

Polityki bezpieczeństwa i plany awaryjne

Blok I – Kompetencje horyzontalne w cyfrowej administracji



– Ikona oznacza, że element jest interaktywny.

Cyberbezpieczeństwo w administracji publicznej

CEL MODUŁU

PHISHING I RANSOMWARE

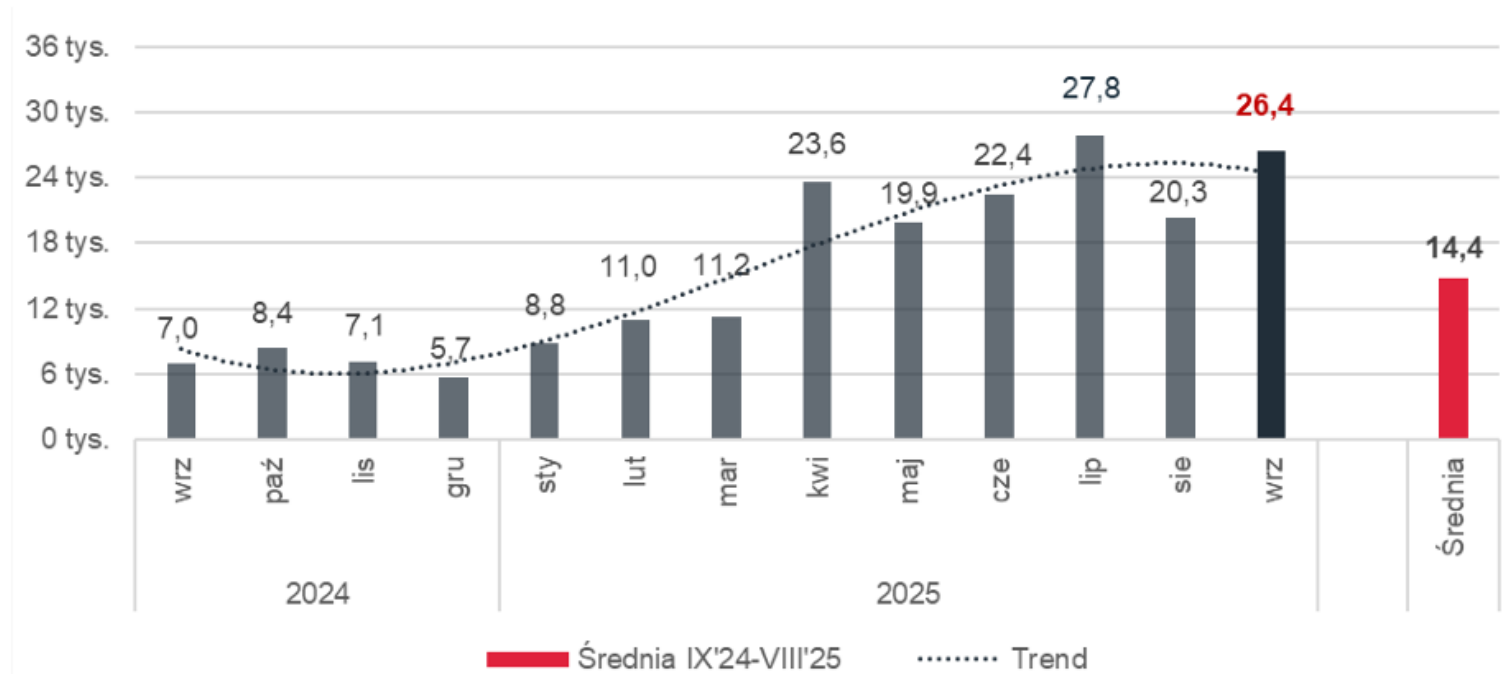
- Zwiększenie świadomości zagrożeń cybernetycznych
- Rozwój praktycznych umiejętności rozpoznawania zagrożeń

CERT.PL > C:/SIRT/MON

- Nauka reagowania na sytuacje niebezpieczne
- Wdrożenie polityk bezpieczeństwa w JST

CERT.PL > NASK

Zarejestrowane incydenty cyberbezpieczeństwa od IX 2024 do IX 2025



Polityka bezpieczeństwa informacji w urzędzie

RAMY PRAWNE

Art. 32 RODO - środki techniczne i organizacyjne

Jednym z podstawowych obowiązków Administratora danych osobowych oraz podmiotu przetwarzającego jest zapewnienie bezpieczeństwa danych.

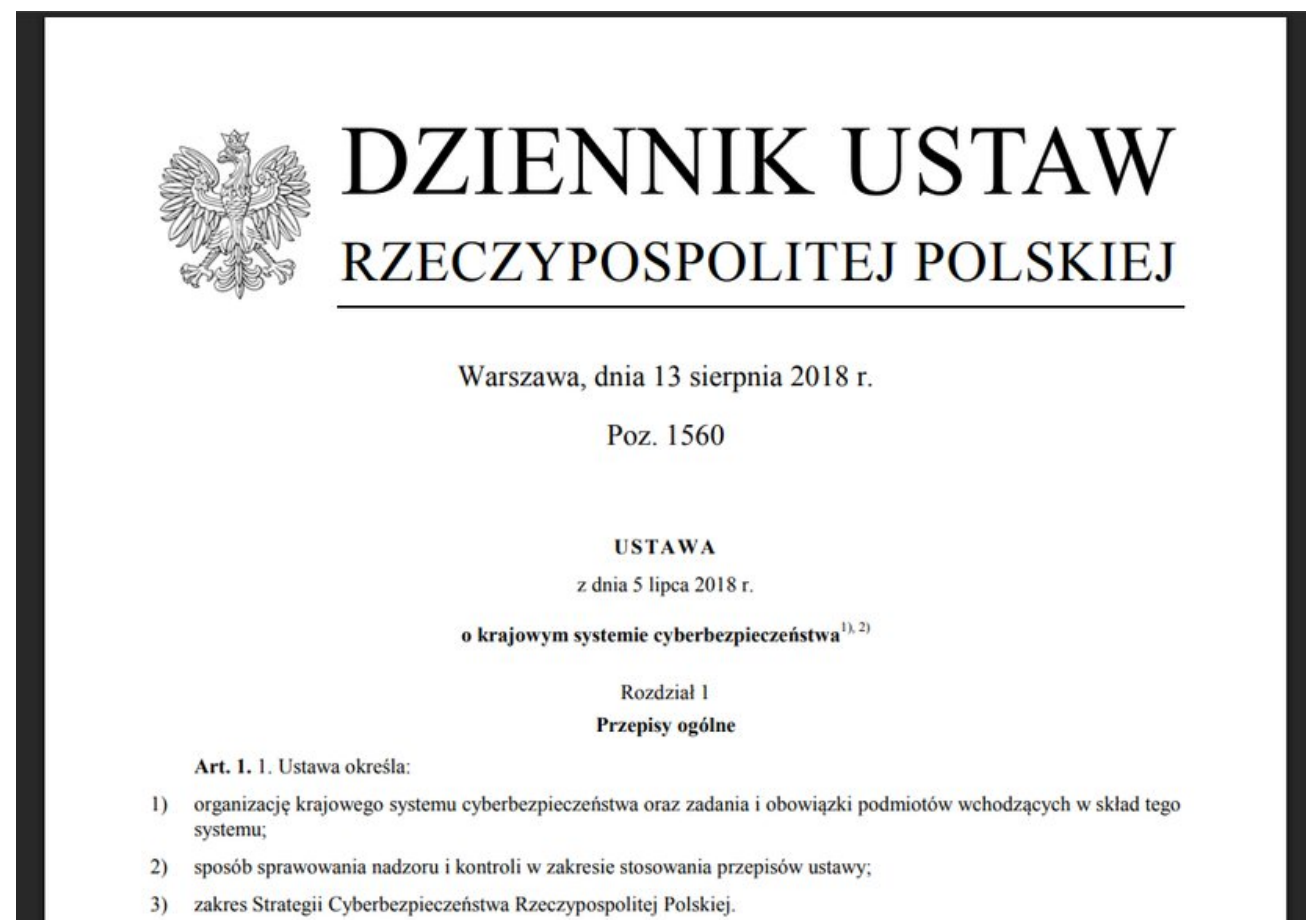


Kary rzędu 20–50 tys. zł dla samorządów za zbyt słabe zabezpieczenia IT i brak regularnych testów

RAMY PRAWNE

Ustawa o krajowym systemie cyberbezpieczeństwa

Pracownicy urzędów muszą dbać o bezpieczeństwo systemów komputerowych i **zgłaszać** cyberataki.



RAMY PRAWNE

Obowiązki administratorów danych publicznych

- stosowanie zabezpieczeń technicznych i organizacyjnych,
- szkolenie personelu,
- zgłaszanie incydentów (np. cyberataków czy wycieków),
- dokumentowanie tego, kto i jak przetwarza dane.



ODPOWIEDZIALNOŚĆ



Kierownik jednostki - nadzór strategiczny
Administrator IT - wdrożenie techniczne
Wszyscy pracownicy - przestrzeganie procedur



Rzeczpospolita
Polska

Sfinansowane przez
Unię Europejską
NextGenerationEU



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Uzupełnienie umiejętności
cyfrowych pracowników JST
w województwie śląskim



Hasła - zasady silnych haseł



PRZYKŁADY ZŁYCH HASEŁ



Uzupełnienie umiejętności
cyfrowych pracowników JST
w województwie śląskim

- Hasło słownikowe, krótkie
- Dane osobowe
- Hasło słownikowe, brak cyfr i znaków specjalnych

XŹŁE

admin123

kowalski1980

password

UNIKAJ:

Powtarzania haseł w różnych systemach
Zapisywanie na karteczkach



CHECKLISTA DOBRYCH PRAKTYK



Uzupełnienie umiejętności
cyfrowych pracowników JST
w województwie śląskim

- Minimum 12 znaków
- Kombinacja liter, cyfr, znaków specjalnych
- Regularna zmiana (co 90 dni)

 **DOBRY**

Epuap&Ezd\$Rodo2024!

Adm1n!str@cj@#Pub1

M0j@Urz4d!2025#Bezp

ZALECAMY:

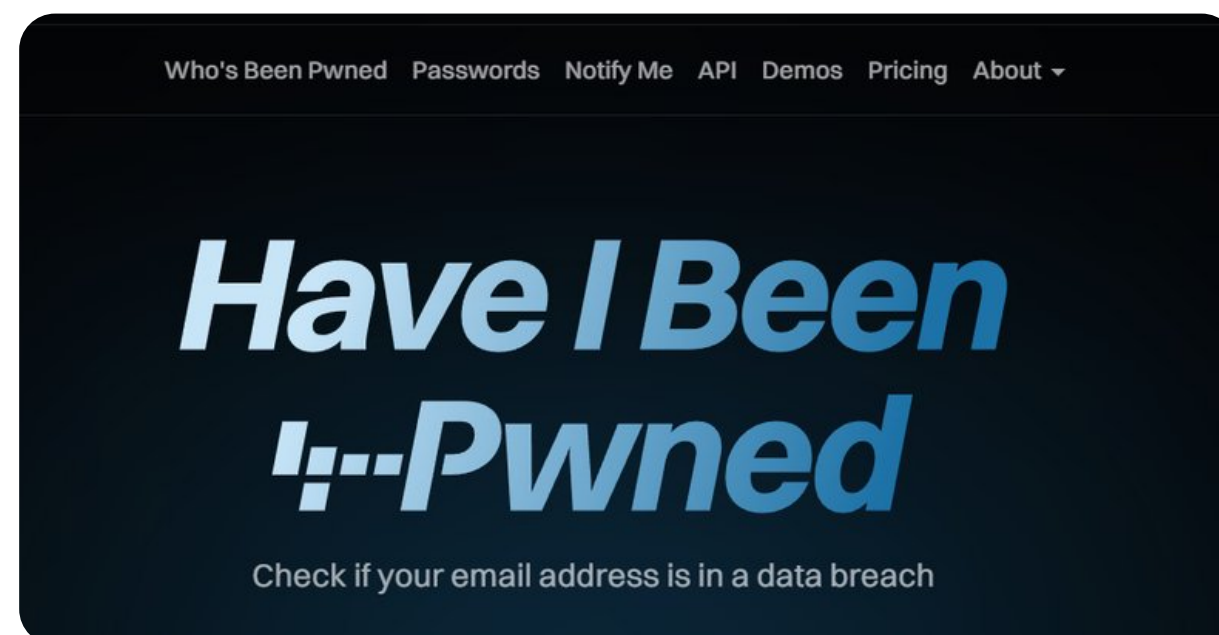
Twórz unikalne hasła dla każdego systemu.
Używaj menedżera haseł

Wskazówka - Użyj pierwszych liter zdania + cyfry + znaki specjalne

JAK SPRAWDZIĆ WYCIEK HASEŁ

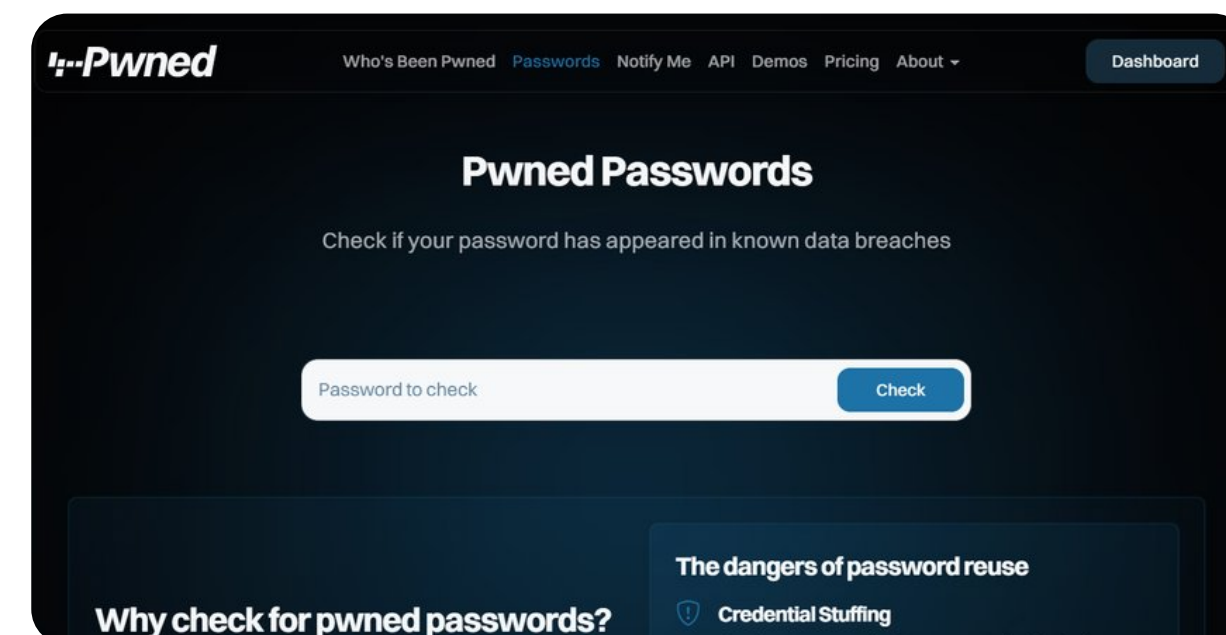
Nigdy nie używaj tego samego hasła w różnych serwisach!
Przejęcie jednego konta otwiera dostęp do pozostałych.

!-Pwned



Nie przechowuj haseł, zapisując je w pliku „Moje hasło” ani na karteczkach.

!-Pwned Passwords



ĆWICZENIE: ZAPROJEKTUJ SILNE HASŁO

Ćwiczenie: zaprojektuj silne hasło



 Uzupełnienie umiejętności
cyfrowych pracowników JST
w województwie śląskim

Ćwiczenie: zaprojektuj silne hasło

Wymyśl własne hasło zgodne z dobrymi praktykami bezpieczeństwa, a następnie sprawdź jego siłę korzystając z narzędzia Psono Password Strength Test.

Krok 1. Zaplanuj hasło

Zapisz pomysł na hasło, które spełnia poniższe zasady:

- minimum 12 znaków (litery, cyfry, znaki specjalne);
- brak danych osobowych (PESEL, imię, adres, nazwa klubu itp.);
- unikalne – niewykorzystywane w innych usługach;
- łatwe do zapamiętania dla Ciebie, trudne do odgadnięcia dla innych.

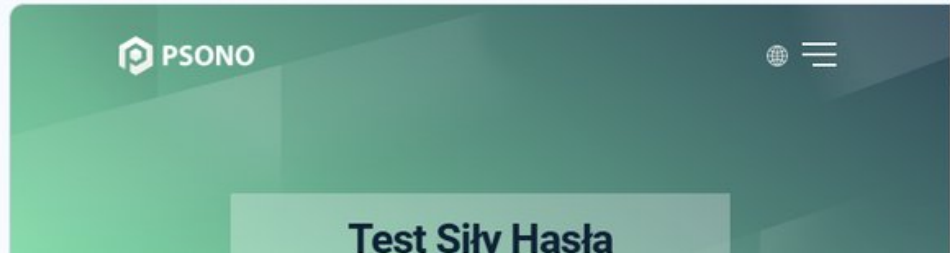
Robocza wersja hasła (lub sposób zapamiętania)

Np. połącz początkowe litery ze zdania, dodaj charakterystyczne liczby lub symbole...

Nie zapisuj ostatecznego hasła w dokumencie, który może trafić w niepowołane ręce. Zanotuj tu jedynie sposób budowania hasła lub jego zaszyfrowaną wersję.

Krok 2. Zweryfikuj siłę hasła

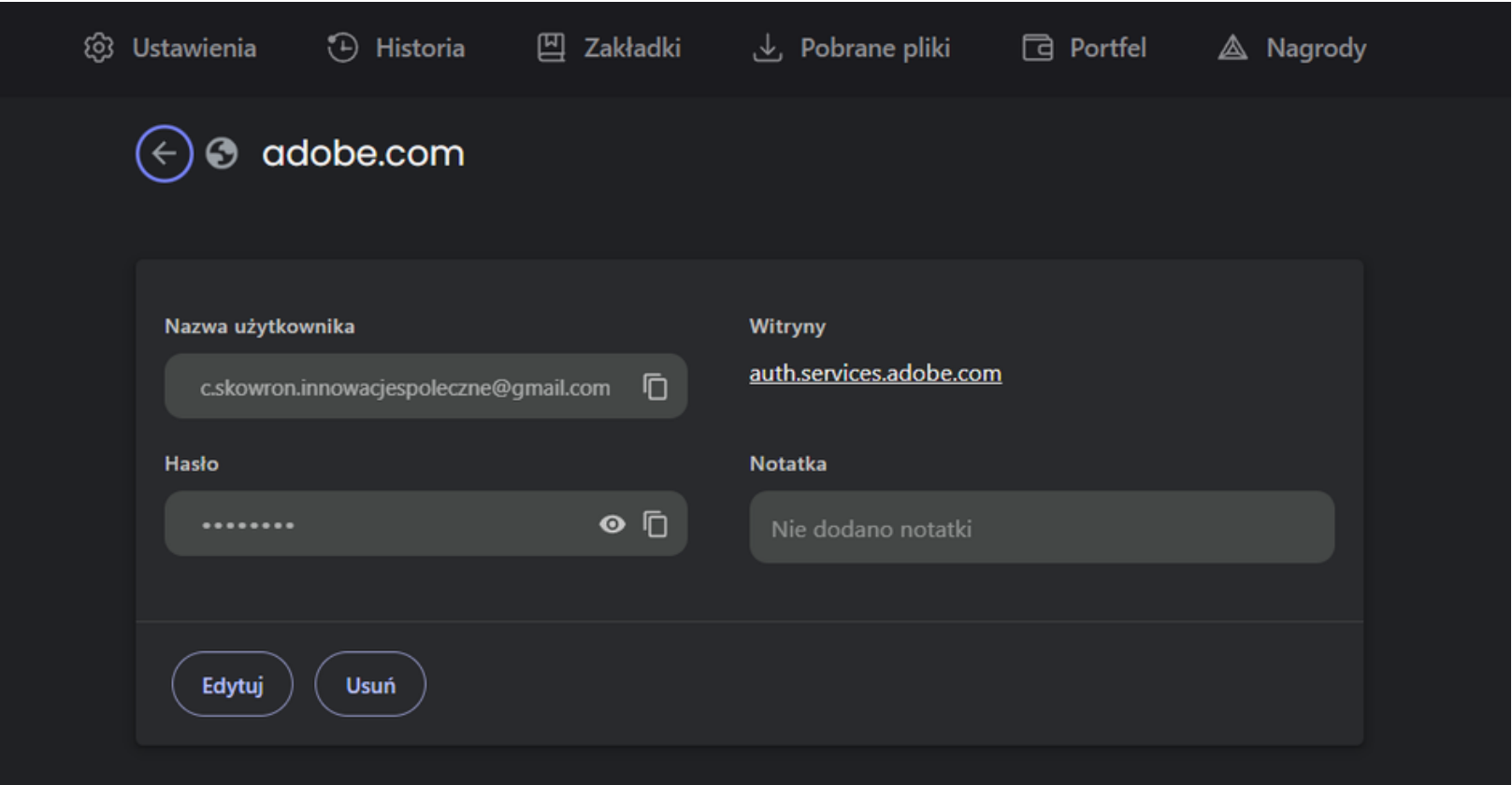
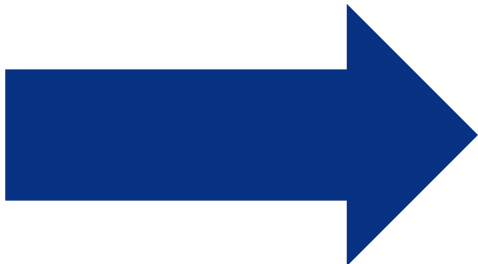
Otwórz okno poniżej i wpisz w nim swoje hasło (lub bardzo podobną wersję) bezpośrednio w narzędziu Psono. Narzędzie pokaże przewidywany czas potrzebny do złamania hasła oraz dodatkowe wskazówki.



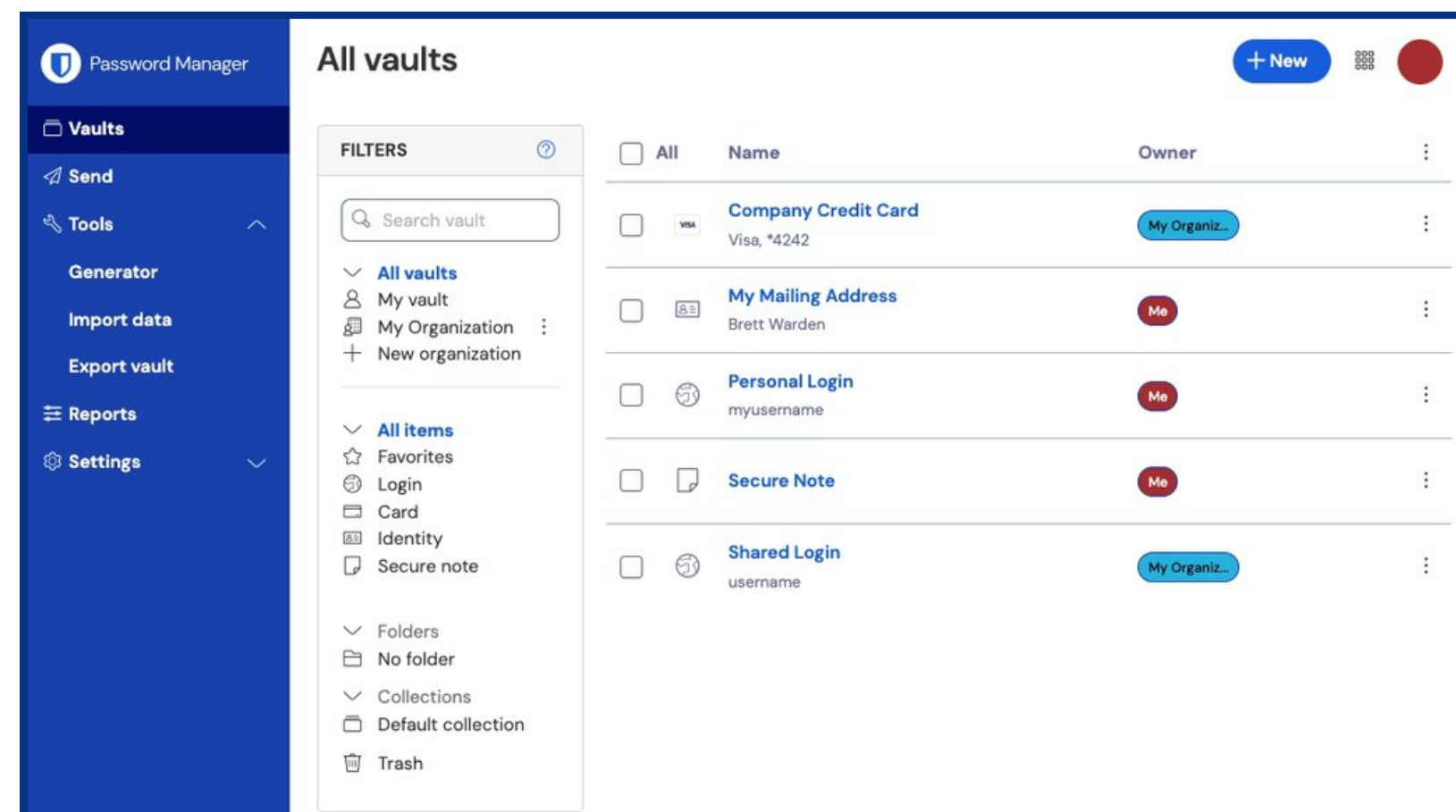
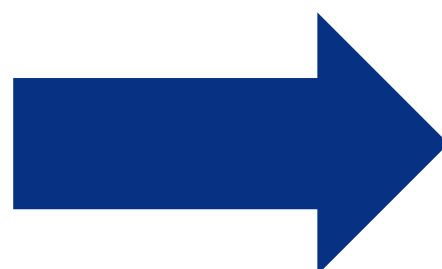
MENEDŻER HASEŁ W PRZEGLĄDARCE



Password Manager



MENEDŻER HASEŁ W POSTACI APLIKACJI



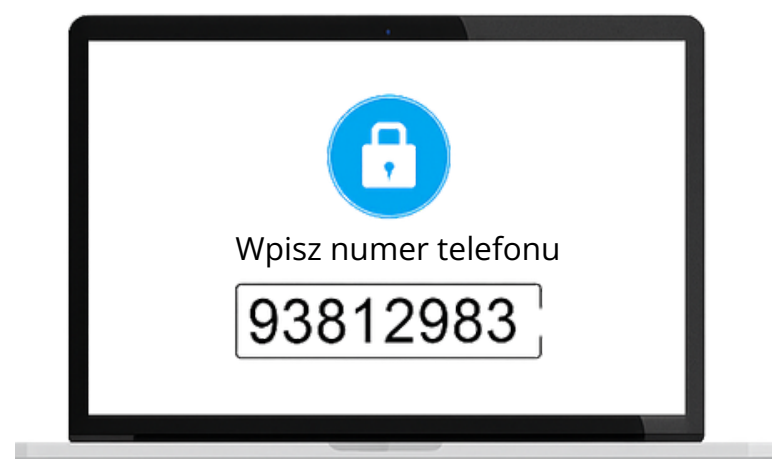
Uwierzytelnianie dwuskładnikowe (2FA)

CZYM JEST 2FA?

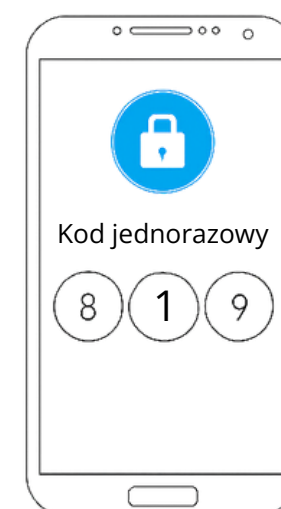
Uwierzytelnianie dwuskładnikowe (2FA) to metoda logowania, która oprócz hasła wymaga potwierdzenia tożsamości za pomocą drugiego elementu, np. kodu SMS lub aplikacji.

PRZYKŁAD UWIERZYTELNIENIA DWUSKŁADNIKOWEGO

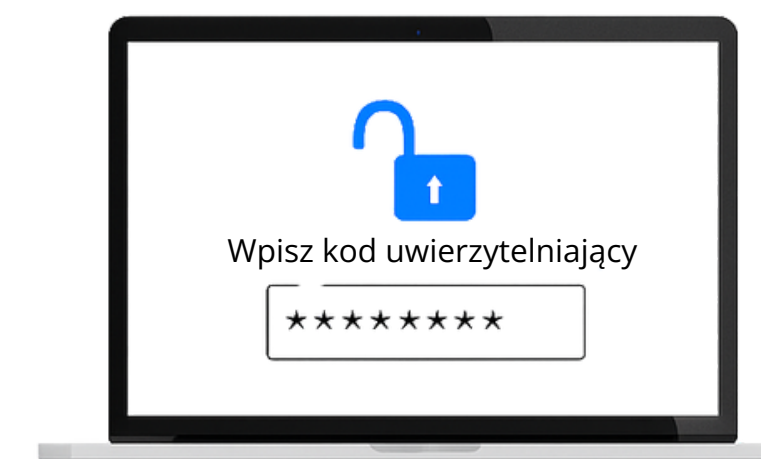
Użytkownik wpisuje numer telefonu



Użytkownik otrzymuje jednorazowy kod



Użytkownik wpisuje kod uwierzytelnienia



KIEDY OBOWIĄZKOWO?

Systemy wymagające 2FA:

- ePUAP (Elektroniczna Platforma Usług Administracji Publicznej)
- EZD (Elektroniczne Zarządzanie Dokumentacją)
- Systemy finansowe i księgowe
- Bazy danych osobowych
- Konta administratorów

Profil zaufany

[Jak korzystać](#) [Bezpieczeństwo](#) [Aktualności](#) [Klauzula informacyjna](#) [Pomoc](#) [Kontakt](#)



Załatwiał sprawy urzędowe przez Internet!

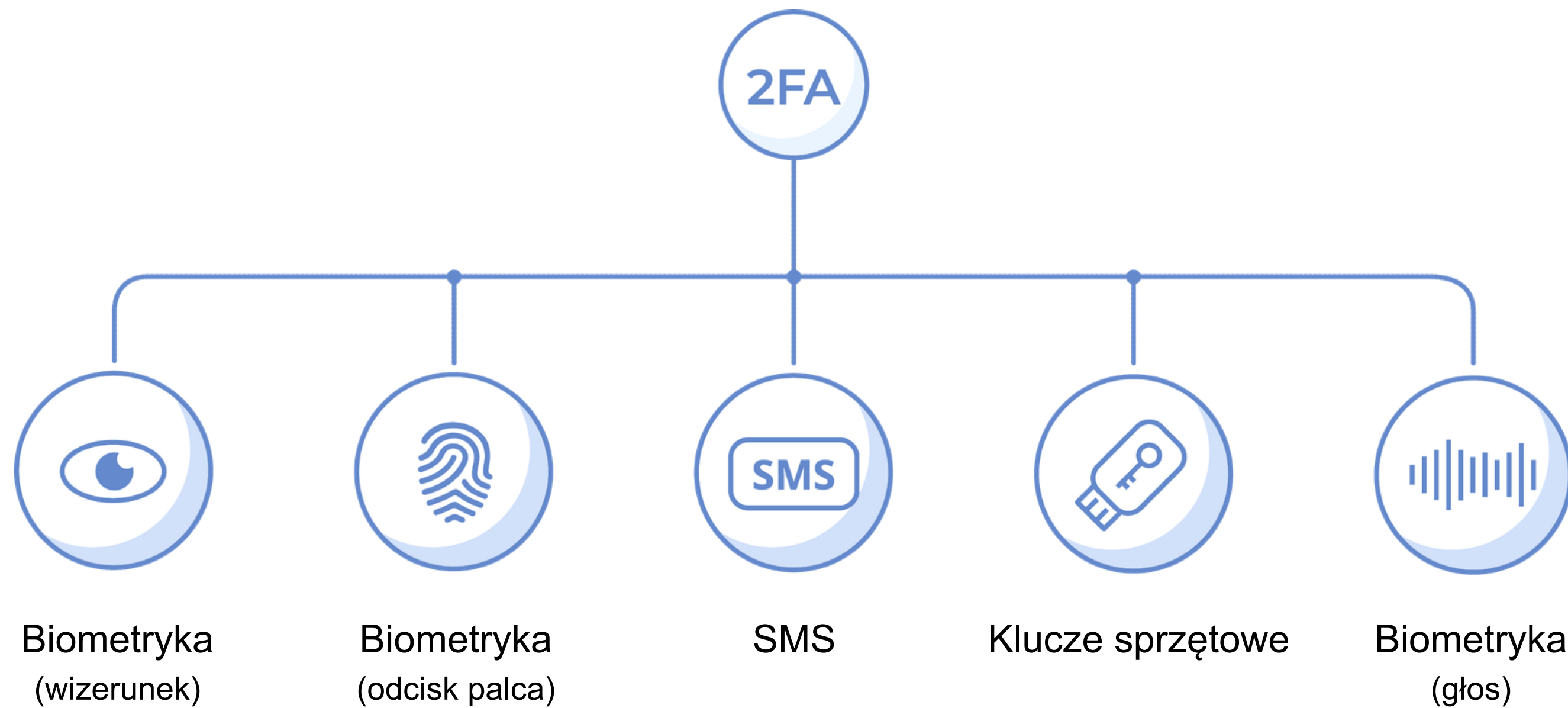
Profil zaufany (PZ) to bezpłatne i bezpieczne narzędzie, dzięki któremu możesz załatwiać sprawy urzędowe bez wychodzenia z domu. Profil zaufany założysz za darmo i to zaledwie w kilka chwil. To naprawdę proste.

ZAŁÓŻ PROFIL ZAUFANY

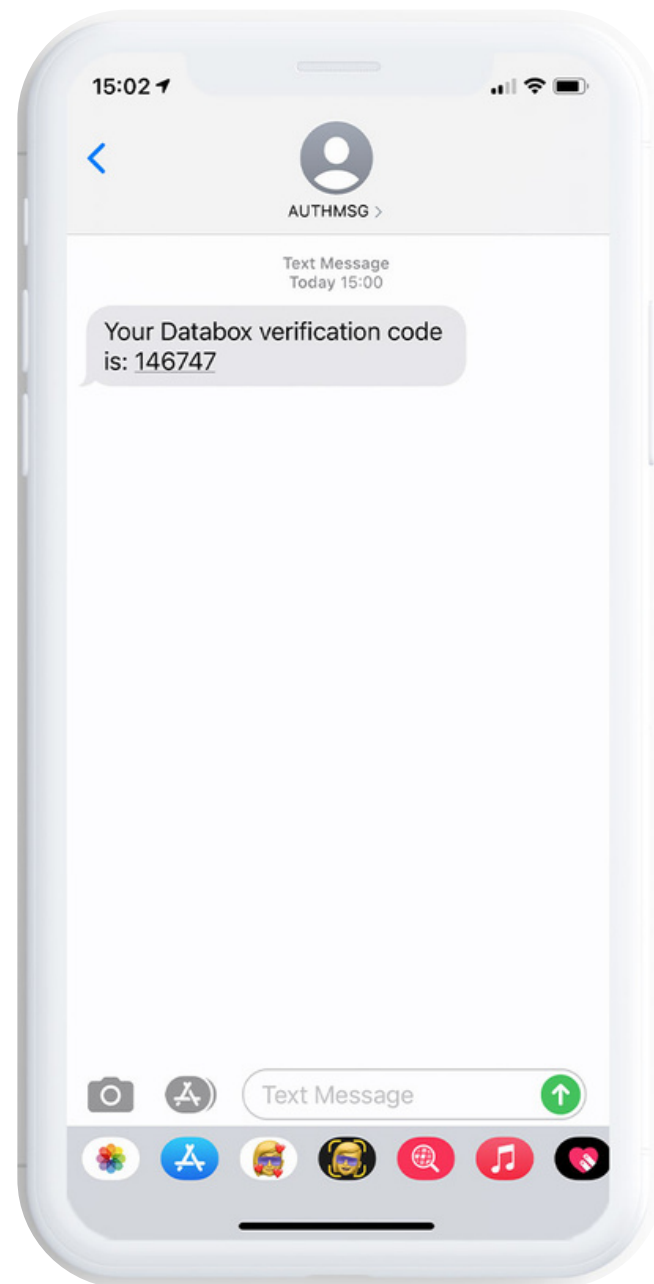
Masz już profil zaufany? Zaloguj się, aby móc zarządzać swoim kontem.

ZALOGUJ SIĘ

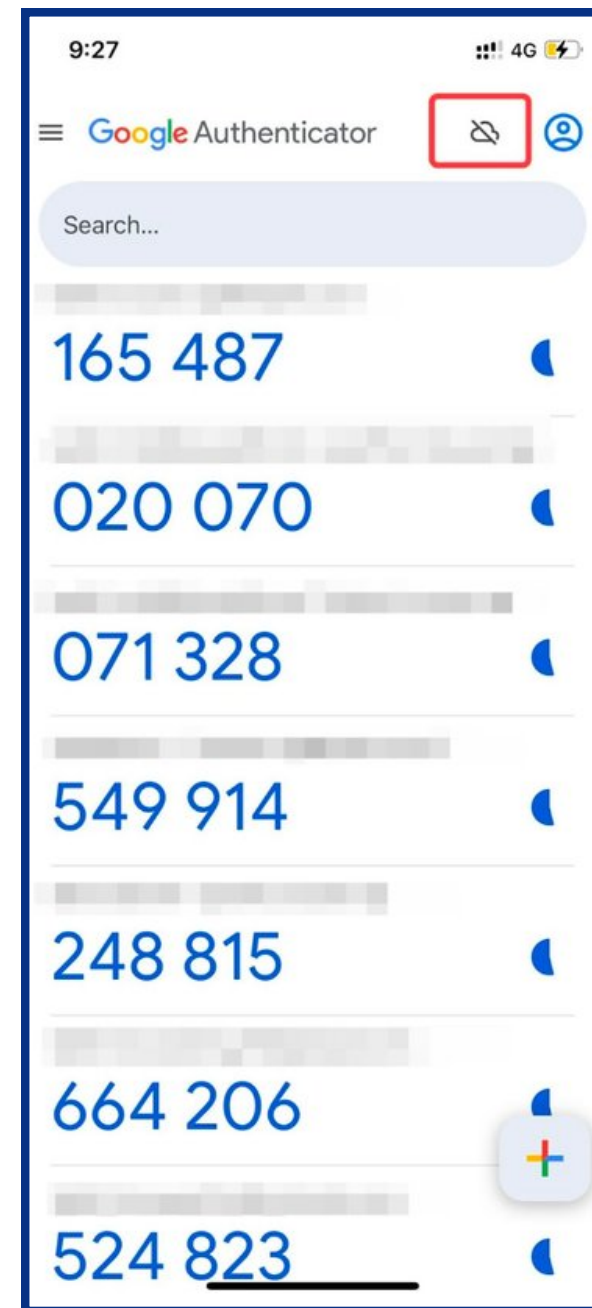
METODY 2FA:



SMS



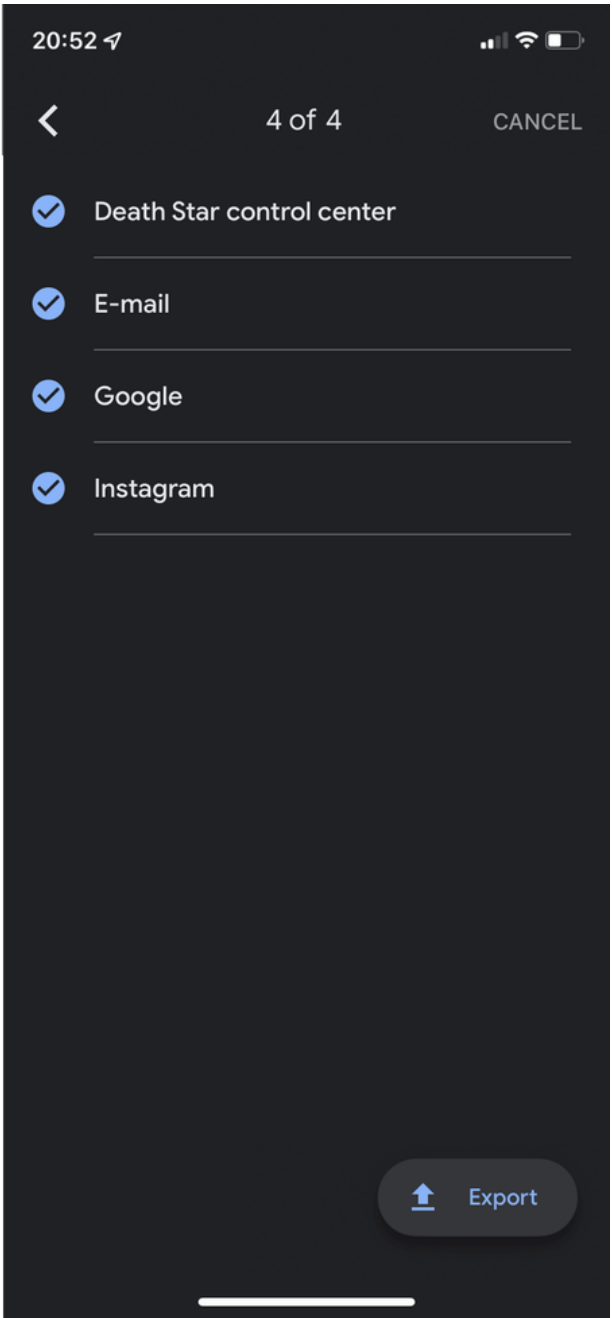
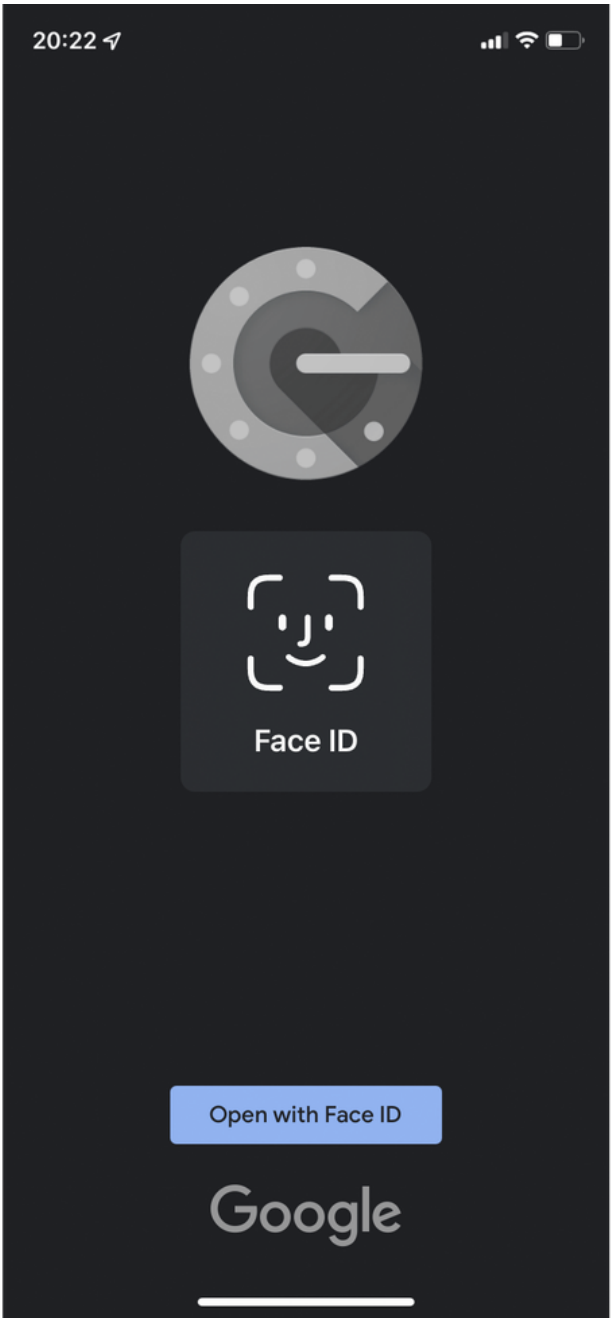
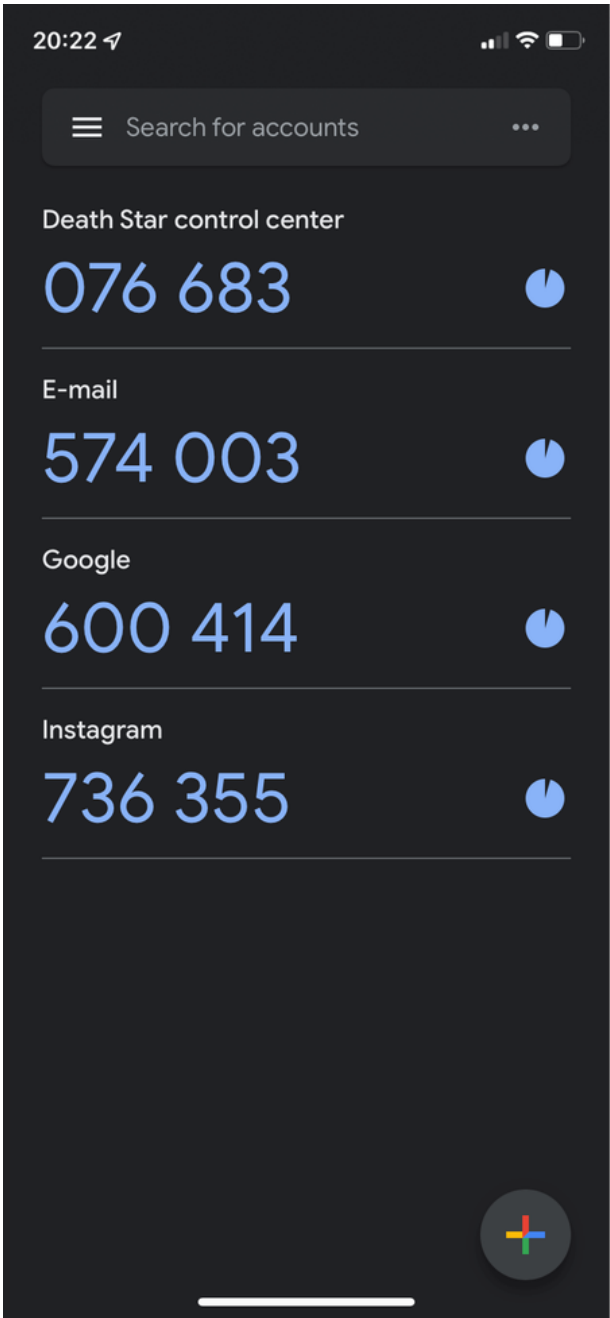
Aplikacja uwierzytelnienia



Klucz sprzętowy



APLIKACJA UWIERZYTELNIENIA



Google Authenticator



Microsoft Authenticator

KLUCZ SPRZĘTOWY - “FIZYCZNY KLUCZ” DO KONTA

Cena: 150-250 zł



Na co zwrócić uwagę:

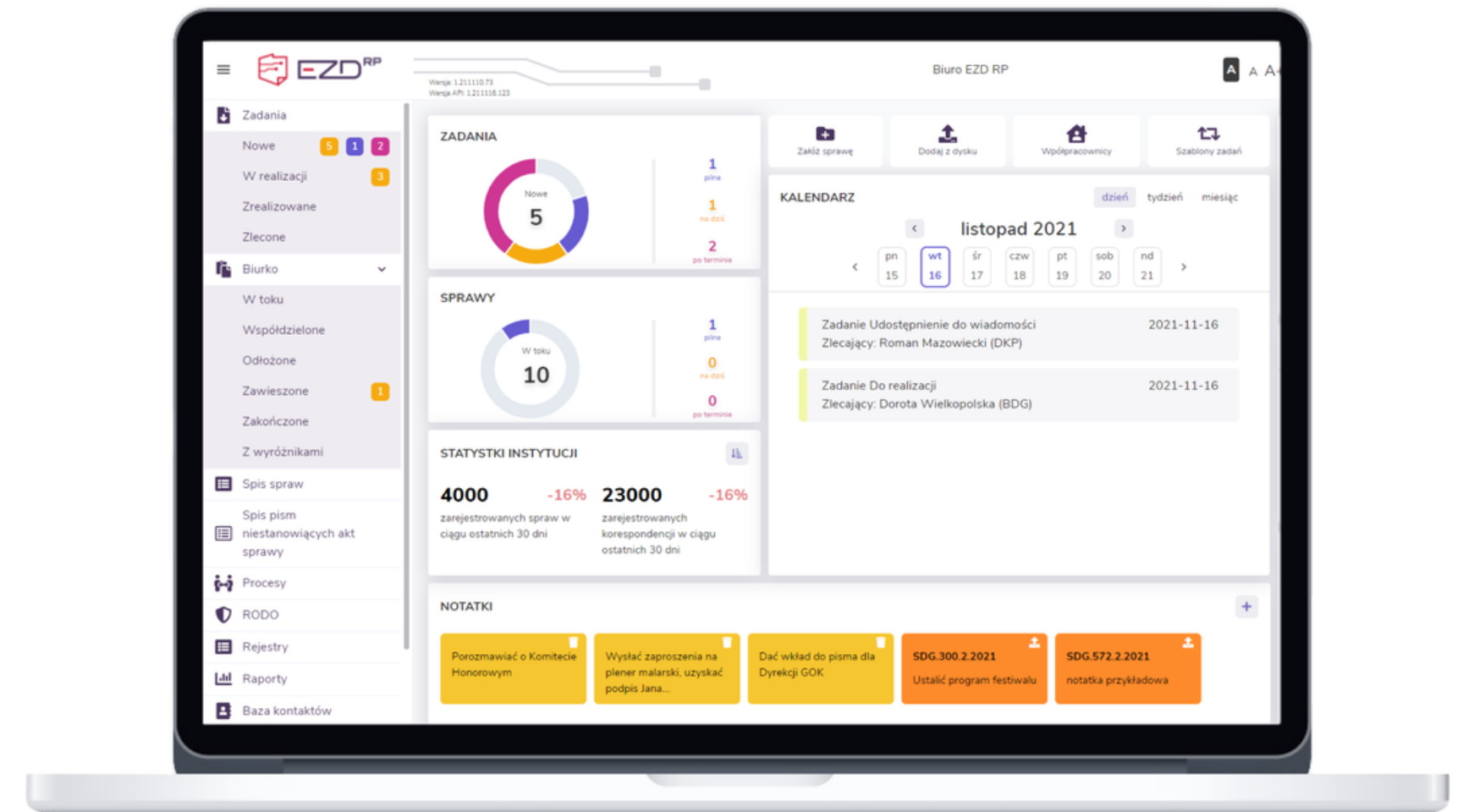
- Obsługa standardów: U2F; FIDO2
- Łączy: USB-A; Lightning; USB-C; NFC
- Wytrzymałość: Wodoodporność, mechaniczne uszkodzenia

Bezpieczna wymiana informacji i plików

WARIANTY WYMIANY

Wewnątrz jednostki

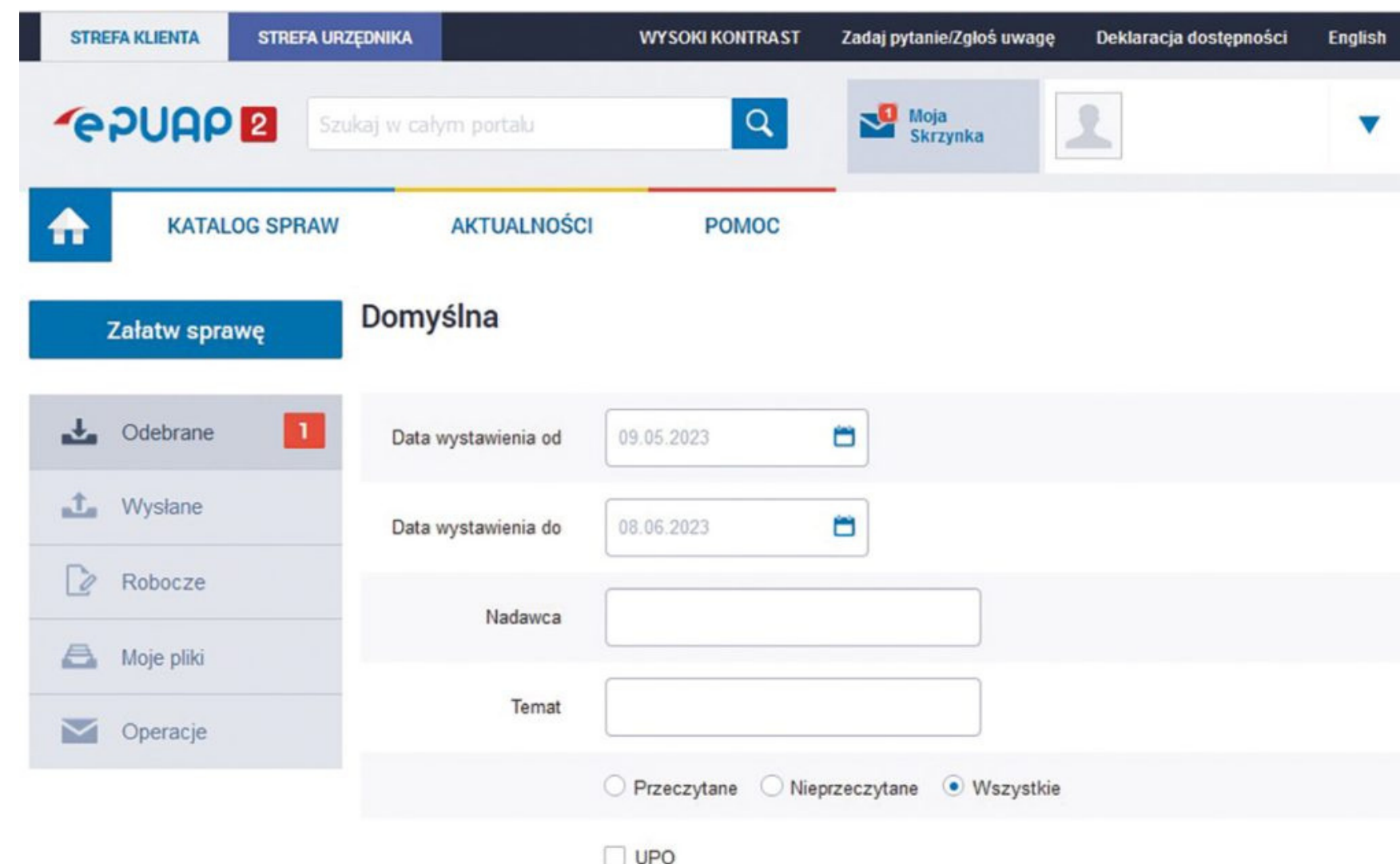
- Sieć wewnętrzna z szyfrowaniem
- Systemy EZD z kontrolą dostępu
- Bezpieczne foldery sieciowe



WARIANTY WYMIANY

Z jednostkami zewnętrznymi

- ePUAP - oficjalna korespondencja
- Szyfrowane e-maile (S/MIME)
- Bezpieczne portale wymiany plików



The screenshot shows the ePUAP portal interface. At the top, there is a navigation bar with tabs for 'STREFA KLIENTA' and 'STREFA URZĘDNIKA', along with links for 'WYSOKI KONTRAST', 'Zadaj pytanie/Zgłoś uwagę', 'Deklaracja dostępności', and 'English'. Below this is a search bar with the text 'Szukaj w całym portalu' and a magnifying glass icon. To the right of the search bar is a 'Moja Skrzynka' (My Mailbox) button with a red notification badge showing the number '1'. Below the search bar is a navigation bar with links for 'KATALOG SPRAW', 'AKTUALNOŚCI', and 'POMOC'. The main content area is titled 'Załatw sprawę' (Settle the matter) and 'Domyślna' (Default). It contains a sidebar with links for 'Odebrane' (Received), 'Wysłane' (Sent), 'Robocze' (Drafts), 'Moje pliki' (My files), and 'Operacje' (Operations). The main area displays a form for searching for documents, with fields for 'Data wystawienia od' (Issued from) and 'Data wystawienia do' (Issued to), both with date pickers. Below these are fields for 'Nadawca' (Sender) and 'Temat' (Subject). At the bottom, there are radio buttons for 'Przeczytane' (Read), 'Nieprzeczytane' (Unread), and 'Wszystkie' (All), and a checkbox for 'UPO'.

UNIKAJ

Prywatne e-maile



Komunikatory



Pendrive'y



PRYWATNE E-MAILE



W Urzędzie Marszałkowskim w Lublinie przez omyłkę wysłano e-mail z danymi setek pracowników (adresy, PESEL-e, numery telefonów).

5 minuty czytania • 22.08.2025 14:51

Wielki wyciek danych z Urzędu Marszałkowskiego. Adresy, numery PESEL i wysokość pensji pracowników



Sławomir Skomra
Dziennikarz



KOMUNIKATORY



Pracownik urzędu omyłkowo wysłał listę adresów osób przebywających na kwarantannie przez komunikator do niewłaściwej osoby.



Komunikatory a RODO w pracy – zasady i obowiązki

Dowiedz się, jak pogodzić komunikatory a RODO w pracy. Poznaj kluczowe zasady, przykłady naruszeń i kary nakładane przez UODO. Zadbaj o zgodność!

 Poradnik Przedsiębiorcy / Jul 16



PENDRIVE'Y



Zgubienie pendrive'a przez kuratora sądowego w Sądzie Rejonowym w Zgierzu

Kurator zgubił pendrive z danymi 400 osób objętych nadzorem. Prezes Sądu Rejonowego został ukarany przez UODO grzywną 10 tys. zł za naruszenie zasad poufności i braku odpowiedniego zabezpieczenia nośnika.

Strona główna > Aktualności > Zagubiony pendrive – administrator ukarany przez UODO

Zagubiony pendrive – administrator ukarany przez UODO

26.08.2021 • Autor: Michał Madecki •

SANKCJE, KARY FINANSOWE RODO



ĆWICZENIE PRAKTYCZNE

Ćwiczenie: Hasła, 2FA i bezpieczne przekazywanie plików

W kolejnych scenariuszach sprawdzisz, jak dobierać zabezpieczenia kont i kanały przesyłania plików.

Jak pracować z testem

- Przeczytaj scenariusz i wybierz rozwiązania, które najlepiej chronią konto lub dane.
- W części pytań poprawnych odpowiedzi może być kilka - zaznacz wszystkie właściwe.
- Po zaznaczeniu wszystkich odpowiedzi, kliknij przycisk "Sprawdź odpowiedzi" na dole strony.

1 Gdzie zapisac haslo?

Zakładasz prywatne konto na YouTube i tworzysz mocne, unikalne hasło.

Wybierz jedna odpowiedz.

A. Karteczka samoprzylepna na monitorze

B. Plik na komputerze (np. "hasla.docx")

C. Menedżer haseł przeglądarki

Ćwiczenie: Hasła 2FA
i bezpieczne przekazywanie plików



CYBERPRZESTĘPCZOŚĆ

SKALA PROBLEMU

Straty spowodowane cyberprzestępstwami: ok. 10,5 bln USD w 2025 r.

Źródło: Cybersecurity Ventures, Cybercrime to Cost the World \$10.5 Trillion Annually by 2025



Jeśli cyberprzestępstwo byłoby państwem, jego gospodarka zajmowałaby trzecie miejsce na świecie.

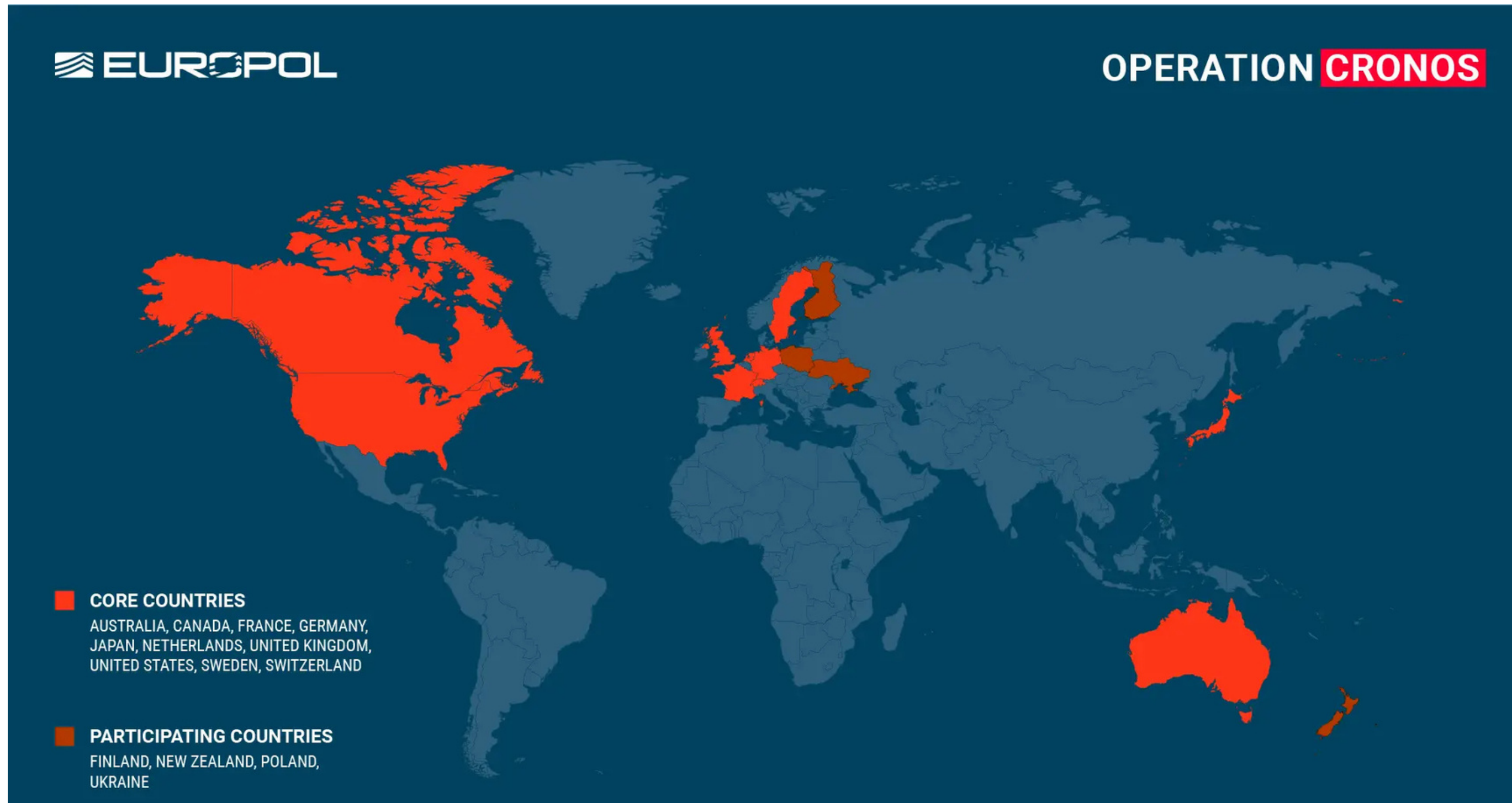
Cyberprzestępczość to dziś pełnoprawna branża — z własnymi procesami, ‘firmami’ i łańcuchem dostaw.

Zorganizowane grupy przestępcze:

LockBit - największy kartel ransomware

LAPSUS\$ - zasłynęła włamaniami do gigantów jak Microsoft, Okta, Samsung

ROZMIAR AKCJI LIKWIDACJI GRUPY LOCKBIT



CO TO PHISHING?

PHISHING

Phishing to metoda oszustwa polegająca na podszywaniu się przez cyberprzestępców pod zaufane osoby, instytucje lub firmy w celu wyłudzenia poufnych informacji

JAK ROZPOZNAĆ PHISHING?

-  Błędy gramatyczne i ortograficzne
-  Treść wzbudzająca wrażenie pilności, zagrożenia
-  Podejrzany adres URL (literówki, dziwne domeny)
-  Prośba o podanie poufnych informacji
-  Niezgodność nazwy domeny i nadawcy
-  Nietypowe załączniki (np. pliki .exe)

Pamiętaj: phishing to przede wszystkim psychologiczna gra, w której celem jest przekonanie Cię, że sytuacja jest prawdziwa i wymaga natychmiastowej reakcji.



ROZPOZNAWANIE I PIERWSZE KROKI

Phishing

Symptomy:

Podejrzane e-maile, linki, załączniki.

Pierwsze kroki:

Nie klikaj, zgłoś IT, ostrzeż zespół

Sledzenie trasy przesyłki DHL

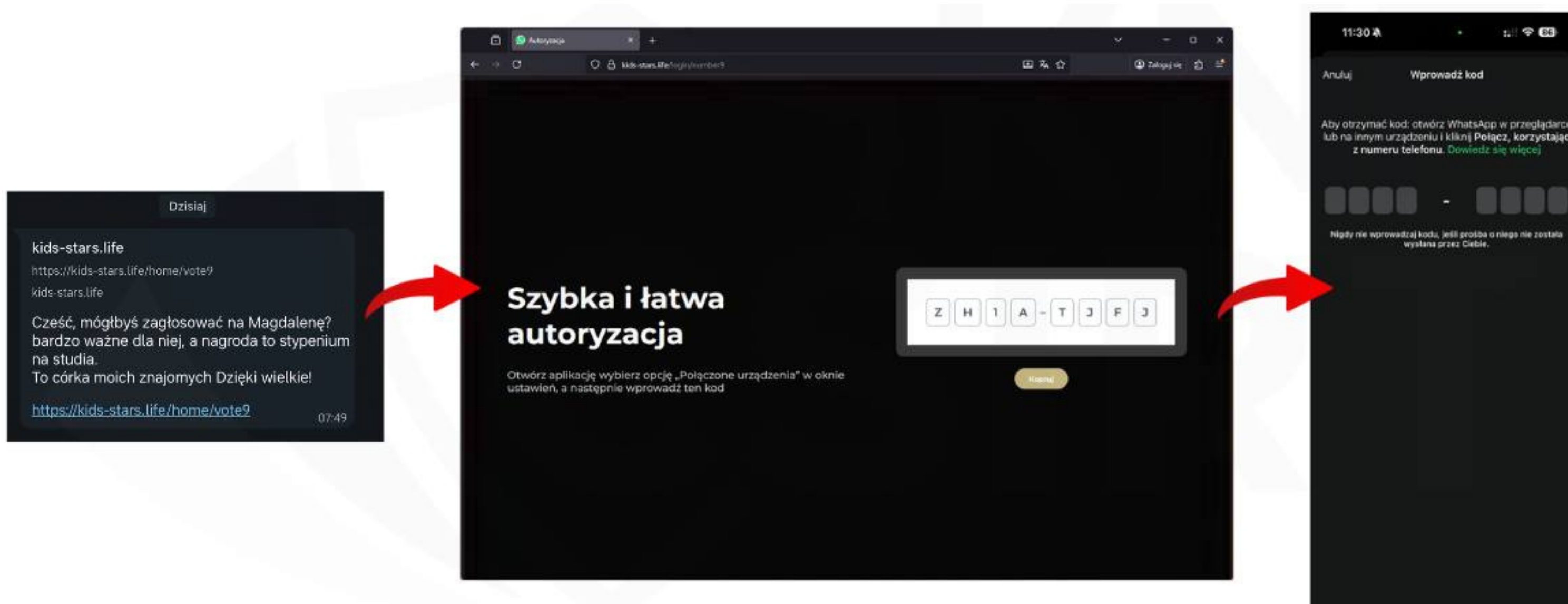
DHL Sendungsverfolgung

Numer przesyłki	3651537486436515
Produkt / serwis	DHL PAKET
Status od środa, 13.05.2015 12:18:29	Przesyłka jest chwilowo przechowywana w bazie doreczania z powodu wakacji, urlopu lub swiat.
Doreczono do	Przesyłka zwrotna do nadawcy http://devcosas.bluedigital.cl/g8sgwetsl Kliknij, aby śledzić łącze
<u>Wyswietl szczegółowe informacje od odbiorcy</u>	

PRZYKŁADY PHISHINGU:

1

Phishing - przejęcie konta WhatsApp



2

Phishing - "zwrot nadpłaty"

Krok 1:

Fałszywy email informuje o rzekomej nadpłacie za energię.

Zwrot środków – informacja

Szanowny Kliencie,

Po przeprowadzeniu okresowego przeglądu rozliczeń za energię elektryczną, stwierdzono różnicę pomiędzy przewidywanym a rzeczywistym zużyciem.

W wyniku tej korekty, system wygenerował kwotę do zwrotu – **przelew zostanie zrealizowany po potwierdzeniu poprawności danych bankowych.**

Kwota przewidziana do zwrotu:

279,29 PLN

Odsetki ustawowe: 6,12 PLN

W celu kontynuacji, prosimy o weryfikację danych przez dostępny kanał komunikacji. W celu klienta:

OSZUSTWO

Zweryfikuj dane

Sprawy: PGE/ZW/2025/009238

Data wystawienia: 11.09.2025

Wiadomość została wygenerowana automatycznie. W razie potrzeby kontaktu, prosimy skorzystać z dostępnych kanałów obsługi klienta PGE.

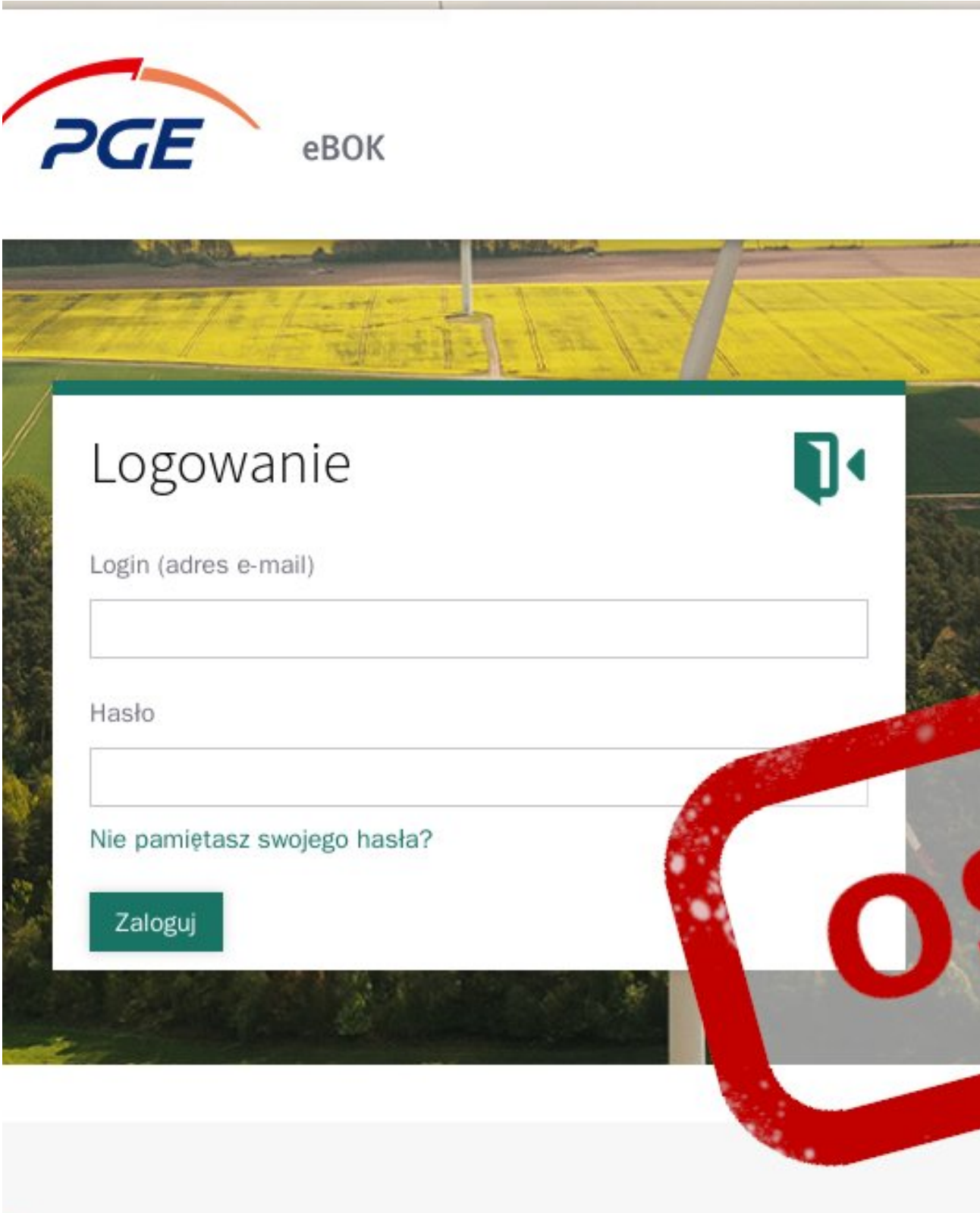
© 2025 Polska Grupa Energetyczna S.A.

2

Phishing - "zwrot nadpłaty"

Krok 2:

Link w wiadomości prowadzi na spreparowaną stronę podszywającą się pod PGE.



PGE eBOK

Logowanie

Login (adres e-mail)

Hasło

[Nie pamiętasz swojego hasła?](#)

Zaloguj

FAKTYCZNY

2



Krok 3:

Na fałszywej stronie przestępcy
wyłudzą dane karty płatniczej.



✓ Metoda zwrotu

SZYBKO I BEZPIECZNIE

☒ Metoda zwrotu



Numer karty

Imię

Nazwisko

Ważne do

Kod CVV



DETAILS

Kwota do zwrócenia

PLN 279,79

Kwota do zwrócenia

PLN 279,79

Numer zamówienia

ffba7993e4a923735e0fa99bt8ab284b

Odbiorca

PGE Polska

Numer

1041

Numer faktury

1010610472015/2025

Czy masz jakiegokolwiek problem z płatnościami? [Kliknij tutaj](#) aby przejść do strony pomocy

The administrator of personal data is Autopay S.A. [Przejdź do polityki prywatności](#)

© Autopay 1999 - 2025

OSZUSTWO

3

Phishing - bilety od nieautoryzowanych podmiotów



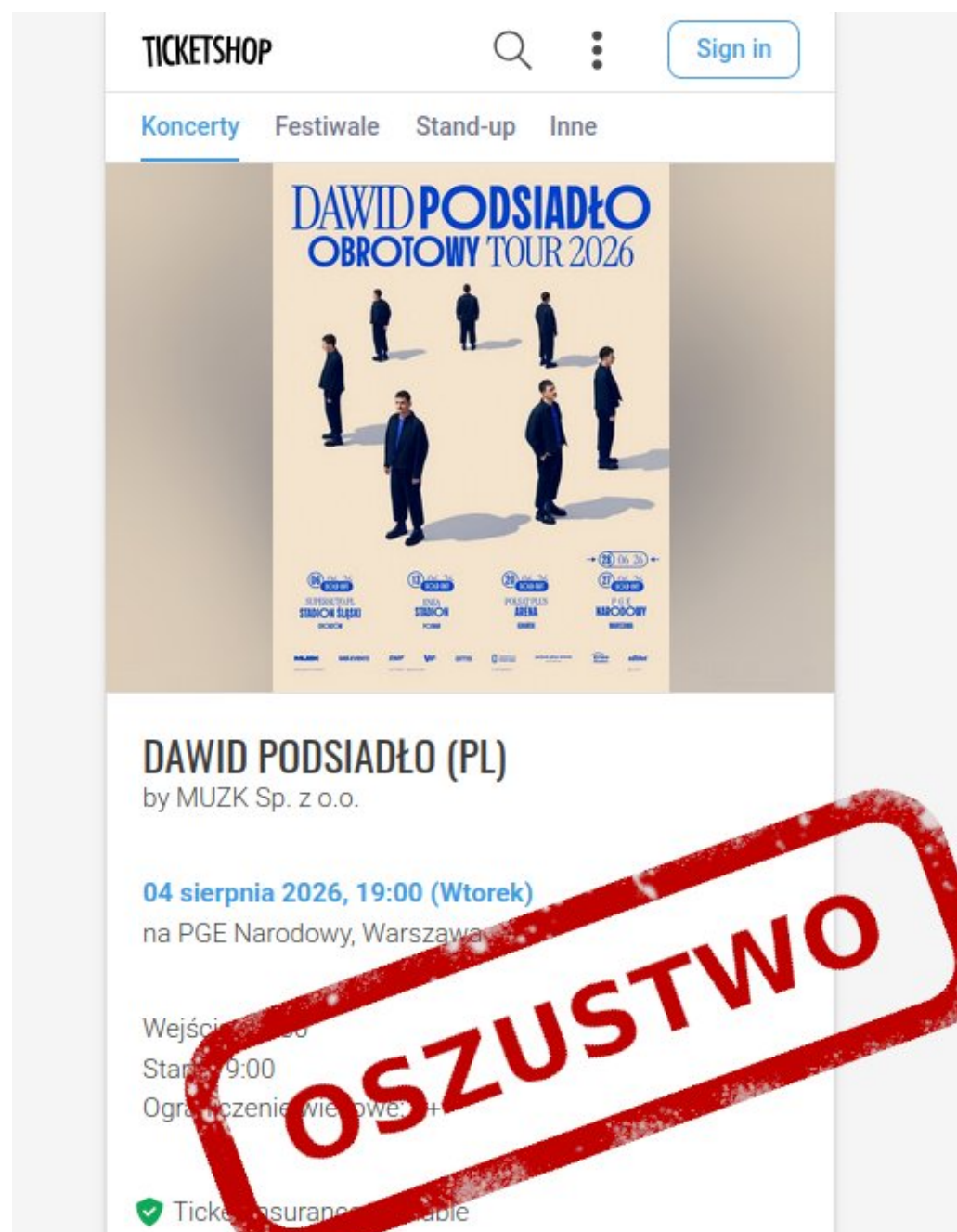
🔥 Metallica – M72 World Tour | Chorzów, 19 maja 2026



ROCKLIVE.PL

🔥 Kup bilet na Metallica - 2026 🙌 Kultowy koncert, którego nie można przegapić...

Learn More



TICKETSHOP

Koncerty Festiwale Stand-up Inne

DAWID PODSIADŁO
OBROTOWY TOUR 2026

DAWID PODSIADŁO (PL)
by MUZK Sp. z o.o.

04 sierpnia 2026, 19:00 (Wtorek)
na PGE Narodowy, Warszawa

Wejście: 19:00
Start: 19:00
Ograniczenie wiekowe: +

Ticket insurance: available

OSZUSTWO

Informujemy o nowej puli biletów na Dawid Podsiadło – Obrotowy Tour 2026

Dołącz do wydarzenia w Warszawie na PGE Narodowym
Sobota, 27 czerwca 2026 r. | start godz. 18:00



DAWID PODSIADŁO
OBROTOWY TOUR 2026

PGE NARODOWY WARSZAWA

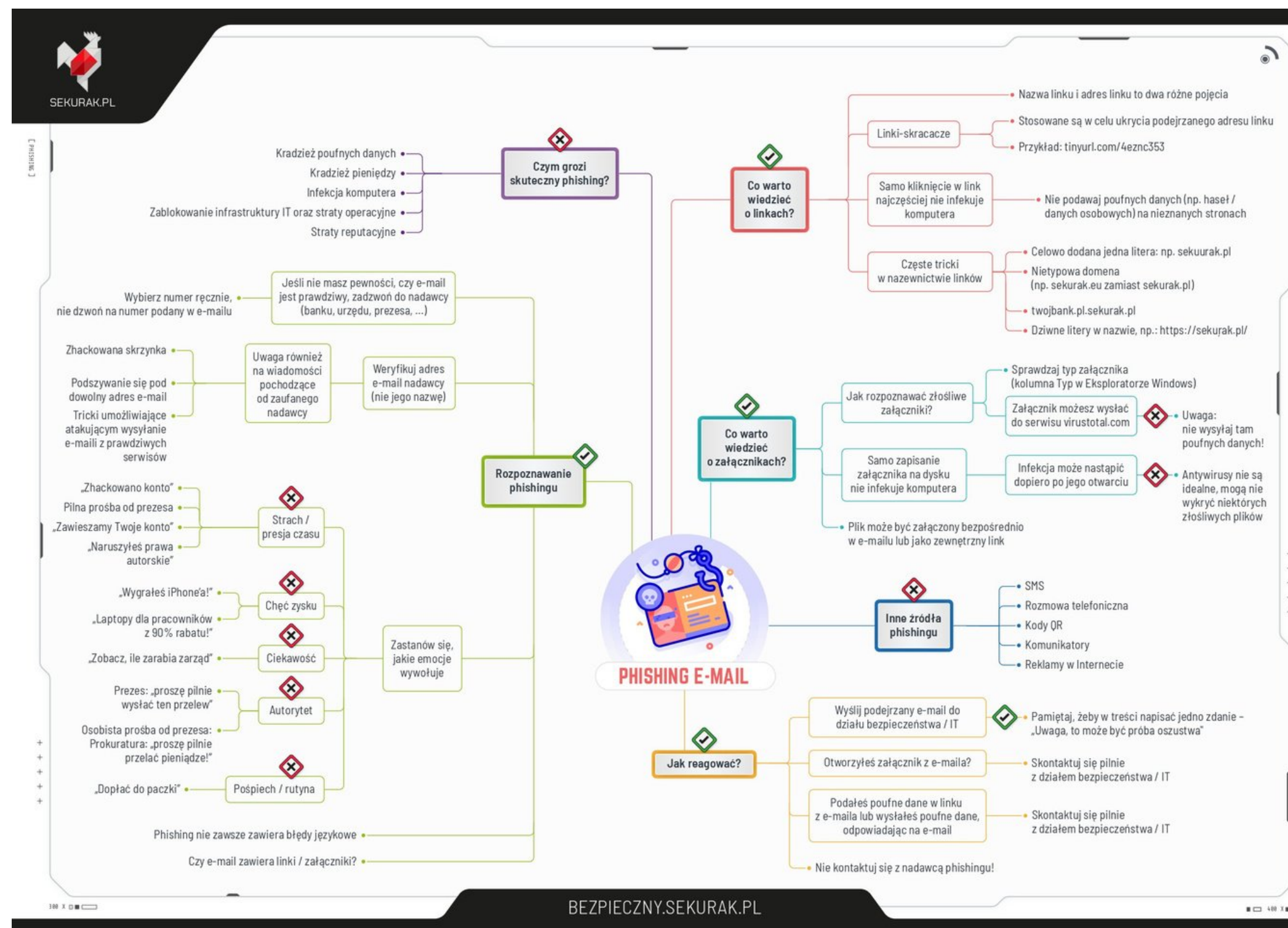
TICKETSHOPPL.COM

Dawid Podsiadło – Obrotowy Tour 2026 | Warszawa |
PGE Narodowy | 27 czerwca 2026

OSZUSTWO

Dowiedz się...

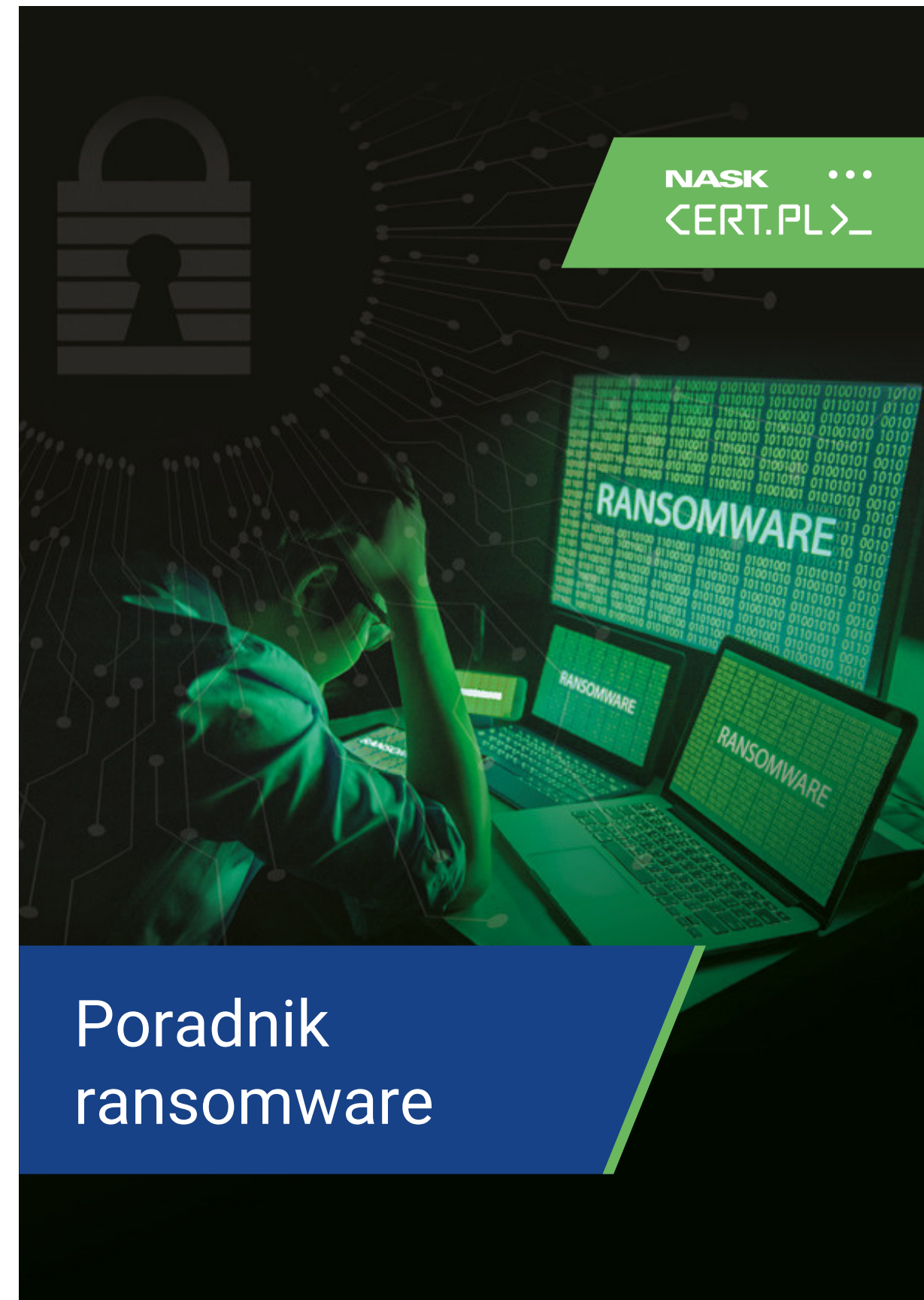
PHISHING E-MAIL - WIEDZA W PIGUŁCE



CO TO RANSOMWARE?

RANSOMWARE

Ransomware to złośliwe oprogramowanie, które szyfruje pliki lub blokuje system i żąda okupu za przywrócenie dostępu, często dodatkowo wykrada dane i grozi ich ujawnieniem.



RANSOMWARE

Symptomy:

Zablokowane pliki, żądanie okupu

Pierwsze kroki:

Odłącz komputer, zgłoś incydent



JAK MOŻE WYGLĄDAĆ ŻĄDANIE OKUPU?



Po instalacji ransomware na ekranie pojawia się komunikat z żądaniem okupu, a dostęp do plików i systemu zostaje zablokowany.

PRZYKŁADY ZASTOSOWANIA RANSOMWARE

Hakerski atak na szpital MSWiA w Krakowie z 8 marca 2025 roku

W systemach informatycznych placówki pojawiła się informacja od osób, które dokonały ataku z żądaniem kontaktu.

Szpital był zmuszony przejść tymczasowo na dokumentację papierową.



Groźny cyberatak na szpital MSWiA w Krakowie

– Szpital MSWiA w Krakowie stał się celem cyberataku. To był groźny atak – poinformował wicepremier, minister cyfryzacji Krzysztof Gawkowski. Uspokoił jednocześnie, że wdrożono procedury awaryjne i nie ma zagrożenia dla życia oraz...

 MenedzerZdrowia



PRZYKŁADY ZASTOSOWANIA RANSOMWARE

Incydent w Acer - marzec 2021

Atak grupy REvil

Okup wynosił aż **50 mln \$**

Firma była zmuszona czasowo
wstrzymać dostęp do kluczowych
systemów IT oraz zabezpieczyć dane
klientów.



Acer Faced With Ransom Up To \$100 Million After Hackers Breach Network

The criminals are demanding a massive \$50 million from their latest target: Taiwanese computer manufacturer Acer. It could climb as high as \$100 million.

F Forbes / Jun 4, 2024



CZYM JEST WYCIEK DANYCH?

WYCIEKI DANYCH

Wyciek danych to incydent bezpieczeństwa, w wyniku którego poufne, chronione lub wrażliwe informacje trafiają w ręce nieupoważnionych osób lub podmiotów

Interaktywny wykres „World's Biggest Data Breaches” — prezentujący największe światowe wycieki danych i ich skalę:



WYCIEKI DANYCH

Symptomy:

Nieautoryzowany dostęp, podejrzana aktywność

Pierwsze kroki:

Zmień hasła, dokumentuj, eskaluj



Ataki hakerskie i złośliwe oprogramowanie (malware)



Błędy ludzkie (przypadkowe udostępnienie informacji, pomyłki)



Nieprawidłowa konfiguracja systemów oraz usług chmurowych



Kradzież lub zagubienie sprzętu z danymi (laptopy, dyski, pendrive'y)

WYCIEKI DANYCH W MCDONALD'S POLSKA

W 2025 roku UODO nałożył karę 16,9 mln zł
za wyciek danych pracowników

Wypadek był spowodowany nieprawidłową
konfiguracją serwera podwykonawcy.



WYCIEKI DANYCH W MINISTERSTWIE CYFRYZACJI



Ministerstwo
Cyfryzacji

W 2024 roku doszło do wycieku danych z powodu błędu pracownika ministerstwa, który przekazał osobie nieuprawnionej dane dotyczące wynagrodzeń.



Najgłośniejsze cyberincydenty w 2024 roku w Polsce i na świecie

Mijający rok przyniósł falę cyberincydentów, których doświadczały zarówno polskie, jak i zagraniczne organizacje. Od Microsoftu przez POLADA po Sanok Rubber Company S.A. – cyberprzestępcy łamią zabezpieczenia, wykradają dane i...

6 PL_SecurityMaga /

WYCIEKI DANYCH Z ALAB, LABORATORIA MEDYCZNE



W listopadzie 2023 roku doszło do największego wycieku danych medycznych w historii Polski z laboratoriów ALAB.

Cyberprzestępcy za pomocą ransomware przejęli i odszyfrowali serwer firmy, wykradając i publikując dane nawet 200 tysięcy pacjentów z lat 2017–2023



ATAK GRUPY NIGHTSPIRE NA PUP W ŻORACH

31 marca 2025 roku grupa ransomware NightSpire zaatakowała Powiatowy Urząd Pracy w Żorach.

Cyberprzestępcy wykradli około 100 GB danych, a następnie opublikowali je w otwartej sieci. Wśród ujawnionych informacji znalazły się numery PESEL i adresy zamieszkania pracowników, korespondencja z Policją dotycząca rejestracji osób bezrobotnych, dokumenty przekazywane sądom, karty wypłat zasiłków oraz umowy o pracę.

Analiza ujawnionych materiałów objęła 18 210 plików z 8 spośród 20 dostępnych katalogów — co oznacza, że pełna skala wycieku może być jeszcze większa.

Incydent został zgłoszony do CERT Polska.



WYCIEKI DANYCH W URZĘDZIE MIASTA MYSZKÓW

18 marca 2026 roku doszło do cyberataku na infrastrukturę informatyczną Urzędu Miasta w Myszkowie.

Systemy urzędowe zostały zaszyfrowane, co sparaliżowało część usług — między innymi przestała działać kasa urzędu. Wśród zagrożonych danych znalazły się numery PESEL, imiona i nazwiska oraz adresy e-mail mieszkańców.

Sprawę niezwłocznie zgłoszono do Urzędu Ochrony Danych Osobowych, zespołu CSIRT NASK oraz organów ścigania. Urząd zaapelował do mieszkańców o zachowanie szczególnej ostrożności wobec podejrzanych telefonów i wiadomości e-mail, a także o rozważenie zastrzeżenia numeru PESEL.



SPRAWDŹ CZY TWOJE DANE WYCIEKŁY



bezpiecznedane.gov.pl



bezpiecznedane.gov.pl

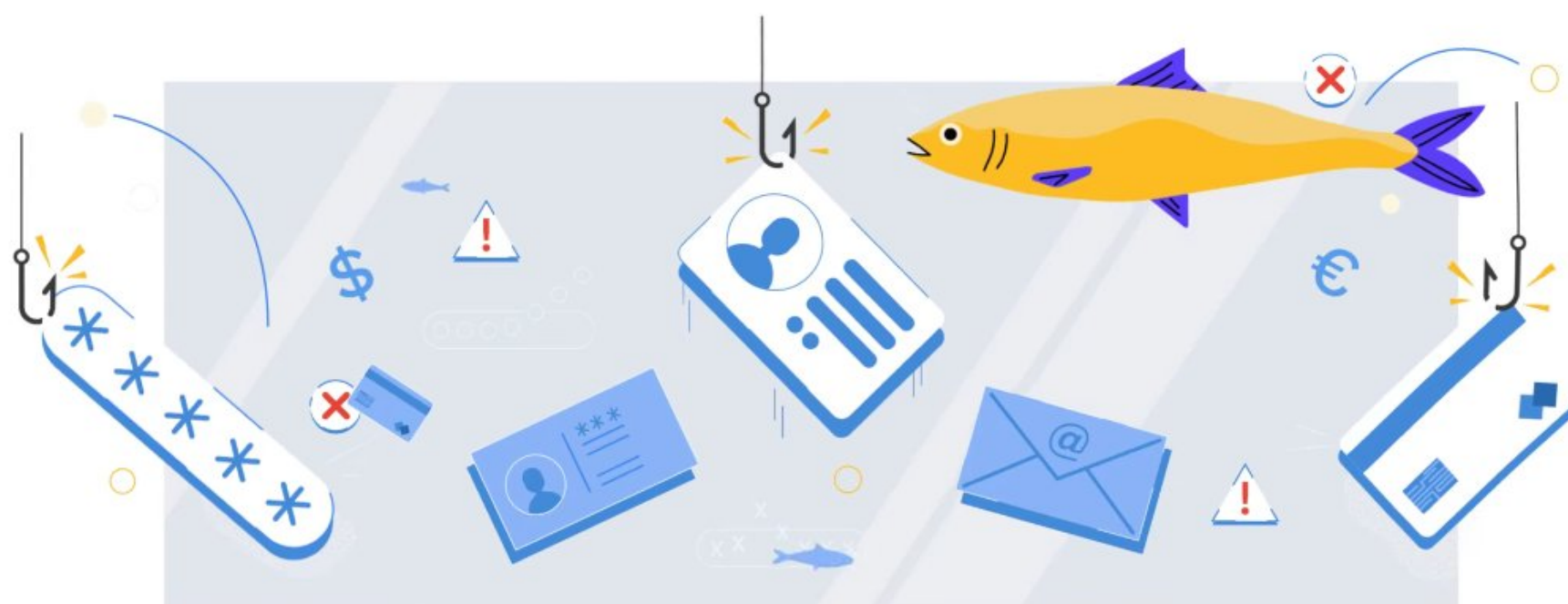
Sprawdź, czy Twoje dane są bezpieczne

Zaloguj się i sprawdź, czy Twoje dane nie zostały udostępnione w sieci!
Korzystanie z naszej wyszukiwarki jest darmowe.

[Sprawdź dane](#)



SPRAWDŹ JAK ROZPOZNAĆ PRÓBĘ WYŁUDZENIA INFORMACJI



Ćwiczenie: Quiz od Google



REAKCJA NA INCYDENT CYBERBEZPIECZEŃSTWA

Ścieżka postępowania: natychmiast poinformuj przełożonego oraz odpowiednią osobę



Ścieżka postępowania: odłącz komputer od sieci, zachowaj dowody



Odłącz zagrożone urządzenie lub system od sieci



Unikaj wykonywania zbędnych operacji na zainfekowanym sprzęcie



Zachowaj wszelkie dowody (np. logi, pliki, zapisy ekranów)

JAKIE SŁUŻBY MOŻEMY POWIADOMIĆ?

CERT NASK (CERT Polska)
sektor cywilny
JST (gminy, powiaty, województwa)



Formularz: **incydent.cert.pl**
Adres e-mail: **cert@cert.pl**
Numer telefonu: **+48 22 380 82 74**
Termin: **do 24h od wykrycia incydentu**

POZOSTAŁE CSIRT-Y (NIE DOTYCZĄ JST)

CSIRT GOV

administracja rządowa i państwowa
(ministerstwa, urzędy centralne)



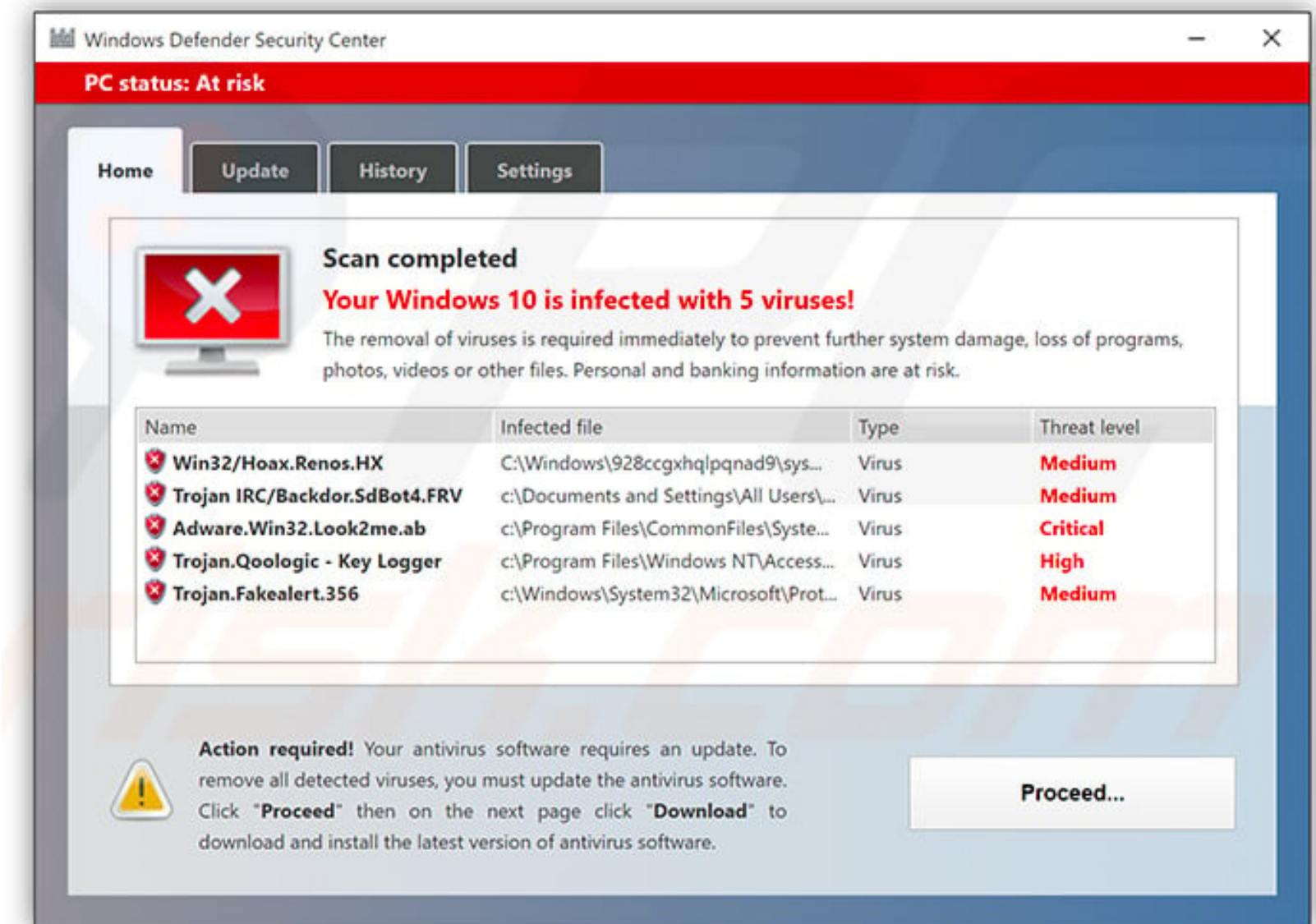
CSIRT MON

sektor wojskowy



ŚCIEŻKA POSTĘPOWANIA: ZAPISZ WSZYSTKIE DZIAŁANIA

- Notuj każdy krok podjęty podczas reagowania na incydent
- Zapisuj daty, godziny, nazwy osób i opisy czynności
- Przechowuj kopie dowodów i logów systemowych
- Dokumentuj komunikację z zespołem IT oraz CSIRT
- Sporządzaj raport końcowy z przebiegu incydentu



ĆWICZENIE: KARTA INCYDENTU

Scenariusz:

Otrzymałeś e-mail od oszusta, który podszywa się za “dyrektora” z prośbą o pilne przesłanie listy pracowników z numerami PESEL na prywatny adres e-mail, bo “system nie działa”.

**Ćwiczenie: Karta reakcji na incydent**

W pracy trafia do Ciebie podejrzany e-mail. Zrozum, co trzeba sprawdzić w wiadomości i jakie kroki zgłoszenia wykonać, aby właściwie zareagować.

Otrzymana wiadomość

Temat: Pilne: lista pracowników z numerami PESEL **Data:** Dziś, godz. 09:42

AZ **Adam Zieliński** <adam.zielinski@gmail.com>
Do: kadry@urzed.pl

Dzień dobry,

Dziś odbywa się nieplanowana kontrola z Urzędu Skarbowego i muszę natychmiast przedłożyć pełną listę pracowników z numerami PESEL. Niestety system HR jest chwilowo niedostępny, dlatego proszę o przesłanie zestawienia na mój prywatny adres: adam.zielinski@gmail.com.

Bardzo zależy mi, by otrzymać tę listę w ciągu **najbliższych 30 minut** — jest to niezbędne do zakończenia kontroli!

Pozdrawiam,
Adam Zieliński
Dyrektor

KROK 1 Analiza wiadomości

Zadanie: Poniżej znajdują się cechy otrzymanej wiadomości. Twoim zadaniem jest wskazanie TYLKO tych elementów, które świadczą o **próbie oszustwa**. Uważaj – niektóre zdania opisują normalną sytuację biurową!

Ćwiczenie: Karta incydentu



ZAGRAJ W NASZĄ SYMULACJĘ “REAKCJA NA PODEJRZANY E-MAIL”



Quest. Podejrzany mail w JST

Interaktywny trening reagowania na phishing

Fabula scenariusza

To zwykły dzień roboczy w urzędzie. Wykonujesz poranne obowiązki, nadrabiasz maile mieszkańców i myślisz o kolejnych punktach planu dnia.

Niespodziewanie dostajesz wiadomość oznaczoną jako bardzo pilną od Twojego kierownika, który prosi o natychmiastową aktualizację danych kadrowych. Czy to faktycznie służbowa prośba, czy zręcznie przygotowana przynęta? Ten quest pozwoli Ci to sprawdzić.

Cel szkolenia

- Rozpoznawanie phishingu w praktyce
- Weryfikacja nadawcy i nagłówek wiadomości
- Właściwa reakcja i zgłaszanie incydentów
- Dokumentowanie i komunikacja w zespole

1 Pierwszy kontakt z mailem

Otrzymujesz wiadomość od kierownika. Co robisz?

Pamiętaj: zawsze sprawdź nadawcę przed podjęciem działań.

Klikam w link i wypełniam formularz - to przecież od

Symulator poczty

Pilne: Aktualizacja danych pracowników do końca dnia

KJ Kierownik JST
kiern@wik@urzed-jst.info

Quiz: Podejrzany mail w JST



STWÓRZ WŁASNY WZÓR POLITYKI BEZPIECZEŃSTWA INFORMACJI (SYMULACJA)



Polityka bezpieczeństwa informacji



Ćwiczenie: Polityka bezpieczeństwa

Przećwicz przygotowanie polityki bezpieczeństwa: wybierz najbezpieczniejsze zasady i od razu zobacz, jak zmienia się finalny dokument.

Twoja Misja:

Jesteś teraz odpowiedzialna za bezpieczeństwo urzędu. Twoim zadaniem jest przeczytać każde pytanie i wybrać najbezpieczniejszą opcję.

● Zielony = Decyzja bezpieczna ● Czerwony = Ryzyko! Spróbuj wybrać inaczej.

● Żółty = Dopuszczalne, ale są lepsze opcje

1. Dane Urzędu

Nazwa jednostki

np. Urząd Gminy Przykład

Osoba odpowiedzialna

np. Jan Kowalski

Data

03/31/2026



[Nazwa Jednostki]

31 marca 2026

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Dokument wygenerowany przez Kreator Polityki Bezpieczeństwa JST

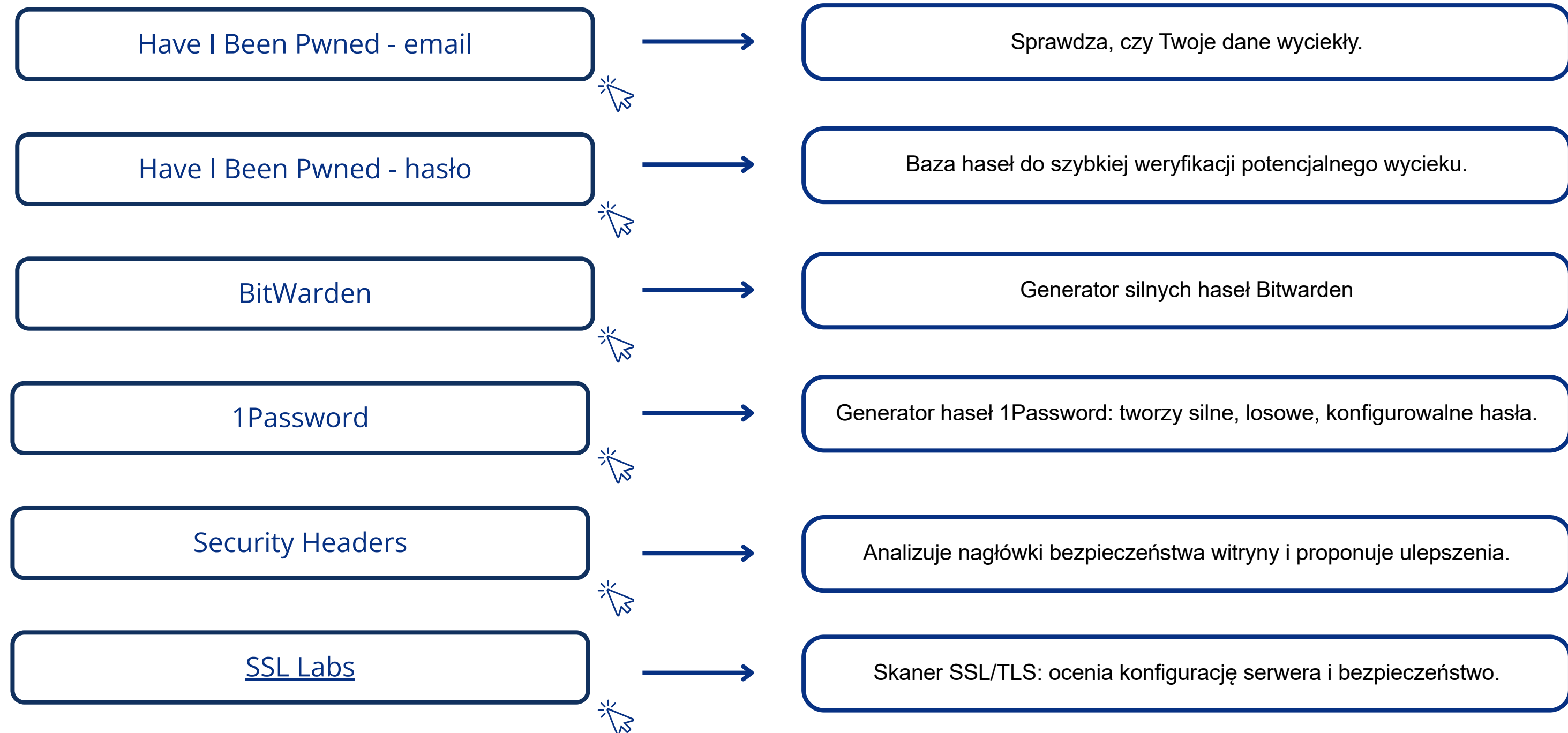
§1 Postanowienia ogólne

Niniejsza Polityka Bezpieczeństwa Informacji (zwana dalej „Polityką”) określa zasady ochrony informacji przetwarzanych w [Nazwa Jednostki]. Polityka obejmuje wszystkich pracowników, współpracowników oraz podmioty trzecie mające dostęp do systemów informatycznych jednostki.

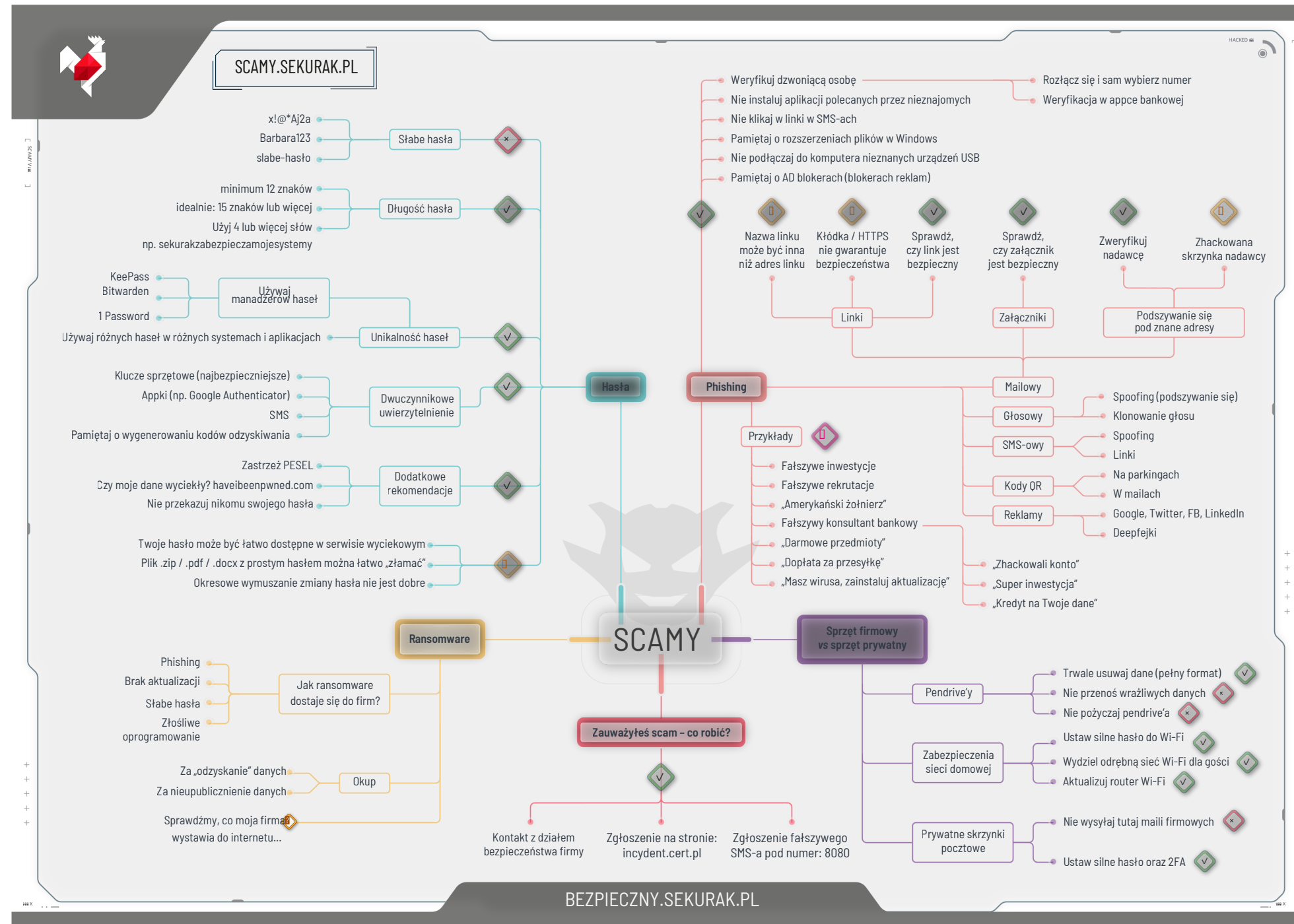
Celem Polityki jest zapewnienie poufności, integralności i dostępności informacji zgodnie z wymaganiami Krajowych Ram Interoperacyjności (KRI), Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa.

§8 Postanowienia końcowe

PRZYDATNE PLATFORMY:



MAPA ZAGROŻENIA



Dziękujemy za uwagę!

Pamiętaj! Cyberbezpieczeństwo to odpowiedzialność każdego pracownika!
