mWeryfikatorStron

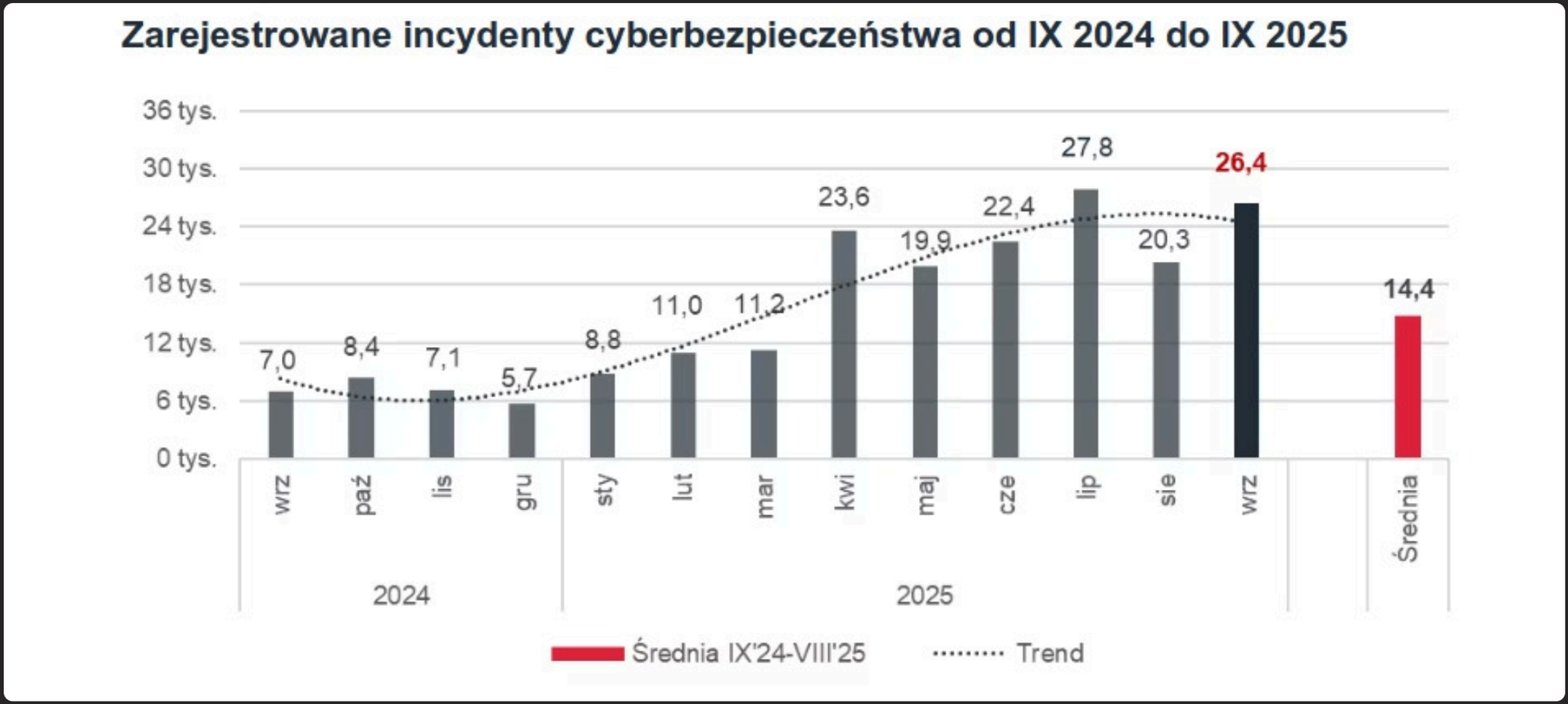
Prezentacja rozwiązania przeciwko phishingowi

Tomasz Dłuski & Tomasz Zelinski

Drużyna T&T

Phishing: rosnące zagrożenie cyfrowe

Liczba ofiar ataków phishingowych systematycznie wzrasta z roku na rok. Postęp w technologiach AI ułatwia cyberprzestępcom tworzenie coraz bardziej przekonujących oszustw, sprawiając że tradycyjne metody ochrony stają się niewystarczające.



Źródło: CERT Polska / CSIRT NASK.

Dlatego nasze rozwiązanie musi być **proste w obsłudze** i **skuteczne** — dostępne dla każdego użytkownika, niezależnie od poziomu wiedzy technicznej.

Wyzwanie: niskie kompetencje cyfrowe

Problem

Większość użytkowników internetu nie posiada wystarczających kompetencji technicznych, aby samodzielnie rozpoznać zaawansowane ataki phishingowe.

- Brak świadomości zagrożeń
- Trudność w weryfikacji autentyczności stron
- Zaufanie do wiarygodnie wyglądających wiadomości
- Błędy nawet świadomych użytkowników pod presją czasu

Nawet doświadczeni użytkownicy, działający pod presją czasu lub w środowisku pełnym dezinformacji, mogą popełnić błąd, klikając w fałszywy link.

Nasze podejście

Rozwiązanie musi działać automatycznie, bez wymagania specjalistycznej wiedzy od użytkownika.

- Intuitywny interfejs
- Automatyczna weryfikacja
- Jasne komunikaty ostrzegawcze

Automatyczna weryfikacja i jasne komunikaty zapewniają ochronę każdemu, niezależnie od poziomu jego kompetencji cyfrowych, minimalizując ryzyko błędu ludzkiego.

Rozwiązanie webowe w akcji

Nasza wtyczka przeglądarkowa działa w czasie rzeczywistym, analizując każdą odwiedzaną stronę i ostrzegając użytkownika przed potencjalnym zagrożeniem.

01

Instalacja wtyczki

Użytkownik pobiera rozszerzenie z oficjalnego sklepu przeglądarki

02

Automatyczna analiza

Wtyczka skanuje każdą odwiedzaną stronę w tle

03

Ostrzeżenie

System wyświetla alert przy wykryciu zagrożenia

04

Bezpieczne przeglądanie

Użytkownik może kontynuować bezpieczną nawigację

Interfejs został zaprojektowany z myślą o prostocie — kolorowe wskaźniki i zrozumiałe komunikaty prowadzą użytkownika przez automatyczny proces weryfikacji.

A co ze smartfonami?

Przeglądarka mobilna nie obsługuje tradycyjnych wtyczek. Jak więc chronić użytkowników korzystających z telefonów i tabletów?

Wyzwanie: 75,8 proc. Polaków korzysta ze smartfona, gdzie instalacja rozszerzeń przeglądarki jest niemożliwa.

Potrzebujemy natywnego rozwiązania mobilnego!

Weryfikacja przez mObywatel

Nasza innowacyjna integracja z aplikacją mObywatel umożliwia bezpieczną weryfikację linków bezpośrednio na smartfonie.

Krok 1: Udostępnij

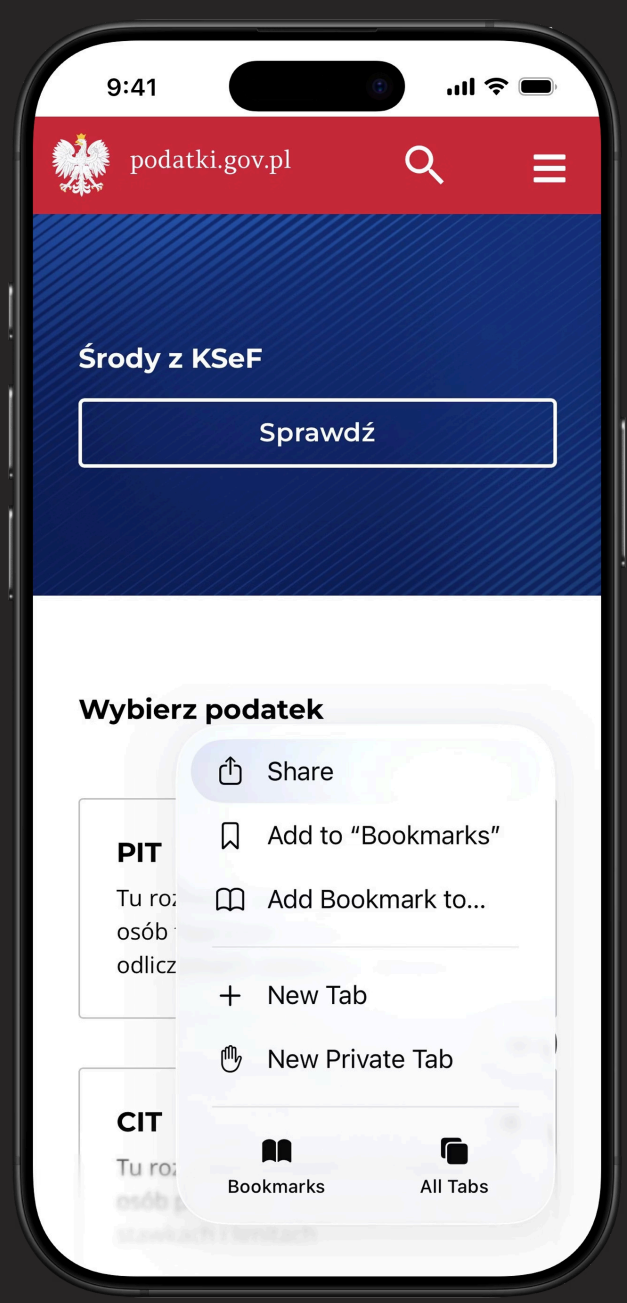
Użytkownik klika „Udostępnij" w przeglądarce mobilnej

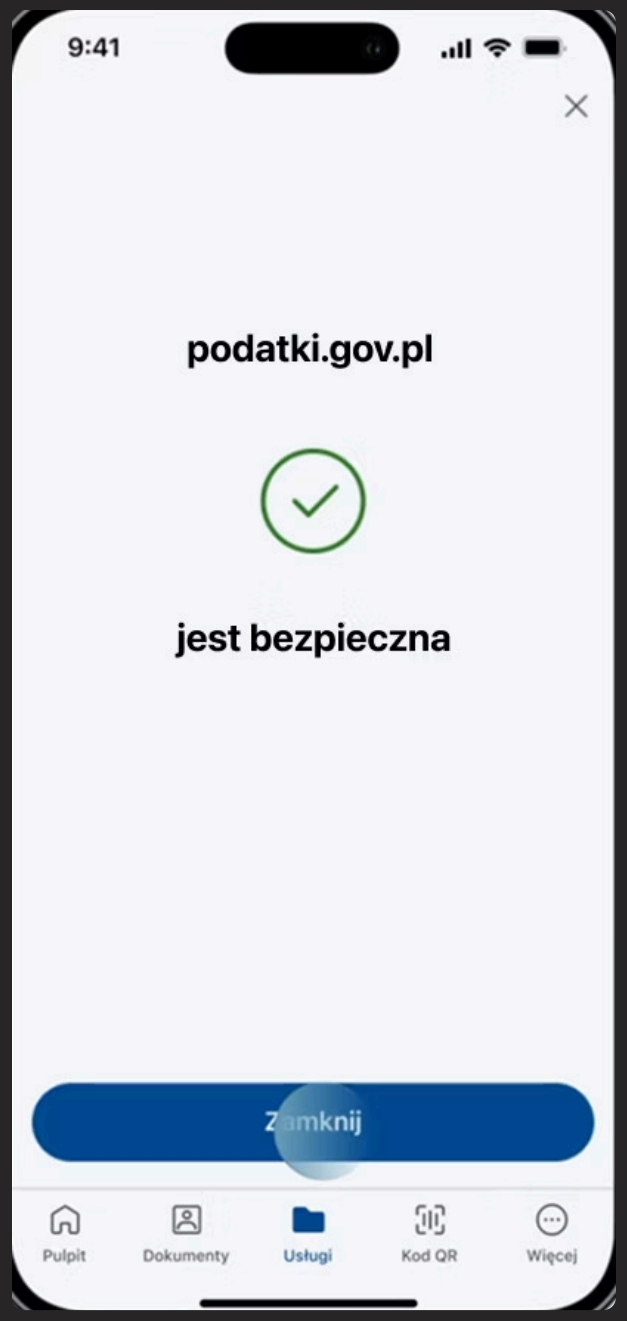
Krok 2: Wybierz mObywatel

Z listy opcji wybiera „mObywatel"

Krok 3: Weryfikacja

Aplikacja analizuje link i wyświetla wynik sprawdzenia





Architektura rozwiązania mobilnego

Warstwa aplikacji

Natywna integracja z menu udostępniania iOS/Android

Baza wiedzy

Stale aktualizowana lista znanych zagrożeń

Wymagania implementacyjne

Zespół mObywatel musi zaimplementować nową opcję w menu udostępniania systemu operacyjnego:

- **iOS:** Rozszerzenie Share Extension z własnym URL scheme
- **Android:** Intent handler dla ACTION_SEND z filtrem URL
- **Backend:** Endpoint REST API do weryfikacji linków w czasie rzeczywistym

Plan wdrożenia i promocji

Skuteczna kampania edukacyjna wymaga dotarcia do szerokiej publiczności przez różnorodne kanały komunikacji.

Materiały drukowane

Ulotki i plakaty informacyjne w urzędach, przychodniach, bibliotekach i innych placówkach użyteczności publicznej

Kampania telewizyjna

Krótkie spoty edukacyjne emitowane w telewizji publicznej, pokazujące jak korzystać z narzędzia

Wsparcie MC

Ministerstwo Cyfryzacji aktywnie wspiera inicjatywy cyberbezpieczeństwa i pomoże w dystrybucji rozwiązania

Grupa docelowa

- Seniorzy i osoby starsze
- Użytkownicy z niskimi kompetencjami cyfrowymi
- Pracownicy sektora publicznego
- Osoby często korzystające z bankowości online

Przyszłe rozszerzenia funkcjonalności

Nasza platforma ma potencjał do rozwoju w kierunku kompleksowego narzędzia bezpieczeństwa online.

Analiza treści

Skanowanie zawartości strony w poszukiwaniu podejrzanych elementów i manipulacyjnych treści

Detekcja AI

Wykorzystanie uczenia maszynowego do wykrywania nowych, nieznanych wzorców ataków

Ochrona danych

Automatyczne ostrzeżenia przed formularzami żądającymi wrażliwych informacji