Finansowane przez Unię Europejską

FUNDACJA EGIDA

BEZPIECZNI W SIECI

Poradnik cyberbezpieczeństwa dla seniorów

Jak bezpiecznie korzystać z internetu
i nie dać się oszukać w sieci

Projekt „Bezpieczni w sieci”
Nr projektu: 2024-3-PL01-ESC30-SOL-000282674
Europejski Korpus Solidarności | Fundacja pomocy prawnej EGIDA, Opole
Opole 2026

Drogi Seniorze, Droga Seniorko,

Internet to wspaniałe narzędzie — pozwala kontaktować się z rodziną, robić zakupy, płacić rachunki, korzystać z usług urzędowych i czerpać rozrywkę. Ale — jak każde narzędzie — wymaga ostrożności.

Ten poradnik przygotowali dla Ciebie młodzi wolontariusze z Opola w ramach projektu „Bezpieczni w sieci". Zebraliśmy w nim najważniejsze zasady, które pomogą Ci bezpiecznie korzystać z internetu i uchronić się przed oszustami.

Nie musisz pamiętać wszystkiego naraz. Wracaj do poszczególnych rozdziałów w razie potrzeby. Przy każdym temacie znajdziesz kolorowe ramki z najważniejszymi wskazówkami:

✓ Zapamiętaj!

Zielona ramka — najważniejsze zasady, które warto zapamiętać.

⚠ Uwaga! Nie daj się oszukać!

Czerwona ramka — ostrzega przed typowymi oszustwami i zagrożeniami.

Praktyczna wskazówka

Niebieska ramka — pomocne rady do zastosowania na co dzień.

Masz pytania? Zadzwoń do kogoś z rodziny lub odwiedź Fundację EGIDA w Opolu. Jesteśmy tu dla Ciebie!

SPIS TREŚCI

MODUŁ 1

Podstawy bezpiecznego korzystania z internetu

Hasła, aktualizacje, sieci Wi-Fi

Bezpieczne korzystanie z internetu zaczyna się od kilku prostych nawyków. Dotyczą one przede wszystkim haseł, aktualizacji oprogramowania oraz korzystania z sieci bezprzewodowych.

Bezpieczne hasła

Hasło to Twój klucz do konta. Im jest mocniejsze, tym trudniej je odgadnąć złodziejowi.

✓ Zapamiętaj!

Hasło powinno mieć co najmniej 8 znaków (najlepiej 12 lub więcej).

Używaj dużych i małych liter, cyfr oraz znaków specjalnych (np. !, @, #).

Nie używaj jako hasła swojego imienia, daty urodzenia ani słowa „hasło”.

Stosuj inne hasło do każdego ważnego konta (e-mail, bank, sklep).

Możesz zapisać hasła w bezpiecznym miejscu — np. w zeszycie przechowywanym w domu.

⚠ Uwaga! Nie daj się oszukać!

Nigdy nie podawaj hasła przez telefon, SMS ani e-mail — nawet jeśli ktoś twierdzi, że dzwoni z banku.

Pracownicy banków i firm NIGDY nie proszą o podanie pełnego hasła.

Aktualizacje oprogramowania

Aktualizacje to poprawki, które usuwają błędy w programach i systemie. Dzięki nim Twój komputer, tablet i telefon są chronione przed nowymi zagrożeniami.

Praktyczna wskazówka

Włącz automatyczne aktualizacje w ustawieniach systemu Windows, Android lub iOS.
Aktualizuj przeglądarkę internetową (np. Chrome, Firefox, Edge).
Aktualizuj program antywirusowy — najlepiej raz w tygodniu.

Sieci Wi-Fi

Sieć Wi-Fi to bezprzewodowe połączenie z internetem. Korzystaj z niej ostrożnie.

⚠ Uwaga! Nie daj się oszukać!

Nie korzystaj z otwartych (publicznych) sieci Wi-Fi do logowania do banku, poczty ani zakupów.
W kawiarni czy hotelu używaj internetu mobilnego, jeśli musisz zalogować się na ważne konto.

✓ Zapamiętaj!

Twoja domowa sieć Wi-Fi powinna być zabezpieczona hasłem (WPA2 lub WPA3).

Jeśli nie wiesz, czy Twoje Wi-Fi jest bezpieczne, zapytaj wnuka lub serwis komputerowy.

MODUŁ 2

Rozpoznawanie phishingu

Fałszywe e-maile i strony internetowe

Phishing to rodzaj oszustwa internetowego. Przestępca podszywa się pod znany bank, sklep, urząd lub firmę kurierskj i wysyła fałszywy e-mail, żeby wyłudzić Twoje dane lub pieniądze.

Jak wygląda phishingowy e-mail?

Fałszywe wiadomości zazwyczaj:

- Twierdzą, że Twoje konto zostało zablokowane lub że grozi Ci kara.
- Proszą o „pilne" kliknięcie w link i zalogowanie się.
- Zawierają błędy językowe lub dziwne znaki.
- Mają podręczny adres nadawcy (np. bank@oplata-123.pl).

⚠ Uwaga! Nie daj się oszukać!

Nigdy nie klikaj w linki w e-mailach, jeśli nie jesteś pewien, że są prawdziwe.

Nigdy nie otwieraj załączników od nieznanych nadawców.

Jeśli e-mail prosi Cię o podanie hasła, numeru karty lub kodu SMS — to oszustwo!

Jak sprawdzić, czy strona jest bezpieczna?

Zanim wpiszesz hasło lub numer karty, sprawdzi adres strony:

1. Adres strony powinien zaczynać się od https:// (litera „s" oznacza bezpieczne połączenie).

2. Obok adresu powinna być widoczna ikonka kłódki.
3. Adres powinien być dokładnie taki, jak znasz (np. www.pkobp.pl, a nie www.pkobp-logowanie.pl).

Praktyczna wskazówka

Jeśli masz wątpliwości, wpisz adres strony banku ręcznie w pasek przeglądarki — nie klikaj w link z e-maila.

Możesz zadzwonić na infolinię banku i zapytać, czy wysłał Ci daną wiadomość.

MODUŁ 3

Smishing i vishing

Oszustwa przez SMS i telefon

Nie tylko przez internet można paść ofiarą oszustwa. Przestępcy coraz częściej kontaktują się przez SMS lub telefon.

Smishing – fałszywe SMS-y

Smishing to phishing przez SMS. Dostajesz wiadomość rzekomo od kuriera, banku, urzędu skarbowego z prośbą o kliknięcie w link i „dopłatę" lub „potwierdzenie danych".

⚠ Uwaga! Nie daj się oszukać!

Nie klikaj w linki w SMS-ach od nieznanych nadawców.

żadna firma kurierska nie wymaga dopłaty przez link w SMS-ie.

Urząd skarbowy nie wysyła SMS-ów z żądaniem natychmiastowej zapłaty.

Vishing – oszustwa przez telefon

Vishing to rozmowa telefoniczna, podczas której przestępca podszywa się pod pracownika banku, policjanta lub pracownika firmy.

Typowe scenariusze:

- „Dzwonię z banku — na Pana/Pani koncie wykryto podejrzaną transakcję. Proszę podać kod z SMS-a."
- „Jestem policjantem — prowadzę śledztwo, potrzebuję Pana/Pani pomocy. Proszę przelewać pieniądze na wskazane konto."

- „Wygrał/a Pan/Pani nagrodę — wystarczy zapłacić opłatę manipulacyjną.”

✓ Zapamiętaj!

Prawdziwy pracownik banku nigdy nie poprosi Cię o podanie pełnego hasła ani o przelanie pieniędzy na „bezpieczne konto”.
Policja nigdy nie prosi przez telefon o przekazanie gotówki.
Jeśli masz wątpliwości — rozłącz się i zadzwoń sam na oficjalny numer banku.
Możesz też zadzwonić do bliskich i opowiedzieć im o rozmowie.

MODUŁ 4

Ochrona danych osobowych

RODO w praktyce – co udostępniać w sieci

Twoje dane osobowe to cenne informacje. Należą do nich: imię i nazwisko, adres zamieszkania, numer PESEL, numer telefonu, adres e-mail, numer dowodu osobistego czy dane karty płatniczej.

Czym jest RODO?

RODO (Rozporządzenie Ogólne o Ochronie Danych) to europejskie prawo, które chroni Twoje dane. Dzięki niemu firmy i urzędy mogą przetwarzać Twoje dane tylko w określonym celu i za Twoją zgodą.

Co możesz udostępniać, a czego nie?

✓ Zapamiętaj!

Nigdy nie podawaj numeru PESEL na stronach internetowych, które nie są urzędami ani bankami.

Nie wpisuj numeru dowodu osobistego w formularzach na nieznanych stronach.

Nie udostępniaj zdjęć dokumentów tożsamości przez internet.

Nie podawaj numeru karty płatniczej na stronach, których nie znasz.

⚠ Uwaga! Nie daj się oszukać!

Uważaj na prośby o „skan dowodu osobistego” od nieznanych firm — to częsty element oszustw.

Jeśli sklep internetowy prosi o numer PESEL, sprawdzi dokładnie, czy to renomowana firma.

Twoje prawa

Jako osoba, której dane dotyczą, masz prawo do:

- Dostępu do swoich danych — możesz zapytać firmę, jakie dane o Tobie posiada.
- Usunięcia danych — możesz poprosić o usunięcie Twoich danych (prawo do bycia zapomnianym).
- Sprostowania — możesz poprosić o poprawienie błędnych danych.
- Sprzeciwu — możesz sprzeciwić się przetwarzaniu danych w celach marketingowych.

MODUŁ 5

Bezpieczne zakupy online

Weryfikacja sklepów i bezpieczne płatności

Zakupy przez internet są wygodne — możesz zamawiać towary bez wychodzenia z domu. Ważne jest jednak, by robić to bezpiecznie i tylko w sprawdzonych sklepach.

Jak sprawdzić sklep przed zakupem?

4. Sprawdź, czy strona sklepu ma certyfikat bezpieczeństwa (https:// i kłódka).
5. Poszukaj danych firmy: nazwa, adres, NIP, KRS — powinny być widoczne na stronie.
6. Przeczytaj opinie innych kupujących (np. na stronie Opineo, Google).
7. Sprawdź politykę zwrotów i reklamacji.
8. Unikaj sklepów, które oferują produkty w cenach „zbyt dobrych, żeby były prawdziwe”.

Praktyczna wskazówka

Renomowane sklepy to np. Allegro, Amazon, Media Expert, Empik, Zalando.
Możesz sprawdzić firmę w rejestrze CEIDG lub KRS (wpisz w Google: CEIDG lub KRS wyszukiwarka).

Bezpieczne płatności

✓ Zapamiętaj!

Płać przez bezpieczne systemy płatności: BLIK, PayPal, przelewy24, karta płatnicza z weryfikacją 3D Secure.

Przed zatwierdzeniem płatności sprawdź: kwotę, odbiorcę i tytuł przelewu.

Nigdy nie płać przelewem tradycyjnym z góry do nieznanego sklepu.

⚠ Uwaga! Nie daj się oszukać!

Jeśli sklep prosi o przelew na konto prywatne — to sygnał ostrzegawczy.

Zbyt niska cena (np. iPhone za 200 zł) to niemal zawsze znak oszustwa.

MODUŁ 6

Bankowość elektroniczna

Bezpieczne logowanie i weryfikacja transakcji

Bankowość elektroniczna pozwala zarządzać kontem bez wychodzenia z domu. Jest wygodna, ale wymaga zachowania szczególnej ostrożności.

Bezpieczne logowanie do banku

✓ Zapamiętaj!

Adres strony banku wpisuj ręcznie w przeglądarce — nigdy nie klikaj w linki z e-maili ani SMS-ów.

Sprawdź, czy adres strony jest poprawny (np. www.pkobp.pl, nie www.pkobp-online24.pl).

Po zakończeniu korzystania z bankowości zawsze się wyloguj.

Nie loguj się do banku z cudzego komputera ani przez publiczne Wi-Fi.

Weryfikacja transakcji — kody SMS

Bank wysyła kody SMS do potwierdzenia przelewów. To dodatkowe zabezpieczenie.

⚠ Uwaga! Nie daj się oszukać!

Zawsze przeczytaj treść SMS-a przed wpisaniem kodu — sprawdź kwotę i numer konta odbiorcy.

Jeśli SMS mówi o innej kwocie niż chciałeś przelewać — nie wpisuj kodu! Natychmiast zadzwoń do banku.

Pracownik banku nigdy nie poprosi Cię przez telefon o podanie kodu SMS.

Regularnie sprawdzaj wyciągi

Praktyczna wskazówka

Raz w tygodniu sprawdzaj historię operacji na koncie.
Jeśli widzisz nieznane transakcje — niezwłocznie zadzwoń do banku i je zablokuj.
Numer alarmowy do zablokowania karty zazwyczaj znajduje się na odwrocie karty płatniczej.

MODUŁ 7

Media społecznościowe

Prywatność, fałszywe profile, dezinformacja

Facebook, Instagram, YouTube — to popularne platformy społecznościowe. Warto jednak korzystać z nich ostrożnie.

Ustawienia prywatności

Praktyczna wskazówka

Ogranicz widoczność swoich postów i zdjęć tylko do znajomych (nie dla wszystkich).

Nie podawaj publicznie adresu zamieszkania, numeru telefonu ani daty urodzenia.

Poproś wnuka lub bliskich, by pomógli Ci ustawić prywatność konta.

Fałszywe profile i oszustwa na Facebooku

⚠ Uwaga! Nie daj się oszukać!

Jeśli nieznajoma osoba prosi Cię o pieniądze przez Facebook — zignoruj i zgłoś profil.

Uważaj na wiadomości od „znajomych" proszących o pożyczkę — ich konto mogło zostać zhakowane.

Nie klikaj w linki do „nagród" lub „niesałowitych promocji" rozsyłanych przez Facebook.

✓ Zapamiętaj!

Możesz zgłosić podejrzane konto lub treść na Facebooku (przycisk „..." przy poście lub profilu).

Jeśli ktoś przejął Twoje konto — natychmiast zmień hasło i zgłoś to Facebookowi.

MODUŁ 8

Fake news i dezinformacja

Jak weryfikować informacje

Fake news to fałszywe informacje, które są celowo rozpowszechniane w internecie, by wywołać strach, złość lub skłonić do pochopnych działań.

Jak rozpoznać fałszywą informację?

- Nagłówek jest sensacyjny i wywołuje silne emocje (strach, oburzenie).
- Artykuł nie podaje źródła ani autora.
- Zdjęcia są przesadzone lub nie pasują do treści.
- Informacja jest dostępna tylko na jednej stronie, a brak jej w znanych mediach.
- Tekst zawiera błędy ortograficzne i stylistyczne.

Praktyczna wskazówka

Sprawdź informację w kilku zaufanych źródłach: TVN24, Polsat News, RMF FM, Polskie Radio, PAP.

Możesz sprawdzić fakty na stronach Demagog.org.pl lub Konkret24 (tvn24.pl).

Zastanow się: czy ta informacja wywołuje silne emocje? Jeśli tak — sprawdź ją zanim udostępnisz.

Nie udostępniaj bez weryfikacji

✓ Zapamiętaj!

Jeśli nie jesteś pewien, czy informacja jest prawdziwa — nie udostępniaj jej dalej.

Fake newsy często dotyczą zdrowia, leków i „cudownych terapii" — zawsze skonsultuj z lekarzem.

Nie daj się wciągnąć w łańcuszki szczęścia i ostrzeżenia, które proszą o udostępnienie.

MODUŁ 9

E-usługi publiczne

Profil Zaufany, ePUAP, e-recepty

Dzięki e-usługom publicznym możesz załatwić wiele spraw urzędowych przez internet, bez konieczności wychodzenia z domu.

Profil Zaufany

Profil Zaufany to bezpłatne narzędzie, które pozwala potwierdzić Twoją tożsamość w kontaktach z urzędami przez internet.

Praktyczna wskazówka

Profil Zaufany możesz założyć przez stronę www.gov.pl lub przez bankowość elektroniczną swojego banku.
Możesz go potwierdzić w urzędzie (np. ZUS, urząd gminy) lub przez bank.
Poproś bliskich lub pracownika urzędu o pomoc przy zakładaniu Profilu Zaufanego.

ePUAP i platforma gov.pl

Na stronie www.gov.pl możesz:

- Złożyć wniosek o wydanie dowodu osobistego lub paszportu.
- Sprawdźć swoje punkty karne.
- Złożyć deklarację podatkową.
- Zameldować się lub wymeldować.

E-recepty

E-recepta to elektroniczna recepta wystawiana przez lekarza. Zamiast papierowego dokumentu dostajesz SMS lub e-mail z kodem, który podajesz w aptece.

✓ Zapamiętaj!

Kod do e-recepty możesz podać telefonicznie lub pokazać SMS w aptece.

E-recepty możesz też sprawdzić w aplikacji moje IKP na stronie pacjent.gov.pl.

Jeśli masz kłopoty z e-receptą, zapytaj farmaceutę w aptece — pomoże.

MODUŁ 10

Platforma ZUS

Usługi emerytalne i rentowe online

Zakład Ubezpieczeń Społecznych (ZUS) udostępnia wiele usług przez internet. Możesz sprawdzić swoje świadczenia bez wizyty w urzędzie.

PUE ZUS – co można tam zrobić?

Na platformie PUE ZUS (www.zus.pl) możesz:

- Sprawdzić wysokość swojej emerytury lub renty.
- Złożyć wniosek o zaświadczenie o wysokości emerytury.
- Sprawdzić swoje ubezpieczenia.
- Wysłać pismo do ZUS bez wychodzenia z domu.
- Umówić wizytę w placówce ZUS.

Praktyczna wskazówka

Możesz zalogować się do PUE ZUS przez Profil Zaufany lub przez bankowość elektroniczną.
Jeśli potrzebujesz pomocy, możesz zadzwonić na infolinię ZUS: 22 560 16 00.
W każdej placówce ZUS są doradcy, którzy pomogą Ci skorzystać z platformy.

⚠ Uwaga! Nie daj się oszukać!

Uważaj na fałszywe strony i SMS-y informujące o „dodatkowych świadczeniach” wymagających podania danych osobowych.

ZUS nie wysyła SMS-ów z prośbą o kliknięcie w link w celu pobrania świadczenia.

MODUŁ 11

Złośliwe oprogramowanie

Wirusy, trojany, ransomware – jak się chronić

Złośliwe oprogramowanie to programy stworzone przez przestępców, które mogą zainfekować Twój komputer lub telefon i kraść Twoje dane lub pieniądze.

Rodzaje złośliwego oprogramowania

- Wirusy – programy, które niszczą pliki lub spowalniają komputer.
- Trojany – ukrywają się pod pozorem normalnego programu i kradna dane.
- Ransomware – szyfruje Twoje pliki i żąda okupu za odblokowanie.
- Spyware – szpieguje Cię i wysyła dane osobowe do przestępców.

Jak się chronić?

✓ Zapamiętaj!

Zainstaluj program antywirusowy i regularnie go aktualizuj (Windows Defender wbudowany w Windows 10/11 jest darmowy i skuteczny).

Nie otwieraj załączników e-mail od nieznanych nadawców.

Nie instaluj programów z nieznanych stron — pobieraj tylko z oficjalnych sklepów.

Regularnie twórz kopie zapasowe ważnych plików (np. zdjęć rodzinnych) na pendrive lub dysku zewnętrznym.

⚠ Uwaga! Nie daj się oszukać!

Jeśli na ekranie pojawi się komunikat o „wirusie” z prośbą o zadzwonienie pod podany numer — to oszustwo! Nie dzwoń.
Jeśli Twój komputer działa wolno lub dziwnie — poproś kogoś bliskiego o pomoc.

MODUŁ 12

Bezpieczeństwo urządzeń mobilnych

Smartfon i tablet – jak korzystać bezpiecznie

Smartfon i tablet to dziś okno na świat. Dzięki nim możesz dzwonić, pisać, przeglądać internet i korzystać z setek aplikacji. Ważne, by robić to bezpiecznie.

Podstawowe zasady bezpieczeństwa

✓ Zapamiętaj!

Ustaw blokadę ekranu — kod PIN, wzór lub odcisk palca.
Instaluj aplikacje tylko z oficjalnych sklepów: Google Play (Android) lub App Store (Apple).
Regularnie aktualizuj system operacyjny i aplikacje.
Nie udzielaj aplikacjom więcej uprawnień, niż potrzebują.

Aplikacje bankowe

Praktyczna wskazówka

Pobierz aplikację bankową tylko ze sklepu Google Play lub App Store.
Nigdy nie wchodź na stronę banku przez link z SMS-a ani e-maila.
Po korzystaniu z aplikacji bankowej wyloguj się.

Kradzież lub zgubienie telefonu

Jeśli zgubisz telefon lub zostanie skradziony:

1. Zadzwoń do banku i zastrzeż karty płatnicze oraz dostęp do bankowości mobilnej.

2. Zmień hasła do kont e-mail i mediów społecznościowych z innego urządzenia.
3. Zgłoś kradzież na Policję.
4. Możesz zdalnie zablokować lub wyczyścić telefon przez Google (Find My Device) lub Apple (Znajdź mój iPhone).

MODUŁ 13

Co zrobić, gdy padniesz ofiarą oszustwa?

Zgłaszanie incydentów, CERT Polska, Policja

Jeśli podejrzewasz, że padłeś ofiarą oszustwa w internecie lub przez telefon — nie czekaj i działaj szybko.

Kroki do podjęcia natychmiast

5. Nie panikuj — zachowaj spokój i nie podejmuj pochopnych działań.
6. Zadzwoń do banku i poinformuj o podejrzanej transakcji lub poproś o zablokowanie konta.
7. Zmień hasła do swoich kont e-mail i mediów społecznościowych.
8. Zbierz dowody: zachowaj SMS-y, e-maile, zrzuty ekranu.
9. Zgłoś sprawę na Policję.

Gdzie zgłosić oszustwo?

Instytucja	Jak zgłosić?
Policja	Zadzwoń: 112 lub 997, lub zgłoś się osobiście na komisariat.
CERT Polska	Zgłoś incydent online: incydent.cert.pl lub zadzwoń: 799 448 084.
Bank	Numer na odwrocie karty lub na stronie banku.

Fundacja EGIDA	Opole — możesz zgłosić się po poradę prawną.

✓ Zapamiętaj!

Nie wstydź się zgłaszać oszustwa — przestępcy są przebiegli i ofiarą może paść każdy.

Im szybciej zareagujesz, tym większa szansa na odzyskanie pieniędzy.

Możesz zadzwonić do bliskich lub sąsiadów — pomogą Ci w trudnej chwili.

Pojęcie	Co to znaczy?
BLIK	Szybki sposób płacenia telefonem. Generujesz 6-cyfrowy kod w aplikacji banku i wpisujesz go przy płatności.
CERT Polska	Zespół ekspertów reagujących na zagrożenia w internecie. Możesz zgłaszać im podejrzane strony i oszustwa.
E-recepta	Recepta wystawiana elektronicznie przez lekarza. Odbierasz ją w aptece podając kod lub numer PESEL.
ePUAP	Platforma rządowa do kontaktu z urzędami przez internet.
Fake news	Fałszywa informacja lub wiadomość, celowo tworzona i rozpowszechniana w internecie.
Hasło	Sekretny ciąg znaków chroniący dostęp do konta.
https://	Bezpieczne połączenie ze stroną internetową. Litera „s” oznacza szyfrowanie.
Malware	Złośliwe oprogramowanie — wszelkie programy stworzone przez przestępców.
Phishing	Oszustwo polegające na podszywaniu się pod znane firmy lub instytucje.

PIN	4–6 cyfrowy kod do logowania lub potwierdzania transakcji.
Profil Zaufany	Bezpłatne narzędzie do potwierdzania tożsamości w kontaktach z urzędami przez internet.
Ransomware	Złośliwy program, który szyfruje pliki i żąda okupu za ich odblokowanie.
RODO	Europejskie prawo chroniące dane osobowe.
Smishing	Oszustwo przez SMS — fałszywa wiadomość z linkiem lub prośbą o dane.
Trojan	Złośliwy program ukryty w pozornie normalnej aplikacji.
Vishing	Oszustwo telefoniczne — przestępca podszywa się pod bank lub Policję.
Wi-Fi	Bezprzewodowe połączenie z internetem.

10 ZŁOTYCH ZASAD BEZPIECZNEGO INTERNETU

Wytnij i przyklej na lodówce lub przy monitorze — miej te zasady zawsze przed oczami!

1	Używaj mocnych haseł i nie udostępniaj ich nikomu.
2	Aktualizuj system i programy – to chroni przed wirusami.
3	Sprawdzaj adresy stron – szukaj https:// i kłódki.
4	Nie klikaj w linki z SMS-ów ani e-maili od nieznanych.
5	Nie podawaj danych osobowych na nieznanych stronach.
6	Kupuj tylko w znanych, sprawdzonych sklepach internetowych.
7	Regularnie sprawdzaj historię transakcji w banku.

8 Nie pobieraj programów z nieznanych stron.

9 W razie wątpliwości – zapytaj bliskich lub zadzwoń na infolinię.

10 Jeśli padłeś ofiarą oszustwa – działaj szybko i zgłoś to na Policję i do banku.

O projekcie

Niniejsze kompendium zostało opracowane w ramach projektu solidarnościowego „Bezpieczni w sieci" (nr 2024-3-PL01-ESC30-SOL-000282674) realizowanego przez grupę pięciu młodych wolontariuszy z Opola w ramach programu Europejski Korpus Solidarności w okresie 1 marca 2025 r. – 28 lutego 2026 r.

Projekt był skierowany do seniorów (osób w wieku 60+) i obejmował 80 godzin bezpłatnych warsztatów z cyberbezpieczeństwa dla 20 uczestników z Opola i okolic.

Organizacja realizująca: Fundacja pomocy prawnej EGIDA, Opole.

Dofinansowane przez Unię Europejską

Finansowane przez Unię Europejską