Klikaj z głową!

Jak rozpoznawać manipulację i bezpiecznie korzystać z internetu

Praktyczny przewodnik dla seniorów



Mazowsze. serce Polski

Mazowsze dla organizacji pozarządowych

Zadanie publiczne współfinansowane ze środków Samorządu Województwa Mazowieckiego

Po co powstała ta broszura?

Internet ułatwia codzienne życie – pozwala komunikować się, załatwiać sprawy i zdobywać wiedzę. Niestety, mogą czyhać też zagrożenia: **oszustwa, manipulacja i kradzież danych.**

ZATRZYMAJ SIĘ — SPRAWDŹ — ZDECYDUJ

Zatrzymaj się – nie działaj od razu

Sprawdź – kto wysłał wiadomość?

Zdecyduj – działaj dopiero, gdy masz pewność



Chroń siebie
Twoje dane i pieniądze są ważne.

Bądź spokojny
Kilka prostych zasad daje Ci bezpieczeństwo.

Korzystaj z internetu
świadomie i z korzyścią dla siebie.

PAMIĘTAJ: Masz prawo powiedzieć: **Najpierw sprawdzę.**

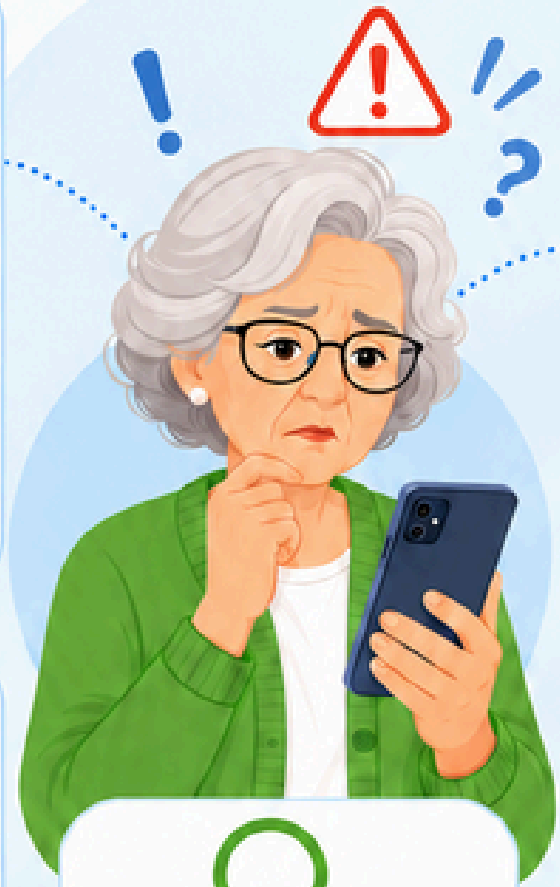
Jak działa manipulacja?

Manipulatorzy używają **emocji**,
aby skłonić Cię do szybkiej reakcji.

Strach

Wzbudzają lęk, abyś działał bez zastanowienia.

Przykład:
Twoje konto zostanie zablokowane



Pośpiech

Wywierają presję czasu, nie dając Ci chwili na namysł.

Przykład:
Oferta ważna tylko dziś

Zaufanie

Podszywają się pod kogoś bliskiego lub instytucję, żeby zyskać Twoje zaufanie.

Przykład:
Pisze Twoja wnuczka

Ciekawość

Wzbudzają ciekawość, żebyś kliknął w podejrzany link.

Przykład:
Zobacz, co się stało

Dobre serce

Odwołują się do Twojej życzliwości i chęci pomocy.

Przykład:
Pomóż pilnie

Jeśli wiadomość wywołuje silne emocje — zatrzymaj się.

Fake news – czyli fałszywa informacja

Fake news to nieprawdziwa lub wprowadzająca w błąd informacja, która wygląda na prawdziwą. Często ma na celu wywołanie emocji, zdobycie kliknięć lub manipulowanie opinią.

Czerwone flagi

Sensacyjny tytuł
Ma wzbudzić emocje i przyciągnąć uwagę.

Brak autora
Nie wiadomo, kto napisał tekst.

Brak daty
Informacja może być nieaktualna.

Dużo wykrzykników
Próba wywołania silnych emocji.

Prośba o natychmiastowe udostępnienie
Często to sposób na szybkie rozpowszechnianie fałszu.

Brak źródeł
Brak odwołań do wiarygodnych źródeł lub dowodów.



Zanim udostępnisz, zapytaj:

- kto to napisał?
- skąd to wiadomo?
- czy inne źródła to potwierdzają?

Jak sprawdzić źródło informacji?

Zanim uwierzysz — sprawdź!

Kto jest autorem?

Sprawdź, kto napisał informację. Czy to ekspert, instytucja, a może osoba prywatna?

Jaki jest adres strony?

Zwróć uwagę na adres (URL). Czy to znana strona, instytucja lub organizacja?
Uważaj na podejrzane adresy!

Czy jest data?

Sprawdź, kiedy informacja została opublikowana lub zaktualizowana. Aktualność ma znaczenie!

Czy inne źródła to potwierdzają?

Poszukaj tej samej informacji w innych, wiarygodnych miejscach. Jedno źródło to za mało.





Jeśli informacja dotyczy zdrowia, pieniędzy lub bezpieczeństwa — sprawdź ją dwa razy.

Fakt czy opinia?

Naucz się odróżniać informacje i podejmować mądre decyzje.

Fakt



Informacja, którą można sprawdzić i potwierdzić w wiarygodnych źródłach.

Przykład:
W Polsce obowiązuje ustawa o ochronie danych osobowych.

Opinia



Czyjeś zdanie, przekonanie lub ocena – może być różna u różnych osób.

Przykład:
Uważam, że zakupy przez internet są wygodne.

Reklama



Komunikat mający na celu zachęcić do kupna produktu lub usługi.

Przykład:
Kup teraz – najlepsza oferta tylko dziś!

Manipulacja

Celowe wprowadzanie w błąd lub wywieranie presji, aby skłonić do określonego działania.

Przykład: „Tylko teraz! Jeśli tego nie zrobisz, stracisz wszystko!"

Minićwiczenie

Zastanów się, co jest faktem, a co opinią.

1. Wczoraj temperatura w Warszawie wyniosła 20°C. .....
2. Ten telefon ma świetny aparat. .....
3. Ten krem sprawi, że będziesz wyglądać 10 lat młodziej! .....
4. Nauka nowych rzeczy poprawia samopoczucie. .....

Weryfikacja
wiadomości krok po kroku

Zatrzymaj się
Nie działaj od razu.
Daj sobie chwilę.

2
Przeczytaj spokojnie
Przeczytaj całą wiadomość uważnie, bez pośpiechu.

3
Sprawdź nadawcę
Kto to wysłał?
Czy znasz tę osobę lub firmę?

4
Nie używaj linku z wiadomości
Linki mogą prowadzić do fałszywych stron.
Nie klikaj.

5
Zapytaj kogoś zaufanego
Skonsultuj się z rodziną lub przyjacielem.

6
Dopiero wtedy zdecyduj
Gdy masz pewność, że to bezpieczne – dopiero działaj.



Brak reakcji jest często bezpieczniejszy niż szybka reakcja.

Podejrzane SMS-y i wiadomości

Oszuści próbują wyłudzić Twoje pieniądze
lub dane osobowe. Bądź czujny i nie daj się oszukać!

5 typowych oszustw



Fałszywy kurier

SMS o niedoręczonej paczce i prośba o dopłatę lub zmianę danych. Link prowadzi do strony oszusta.



Fałszywy bank

Wiadomość o zablokowanym koncie lub podejrzanej transakcji. Prośba o kliknięcie linku i zalogowanie się.



Fałszywy urząd

SMS o dopłacie, podatku lub zwrocie pieniędzy. Link prowadzi do fałszywej strony urzędu.



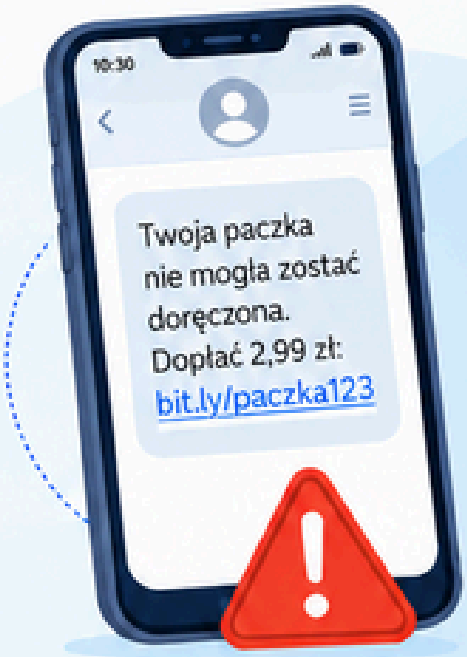
Fałszywy członek rodziny

Wiadomość: „To ja, zmieniłem numer. Mam problem, potrzebuję pilnie pieniędzy". Prośba o szybki przelew lub kod BLIK.



Fałszywy konkurs

Informacja o wygranej atrakcyjnej nagrody. Prośba o podanie danych lub opłatę za przesyłkę. To tylko przynęta!



Podejrzany SMS? Zatrzymaj się i sprawdź!

Co zrobić?

- **Nie klikaj linku** w podejrzanym SMS-ie.
- **Nie odpisuj** na takie wiadomości.
- **Nie podawaj** swoich danych osobowych ani loginów.
- **Przekaż SMS** na numer 8080. Pomagasz chronić siebie i innych.
- **Skontaktuj się z bankiem,** jeśli podałeś swoje dane lub wykonałeś przelew.

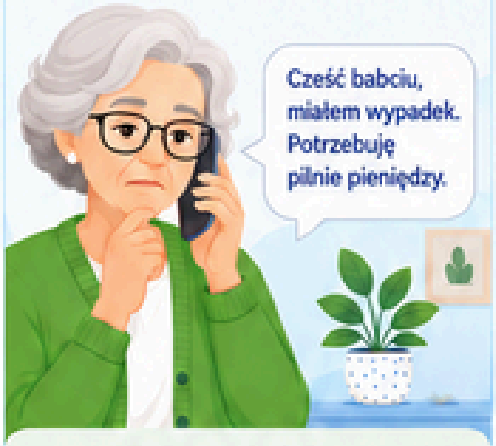
Link z SMS-a? Najpierw pauza.

Oszustwa na wnuczkę, na policjanta i na pilną pomoc

Uważaj na oszustów, którzy wykorzystują zaufanie i pośpiech.

NA WNUCZKA

Dzwoni osoba podająca się za członka rodziny.



Proszą o pieniądze dla Ciebie lub dla bliskiej osoby.

NA POLICJANTA

Dzwoni osoba podająca się za policjanta.



Twierdzą, że Twoje oszczędności są zagrożone i trzeba je „chronić".

NA PILNĄ POMOC

Dzwoni osoba z informacją o nagłej, dramatycznej sytuacji.



Wywierają presję i każą działać natychmiast.

Co zrobić?

Rozłącz się
Nie prowadź rozmowy.

Zadzwoń na znany numer
Skontaktuj się z bliską osobą i sprawdź, czy wszystko w porządku.

Nie przekazuj gotówki
Nie dawaj pieniędzy obcym.

Nie rób przelewu pod presją
Nie działaj w pośpiechu.

Skontaktuj się z policją
Zadzwoń pod numer 112 lub 997, gdy masz wątpliwości.

> *Nie podejmuję decyzji przez telefon. Najpierw sprawdzę.*



Hasła, kody i dane osobowe

Nigdy ich nie udostępniaj!

- **PIN** do karty lub telefonu
- **Hasło do banku**
- **Numer karty** płatniczej
- **Kod BLIK**
- **CVV/CVC** z karty
- **Login** do poczty e-mail
- **Kod SMS** z banku lub innych usług
- **PESEL** bez potrzeby



Dobre hasło

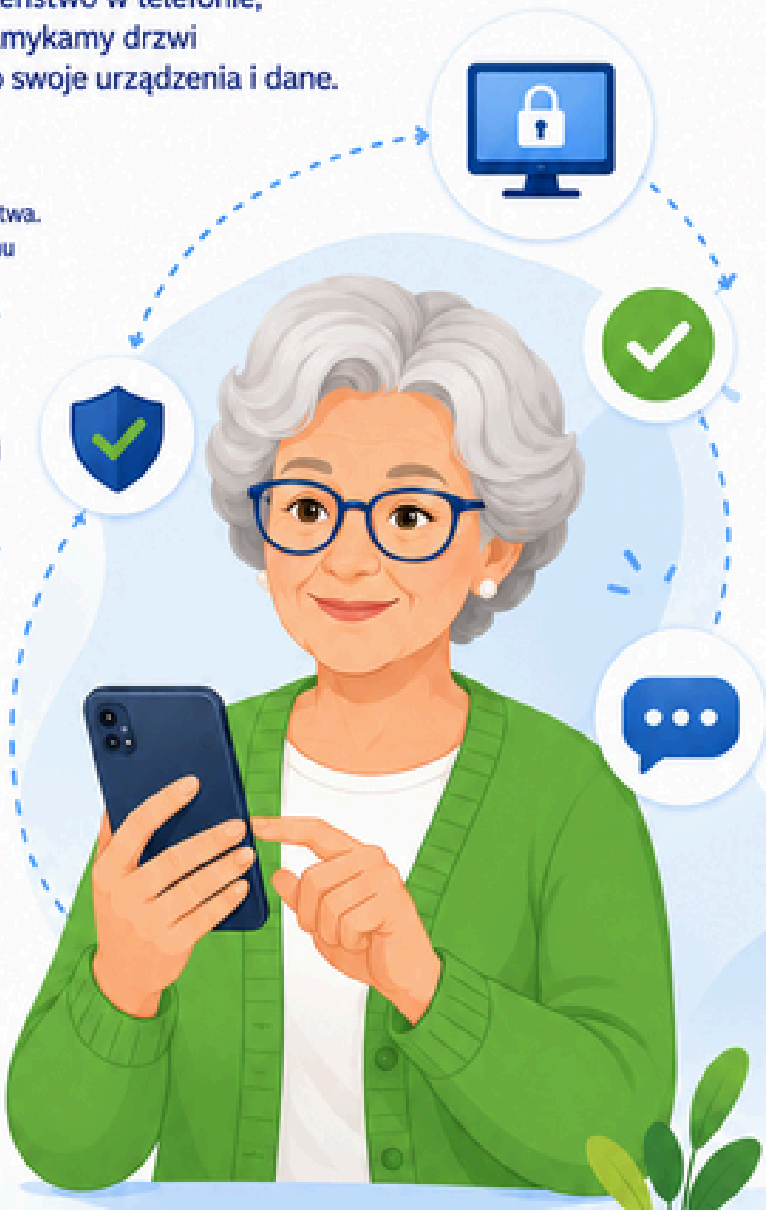
- **Długie** – im dłuższe, tym lepsze
- **Trudne do odgadnięcia**
- **Inne do każdego ważnego konta**
- **Niezwiązane z datą urodzenia**

Kod SMS z banku służy Tobie, nie rozmówcy.

Nie podawaj go nikomu – nawet jeśli prosi i twierdzi, że jest z banku.

Higiena cyfrowa – codzienne dobre nawyki

Higiena cyfrowa to codzienne dbanie o bezpieczeństwo w telefonie, komputerze i internecie. Tak jak myjemy ręce, zamykamy drzwi i pilnujemy dokumentów, tak samo warto dbać o swoje urządzenia i dane.



1 Aktualizuj telefon i komputer

Aktualizacje często naprawiają luki bezpieczeństwa. Jeśli urządzenie proponuje aktualizację systemu lub aplikacji, nie odkładaj tego bez końca.

2 Uważaj na publiczne Wi-Fi

W kawiarni, urzędzie, autobusie czy przychodni nie loguj się do banku, jeśli korzystasz z publicznej sieci Wi-Fi. Bezpieczniej użyć własnego internetu w telefonie.

3 Pobieraj aplikacje tylko z oficjalnych sklepów

Nie instaluj aplikacji z linków przesłanych SMS-em lub przez komunikator.

4 Blokuj ekran

Ustaw kod, odcisk palca lub inną blokadę telefonu. Telefon bez blokady jest jak otwarta torebka z dokumentami.

5 Uważaj na zdjęcia dokumentów

Nie wysyłaj zdjęcia dowodu osobistego, prawa jazdy, karty bankowej ani recepty osobom, których nie znasz i których próśb nie możesz potwierdzić.

6 Ogranicz udostępnianie informacji

Nie wszystko trzeba publikować. Informacje o wyjeździe, samotnym mieszkaniu, chorobie, oszczędnościach lub rodzinie mogą zostać wykorzystane przez nieuczciwe osoby.

Checklista dobrych nawyków

- Mam blokadę telefonu.
- Aktualizuję urządzenia.
- Nie klikam podejrzanych linków.
- Nie podaję kodów i haseł.
- Sprawdzam nadawcę wiadomości.
- Pytam zaufaną osobę, gdy mam wątpliwości.

Chroń siebie i swoje dane | Bądź uważny na co dzień | Pytaj, sprawdzaj, rozmawiaj

Bezpiecznie i świadomie w sieci

Bezpieczne płatności i zakupy w internecie

Zakupy online są wygodne, ale wymagają ostrożności.
Oszuści tworzą fałszywe sklepy, fałszywe promocje i fałszywe ogłoszenia.

1 Uważaj na zbyt piękne okazje

Jeśli produkt kosztuje dużo mniej niż w innych sklepach, zachowaj czujność. Bardzo niska cena może być przynętą.

Przykład: Nowy telefon za 199 zł, markowe buty za 29 zł, opał lub pellet za połowę ceny – to może być oszustwo.



2 Sprawdź sklep

- sprawdź nazwę sklepu,
- poszukaj opinii w kilku miejscach,
- zobacz, czy podano pełne dane firmy,
- sprawdź, czy jest regulamin i kontakt,
- uważaj, jeśli jedyną formą kontaktu jest formularz lub komunikator,
- zachowaj potwierdzenie zamówienia.

3 Nie działaj poza platformą sprzedażową

Jeśli sprzedajesz lub kupujesz przez znany portal, nie przechodź do prywatnych linków wysyłanych przez kupującego lub sprzedającego.

Oszust może napisać:
"Kliknij tutaj, żeby odebrać pieniądze."
"Kurier już czeka, potwierdź kartę."
"Podaj dane karty, żeby dostać przelew."
To nie jest normalna procedura.

4 Bezpieczniej

- Płać metodami, które dają potwierdzenie.
- Nie podawaj danych karty przez link z wiadomości.
- Nie wpisuj danych bankowych na stronie, której nie znasz.
- Przy większych zakupach poproś kogoś zaufanego o pomoc w sprawdzeniu oferty.

Zasada

Gdy ktoś chce Ci dać pieniądze, nie powinien prosić o pełne dane Twojej karty.

Bądź czujny – to najlepsza ochrona.

W razie wątpliwości skonsultuj się z bliską osobą.

Podejrzane sytuacje zgłoś do swojego banku.

Bezpieczeństwo w internecie zaczyna się od Ciebie.

Media społecznościowe i komunikatory

Facebook, WhatsApp, Messenger i inne komunikatory pomagają być bliżej ludzi. Można rozmawiać z rodziną, śledzić lokalne wydarzenia, oglądać zdjęcia i uczestniczyć w grupach. Ale także tam mogą pojawiać się fałszywe informacje i oszustwa.



1 Uważaj na wiadomości od znajomych

Jeśli znajomy prosi o kod BLIK, szybki przelew albo kliknięcie linku, najpierw zadzwoń do niego. Jego konto mogło zostać przejęte.

Przykład wiadomości:
"Pożyczysz 500 zł? Oddam wieczorem. Wyślij kod BLIK." Nawet jeśli wiadomość przychodzi z prawdziwego profilu znajomego, to nie musi pisać znajomy.

2 Uważaj na łańcuszki

- „Wyślij to do 10 osób."
- „Jeśli nie udostępnisz, stanie się coś złego."
- „Tylko wybrani wiedzą prawdę."

Łańcuszki często wykorzystują emocje i nie pomagają w rzetelnym informowaniu.

3 Uważaj na fałszywe zbiórki

- sprawdź organizatora,
- sprawdź stronę zbiórki,
- zobacz, czy podano cel i dane,
- nie wpłacaj pod presją,
- w razie wątpliwości zapytaj rodzinę lub znajomych.

4 Komentarze to nie zawsze prawda

To, że wiele osób coś komentuje lub udostępnia, nie oznacza, że informacja jest prawdziwa. Popularność nie jest dowodem.

5 Zrób tak

- Czy znam źródło?
- Czy to nie jest stary post?
- Czy ktoś próbuje mnie przestraszyć?
- Czy mam pewność, zanim podam dalej?

Hasło
Nie każde 'udostępnij' jest pomocą.

Co zrobić, jeśli kliknąłem lub podałem dane?

Każdemu może się zdarzyć błąd. Oszuści są coraz sprytniejsi i potrafią przygotować wiadomości wyglądające bardzo wiarygodnie. Najważniejsze to nie wstydzić się i działać szybko.

1 Jeśli kliknąłeś podejrzany link



- Nie wpisuj żadnych danych.
- Zamknij stronę.
- Nie pobieraj plików.
- Nie instaluj aplikacji.
- Zrób zrzut ekranu, jeśli potrafisz.
- Pokaż wiadomość zaufanej osobie.

2 Jeśli podałeś dane logowania



- Jak najszybciej zmień hasło.
- Jeśli używasz tego samego hasła w innych miejscach, zmień je także tam.
- Sprawdź, czy na koncie nie ma podejrzanych działań.
- Skontaktuj się z obsługą danej usługi.

3 Jeśli podałeś dane bankowe lub kod



- Natychmiast zadzwoń do banku.
- Zablokuj kartę, jeśli to konieczne.
- Zmień hasło do bankowości internetowej.
- Sprawdź historię transakcji.
- Zgłoś sprawę odpowiednim służbom.

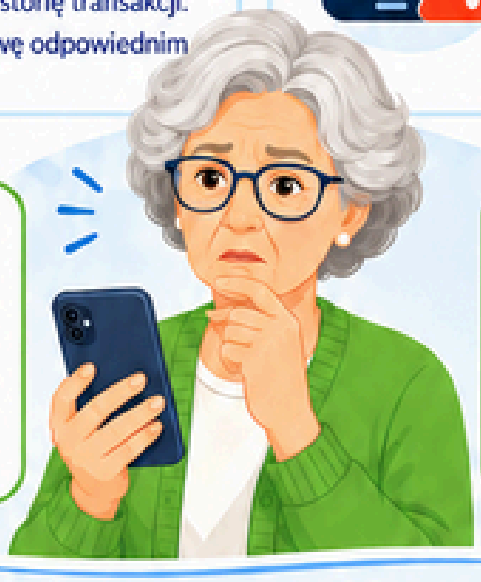
4 Jeśli zainstalowałeś podejrzaną aplikację



- Odłącz urządzenie od internetu, jeśli umiesz.
- Nie loguj się do banku z tego urządzenia.
- Poproś o pomoc zaufaną osobę lub serwis.
- Skontaktuj się z bankiem z innego, bezpiecznego telefonu.

Ważne

Nie ukrywaj sprawy z powodu wstydu. Szybka reakcja może ograniczyć straty.



Zdanie do zapamiętania

Pomyłka to nie koniec. Najważniejsze: reaguj szybko.

Rozmawiaj z bliskimi | Weryfikuj informacje | Korzystaj z oficjalnych źródeł | Reaguj szybko

Twoja karta bezpieczeństwa

Wytnij, przepisz lub sfotografuj tę stronę.
Możesz trzymać ją przy telefonie, na lodówce albo w notesie.



ZATRZYMAJ SIĘ — SPRAWDŹ — ZDECYDUJ

10 zasad bezpiecznego klikania

1. Nie klikam linków z podejrzanych SMS-ów.
2. Nie podaję hasła, PIN-u, kodu BLIK ani kodu SMS.
3. Nie robię przelewów pod presją.
4. Nie wierzę w każdą sensacyjną wiadomość.
5. Sprawdzam autora, datę i źródło informacji.
6. Nie udostępniam dalej wiadomości, jeśli nie mam pewności.
7. Nie instaluję aplikacji z linku przesłanego przez obcą osobę.
8. Przy prośbie o pieniądze dzwonię do bliskiej osoby na znany numer.
9. Gdy coś mnie niepokoi, pytam kogoś zaufanego.
10. W razie oszustwa szybko kontaktuję się z bankiem lub odpowiednią instytucją.

Gdzie szukać pomocy?

Podejrzany SMS:
Przekaż wiadomość na numer **8080**

Podejrzana strona, e-mail lub inne zdarzenie w internecie:
incydent.cert.pl

Możesz także skorzystać z adresu:
cert@cert.pl

Gdy zagrożone są pieniądze:
natychmiast skontaktuj się ze swoim bankiem.

Gdy doszło do oszustwa:
skontaktuj się z policją lub najbliższą jednostką.

Gdy nie wiesz, co zrobić:
poproś o pomoc zaufaną osobę, rodzinę, sąsiada, pracownika biblioteki, domu kultury, ośrodka pomocy społecznej lub organizacji senioralnej.

Najważniejsze zdanie

Mam prawo sprawdzić.
Mam prawo odmówić.
Mam prawo poprosić o pomoc.

Bądź czujny, ale nie daj się wykorzystać.

Twoje bezpieczeństwo jest najważniejsze.

Małe decyzje dziś – spokój jutro.

Bezpieczny senior w sieci.

O projekcie



Broszura „Klikaj z głową!” została przygotowana w ramach działań edukacyjnych wspierających seniorów w bezpiecznym i świadomym korzystaniu z internetu.

Jej celem jest wzmacnianie samodzielności, spokoju i sprawczości seniorów w codziennym kontakcie z telefonem, internetem, wiadomościami, mediami społecznościowymi i usługami cyfrowymi.

FUNDACJA NA RZECZ NAUKI I INNOWACYJNOŚCI



Razem po bezpieczniejszy cyfrowy świat!

Kontakt

Realizator projektu: Fundacja Na Rzecz Nauki i Innowacyjności

Biuro Projektu
„Klikaj z głową!”
Zdunków 27, 26-920 Gniewoszów

Telefon: 661 231 670

E-mail: fni@o2.pl

Strona internetowa: https://www.fni.org.pl/

Wersja PDF broszury:

Ilustracje wykorzystane w publikacji zostały przygotowane z użyciem narzędzi sztucznej inteligencji. Treść merytoryczna publikacji została zweryfikowana i zatwierdzona przez Fundację Na Rzecz Nauki i Innowacyjności.

Mazowsze. serce Polski

Mazowsze dla organizacji pozarządowych

Zadanie publiczne współfinansowane ze środków Samorządu Województwa Mazowieckiego