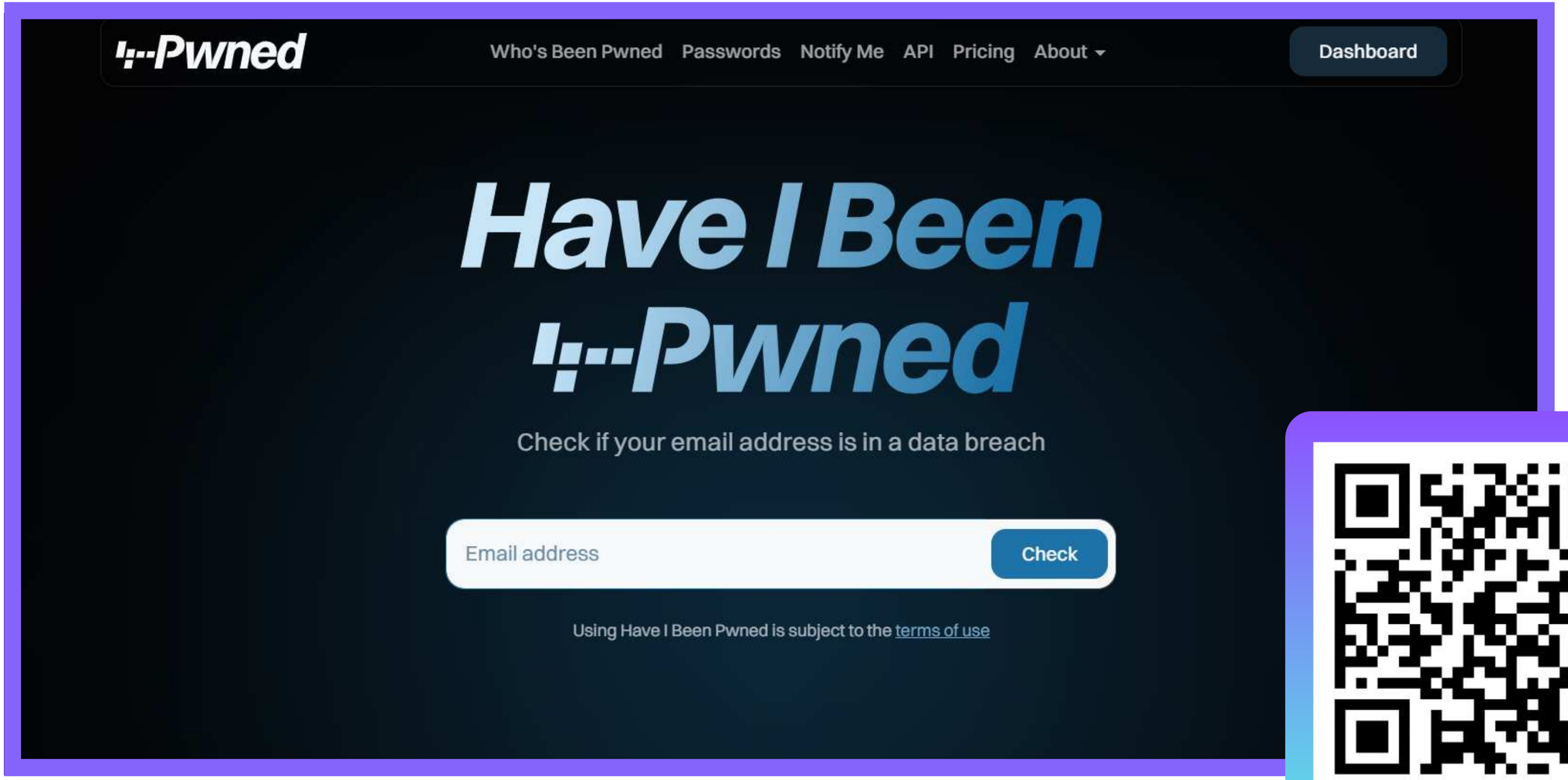
Sprawdzanie adresów e-mail i linków

Nie podawanie poufnych danych przez e-mail lub SMS.

Trzy mity bezpieczeństwa w sieci



Have I Been Pwned

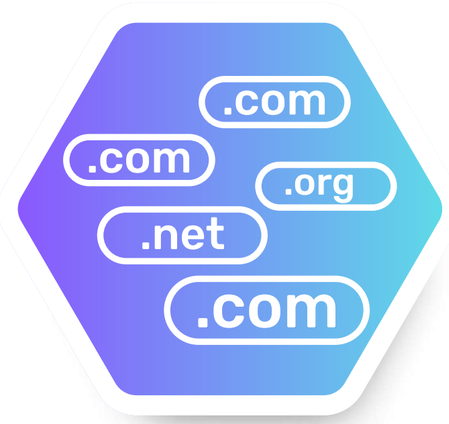


BEZPIECZNE STRONY INTERENTOWE

CECHY BEZPIECZNYCH STRON INTERNETOWYCH

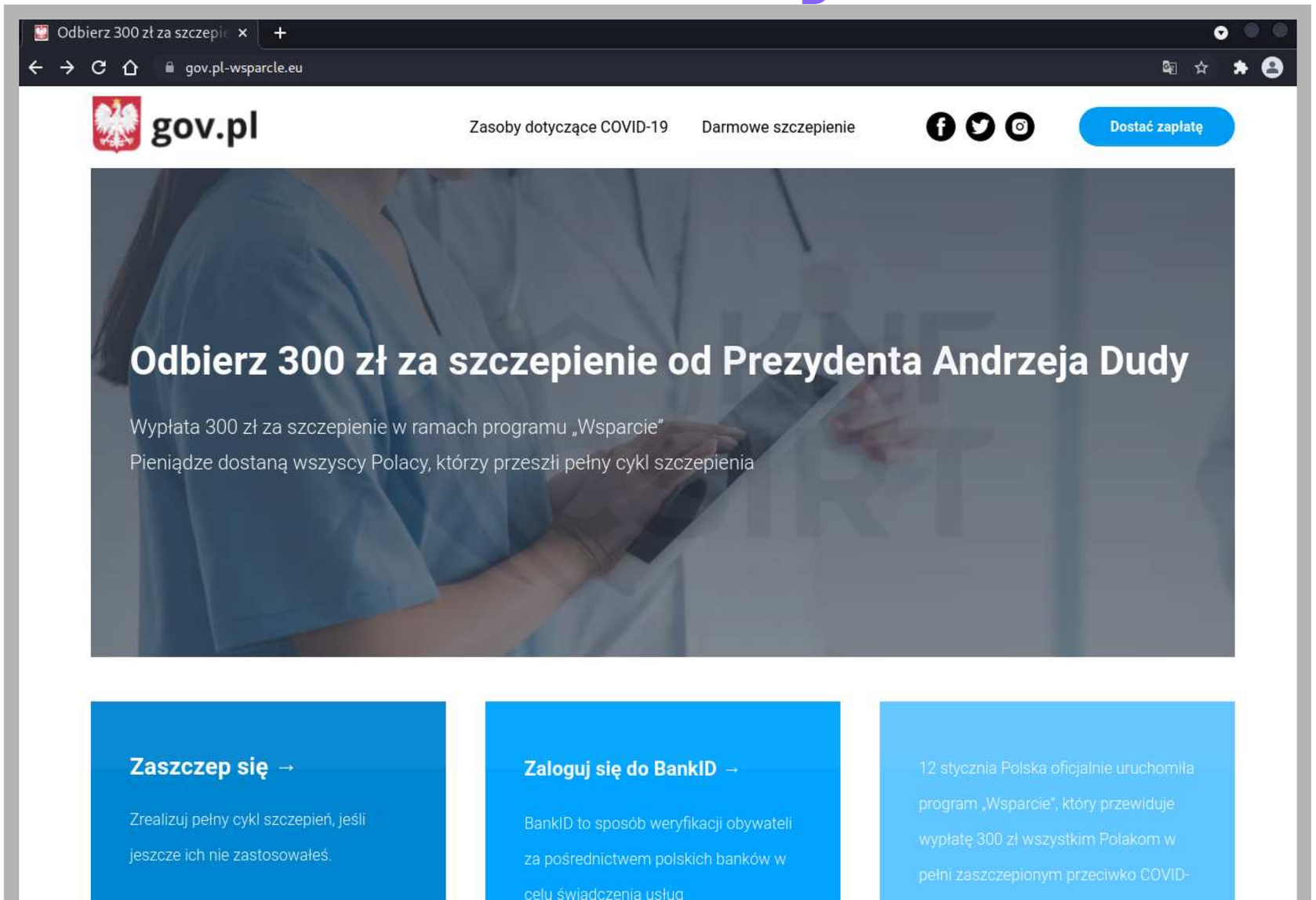
CERTYFIKAT SSL

ADRES STRONY INTERNETOWEJ BEZ LITERÓWEK



NAZWA DOMENY

Przykład fałszywych stron internetowych



CERT.pl


https://powodz-eskarbonka.wosp.org.pl
eSkarbonka
NAPĘDZANA PRZEZ MASTERCARD
POWÓDŹ - POMOC
wielka orkiestra świątecznej pomocy
wielka orkiestra świątecznej pomocy
POWODZ.WOSP.ORG.PL
CAŁA POLSKA POMAGA
Wspólnie zebraliśmy już
https://powodz-eskarbonka.top
eSkarbonka
NAPĘDZANA PRZEZ MASTERCARD
POWÓDŹ - POMOC
wielka orkiestra świątecznej pomocy
wielka orkiestra świątecznej pomocy
POWODZ.WOSP.ORG.PL
CAŁA POLSKA POMAGA
OSZUSTWO

Bezpieczne korzystanie z urządzeń mobilnych i komputerwów

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

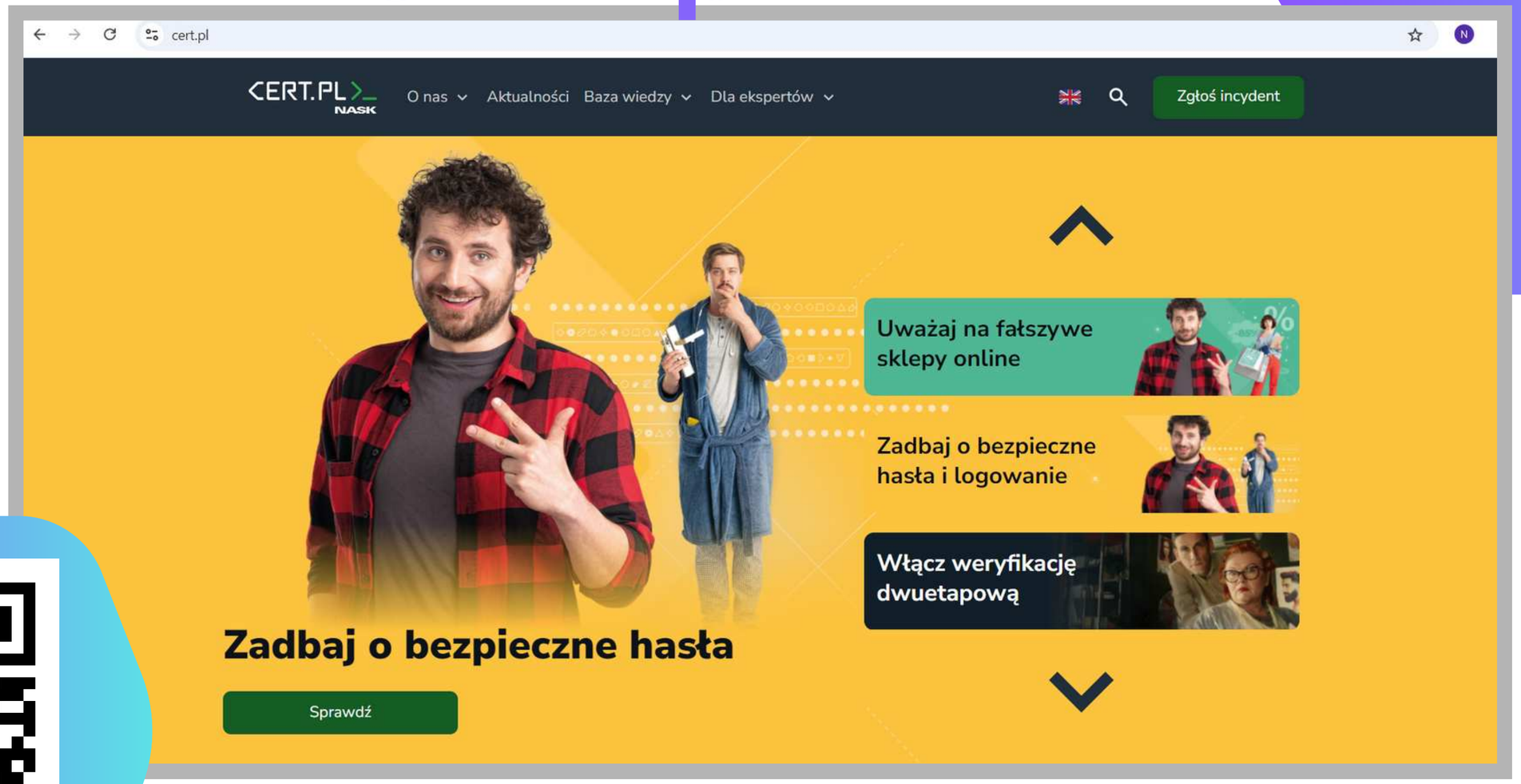
Co zrobić gdy podejrzewamy, że nasze urządzenie zostało zainfekowane?

ODŁĄCZ URZĄDZENIE OD INTERNETU

PRZYWRÓĆ DO USTAWIEŃ FABRYCZNYCH

ZMIEŃ HASŁA NA INNYM URZĄDZENIU

CERT.pl


cert.pl
CERT.PL NASK
O nas
Aktualności
Baza wiedzy
Dla ekspertów
Zgłoś incydent
Uważaj na fałszywe sklepy online
Zadbaj o bezpieczne hasła i logowanie
Włącz weryfikację dwuetapową
Zadbaj o bezpieczne hasła
Sprawdź

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