KOMITET DO SPRAW POŻYTKU PUBLICZNEGO
NIW Narodowy Instytut Wolności
Rządowy Program Wsparcia Organizacji Pozarządowych Moc Małych Społeczności
Zbigniew Dżugaj Starosta Kraśnicki

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI

MOC MAŁYCH SPOŁECZNOŚCI • LUBELSKIE

Jak nie dać się oszukać w telefonie i Internecie

Praktyczny poradnik bezpieczeństwa dla każdego

AUTOR
Michał Wróblewski

1. Rozpoznawaj zagrożenia
2. Chroń swoje dane
3. Korzystaj bezpiecznie
4. Wiedz, jak reagować

REALIZACJA PROJEKTU

Projekt " Cyberbezpieczni w Sołectwie Lasy" jest realizowany w ramach UMOWY MIKROGRANTU NR 30/MMS/2026/LGD.

PARTNERZY
Zielony Pierścień Lokalna Grupa Działania
Chorągiew Lubelska ZHP
Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

2. NAJCZĘSTSZE OSZUSTWA

Najczęstsze oszustwa telefoniczne i internetowe



Oszuści wykorzystują telefon, internet i nasze zaufanie, aby zdobyć pieniądze lub dane osobowe. Podszywają się pod znane osoby i instytucje, wykorzystują pośpiech, strach i emocje. Poniżej znajdziesz najczęstsze metody oszustw, z którymi możesz się spotkać.

1 Oszustwo na pracownika banku

Dzwoni osoba, która informuje o rzekomym zagrożeniu pieniędzy na koncie. Nakłania do podania kodów, instalacji aplikacji lub wykonania przelewu na „bezpieczne konto".



2 Oszustwo na wnuczka, dziecko lub członka rodziny

Osoba podaje się za bliską osobę, która pilnie potrzebuje pieniędzy. Może twierdzić, że zgubiła telefon, miała wypadek lub znalazła się w trudnej sytuacji.



3 Fałszywe SMS-y i wiadomości z linkami

Wiadomość informuje o dopłacie do paczki, blokadzie konta, zaległym rachunku lub konieczności potwierdzenia danych. Link może prowadzić do strony wyłudzającej dane lub dane logowania.



4 Oszustwo podczas zakupów i sprzedaży w internecie

Fałszywy sprzedawca pobiera pieniądze i nie wysyła towaru. Oszust podający się za kupującego może przesłać link do rzekomego odbioru zapłaty, który służy do wyłudzenia danych.



5 Wyłudzenie kodu BLIK

Oszust przejmuje konto w mediach społecznościowych lub podszywa się pod znajomego i prosi o pilną pomoc finansową. Prosi o kod BLIK, licząc na to, że ofiara zatwierdzi wypłatę lub płatność.



6 Fałszywe inwestycje i obietnice szybkiego zysku

Oszuści obiecują wysokie zyski bez ryzyka. Namawiają do wpłat lub kontaktują się w sprawie rzekomej inwestycji. Często pokazują fikcyjne zyski, aby skłonić do kolejnych wpłat.



7 Fałszywa pomoc techniczna

Ktoś informuje o rzekomym wirusie, problemie z telefonem lub zagrożeniu konta. Nakłania do instalacji programu, przekazania dostępu do urządzenia albo podania danych.



8 Oszustwa z wykorzystaniem sztucznej inteligencji

Przestępcy mogą tworzyć fałszywe zdjęcia, nagrania lub naśladować głos bliskiej osoby. Sam głos czy obraz nie wystarczą więc do potwierdzenia, że naprawdę rozmawiamy z kimś znajomym.



Co łączy te oszustwa?

Niezależnie od metody oszuści często stosują te same sztuczki:

Pośpiech
„Musisz zrobić to natychmiast!"

Strach
„Twoje pieniądze są zagrożone!"

Presja
„Nie rozłączaj się i nikomu nie mów."

Zaufanie
„Jestem pracownikiem banku" lub „To ja, Twoje dziecko".

Obietnica korzyści
„Zarobisz szybko i bez rzyyka!"

Pamiętaj! Nie podejmuj decyzji finansowych pod presją rozmówcy. Przerwij kontakt, jeśli coś budzi Twoje wątpliwości, a następnie niezależnie sprawdź, czy przedstawiona historia jest prawdziwa.

3. OSZUSTWO NA PRACOWNIKA BANKU

Typowa rozmowa z rzekomym pracownikiem banku

Przestępcy często podszywają się pod pracowników banków. Dzwonią, aby wzbudzić strach i nakłonić Cię do podania danych, kodów lub wykonania przelewu.

1 Dzwoni telefon...



2 Oszust wzbudza strach...



3 Prosi o podanie danych...



4 Może poprosić o zainstalowanie aplikacji...



5 Na koniec namawia do przelewu...



6 Później orientuje się, że to oszustwo



Na co zwrócić uwagę?

- Rozmówca wywołuje strach i pośpiech.
- Podaje się za pracownika banku, policjanta lub innej instytucji.
- Prosi o podanie kodów SMS, kodów BLIK, haseł do banku.
- Nakłania do instalacji aplikacji lub kliknięcia w link.
- Proponuje wykonanie przelewu na „bezpieczne konto".

Co zrobić?

1. Zakończ rozmowę, jeśli masz wątpliwości.
2. Nie podawaj żadnych kodów, haseł ani danych.
3. Nie instaluj aplikacji na polecenie rozmówcy.
4. Samodzielnie znajdź oficjalny numer swojego banku (np. na karcie lub stronie internetowej) i zadzwoń, aby sprawdzić, czy rzeczywiście jest zagrożenie.
5. Jeśli podałeś dane lub wykonałeś przelew – natychmiast skontaktuj się z bankiem i zgłoś sprawę.

Czego nie robić?

- Nie podawaj kodów SMS i kodów BLIK.
- Nie podawaj haseł do banku.
- Nie instaluj żadnych aplikacji na polecenie innych osób.
- Nie klikaj w linki przesyłane w wiadomościach.
- Nie wykonuj przelewów na „bezpieczne konto".

Pamiętaj!

Prawdziwy bank nigdy nie prosi o podanie kodów SMS, kodów BLIK ani haseł i nie nakłania do instalowania dodatkowych aplikacji. W razie wątpliwości zawsze skontaktuj się z bankiem samodzielnie.

4. FAŁSZYWE SMS-Y I WIADOMOŚCI Z LINKAMI

Nie klikaj w podejrzane linki!

Fałszywa wiadomość może prowadzić do utraty pieniędzy.

Oszuści wysyłają SMS-y i wiadomości e-mail, które wyglądają jak informacje od firm kurierskich, banków, urzędów lub innych znanych instytucji.

1 Pan Jan otrzymuje SMS-a



2 Wiadomość wygląda wiarygodnie



3 Po kliknięciu w link otwiera się strona



4 Pan Jan zauważa podejrzane szczegóły



Na co Pan Jan zwrócił uwagę?

- adres strony jest inny niż oficjalny,
- wiadomość pochodzi z nieznanego numeru,
- prośba o podanie danych karty płatniczej,
- niewielka kwota dopłaty ma skłonić do szybkiej decyzji,
- na stronie widoczny jest nacisk czasu (np. „Zapłać teraz, aby paczka nie została zwrócona").

5 Pan Jan samodzielnie sprawdza przesyłkę



6 Fałszywe wiadomości mogą dotyczyć też:

- dopłaty do paczki,
- blokady konta w banku,
- zaległych płatności (np. za prąd, gaz, telefon),
- weryfikacji danych osobowych,
- rzekomych nagród lub zwrotów podatków,
- wygranej w konkursie lub innych atrakcyjnych ofert.

Sygnały ostrzegawcze

- Większość takich wiadomości pochodzi z nieznanych numerów lub adresów e-mail.
- Niewielka kwota dopłaty (np. 1,49 zł), która ma skłonić do szybkiej decyzji.
- Link prowadzi do strony o podejrzanym adresie (np. z literówkami lub dodatkowym słowem).
- Prośba o podanie danych karty płatniczej, kodów SMS lub danych logowania.
- Presja czasu – jeśli nie zapłacisz, paczka zostanie zwrócona lub usługa zostanie zablokowana.

Co zrobić?

1. Nie klikaj w linki z podejrzanych wiadomości.
2. Nie podawaj danych karty, kodów SMS ani danych logowania.
3. Sprawdź informacje samodzielnie na oficjalnej stronie lub w aplikacji firmy (np. InPost, Poczta Polska). Adres wpisz ręcznie – nie korzystaj z linku z wiadomości.
4. W razie wątpliwości skontaktuj się bezpośrednio z daną firmą, korzystając z oficjalnych danych kontaktowych (numer telefonu lub strona internetowa).

Jeśli podałeś już dane

1. Natychmiast skontaktuj się z bankiem i rozważ zastrzeżenie karty płatniczej.
2. Zmień hasła do ważnych kont (np. bank, poczta e-mail).
3. Zgłoś wiadomość jako próbę oszustwa – prześlij SMS na numer **8080** (CERT Polska).
4. Sprawdź, czy na Twoim koncie nie wykonano nieautoryzowanych transakcji.
5. Zgłoś sprawę na policję, jeśli straciłeś pieniądze.

5. OSZUSTWO NA CZŁONKA RODZINY

„Dziadku, potrzebuję pomocy!"

Oszuści podają się za bliskich i proszą o pilne pieniądze.

Przestępcy często podszywają się pod wnuków, synów lub córki. Wzbudzają silne emocje, wywierają presję czasu i proszą o pieniądze, tłumacząc, że znaleźli się w trudnej sytuacji.

1 Pan Jan odbiera telefon



2 Oszust wyjaśnia sytuację



3 Oszust wywiera presję



4 Pan Jan postanawia sprawdzić



5 Prawda wychodzi na jaw



6 Pan Jan uniknął oszustwa



Sygnały ostrzegawcze

- Telefon od rzekomego wnuka, syna lub córki, który jest w nagłej sytuacji (np. wypadek, zatrzymanie przez policję).
- Informacja, że rozmówca dzwoni z innego telefonu (np. kolegi), bo jego się zepsuł.
- Pilna prośba o przekazanie gotówki lub wykonanie przelewu.
- Prośba o zachowanie tajemnicy i nieinformowanie innych członków rodziny.
- Silna presja czasu i emocjonalne wzbudzanie strachu lub poczucia winy.

Co zrobić?

1. Zakończ rozmowę, jeśli wzbudza Twoje wątpliwości.
2. Samodzielnie zadzwoń do bliskiej osoby na znany Ci numer telefonu.
3. Potwierdź sytuację u innego członka rodziny.
4. Nie działaj pod presją czasu. Daj sobie chwilę na spokojne sprawdzenie informacji.
5. W razie wątpliwości skontaktuj się z policją (numer 112) lub porozmawiaj z zaufaną osobą.

Jeśli już przekazałeś pieniądze

1. Jak najszybciej skontaktuj się z bankiem i zgłoś próbę oszustwa.
2. Poproś o zablokowanie przelewu, jeśli jest to jeszcze możliwe.
3. Zgłoś sprawę na policję (numer 112).
4. Przekaż policji wszystkie informacje (np. numer telefonu, numer konta, szczegóły rozmowy).

6. FAŁSZYWE OGŁOSZENIA I ZAKUPY W INTERNECIE

Atrakcyjna okazja? Uważaj!

Oszuści kuszą niską ceną i próbują wyłudzić Twoje pieniądze.

Fałszywe ogłoszenia mogą dotyczyć różnych produktów: rowerów, elektroniki, mebli, narzędzi czy biletów. Cena znacznie niższa od rynkowej powinna wzbudzić Twoją czujność.

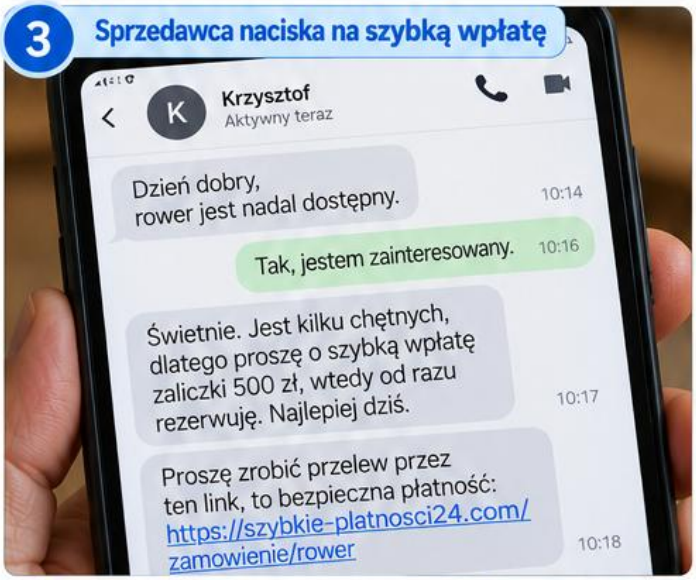
1 Pan Jan znajduje atrakcyjne ogłoszenie



2 Ogłoszenie wygląda wiarygodnie



3 Sprzedawca naciska na szybką wpłatę



4 Pan Jan zauważa niepokojące szczegóły



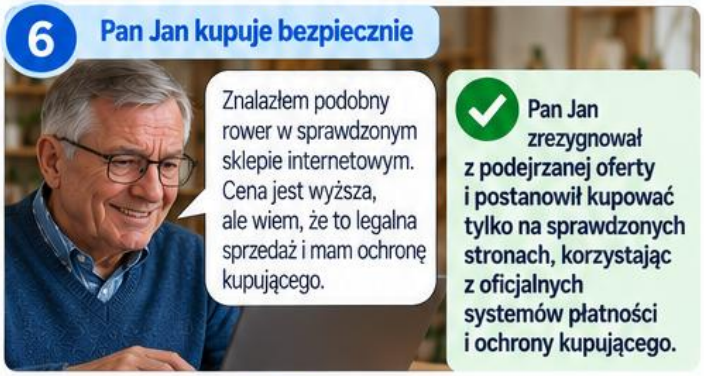
Pan Jan zauważa, że coś się nie zgadza:

- cena jest znacznie niższa od rynkowej,
- sprzedawca nalega na szybką wpłatę zaliczki,
- prosi o płatność poza serwisem ogłoszeniowym,
- przesłał link do strony o podejrzanym adresie (nie jest to oficjalna strona znanego serwisu).

5 Pan Jan sprawdza sprzedawcę



6 Pan Jan kupuje bezpiecznie



Pan Jan zrezygnował z podejrzanej oferty i postanowił kupować tylko na sprawdzonych stronach, korzystając z oficjalnych systemów płatności i ochrony kupującego.

Sygnały ostrzegawcze

- Cena znacznie niższa od rynkowej.
- Sprzedawca nalega na szybką decyzję i wpłatę zaliczki.
- Prośba o płatność poza serwisem ogłoszeniowym (przelew na konto prywatne).
- Link do strony o nietypowym adresie.
- Konto sprzedawcy jest nowe, bez opinii.
- Brak możliwości odbioru osobistego lub tylko wysyłka.

Co zrobić?

1. Sprawdź sprzedawcę – historię konta, liczbę ocen i komentarze.
2. Nie klikaj w linki otrzymane w wiadomościach.
3. Korzystaj z oficjalnej strony lub aplikacji serwisu ogłoszeniowego / sklepu.
4. W razie wątpliwości porównaj cenę z innymi ofertami.
5. Wybieraj bezpieczne metody płatności, które dają ochronę kupującego.

Jeśli wysłałeś już pieniądze

1. Jak najszybciej skontaktuj się z bankiem i spróbuj zablokować przelew.
2. Zachowaj całą korespondencję, potwierdzenia płatności i zrzuty ekranu.
3. Zgłoś sprawę na policję (numer 112) oraz w serwisie ogłoszeniowym.
4. Opisz sytuację i przekaż wszystkie dostępne informacje (link, numer konta, dane sprzedawcy).

7. OSZUSTWO NA BLIK I PRZEJĘTE KONTO ZNAJOMEGO

Znajomy prosi o pomoc?

Oszust może napisać z przejętego konta Twojego znajomego.

Przestępcy często przejmują konta w mediach społecznościowych (np. Facebook, Messenger) i piszą do znajomych z prośbą o kod BLIK lub szybki przelew. Wiadomość wygląda wiarygodnie, bo pochodzi od znanej osoby.

1 Pan Jan otrzymuje wiadomość od znajomego



2 Znajomy prosi o kod BLIK



3 Pan Jan ma wątpliwości



4 Pan Jan dzwoni do znajomego na znany numer



5 To była próba oszustwa



Nie podałem kodu BLIK i nie straciłem pieniędzy!

6 Jak rozpoznać podobne sytuacje?



Zwróć uwagę, jeśli:

- wiadomość jest nietypowa jak na daną osobę,
- znajomy prosi o kod BLIK lub szybki przelew,
- tłumaczy, że nie może wykonać przelewu zwykłą metodą,
- wywiera presję czasu, bo „to bardzo pilne",
- pisze o nagłej sytuacji, np. problemach z telefonem, aplikacją lub płatnościami.

Sygnały ostrzegawcze

- Prośba o kod BLIK lub szybki przelew.
- Wiadomość od znajomego, ale o nietypowej treści.
- Nagła sytuacja i presją czasu.
- Tłumaczenie, że nie działa aplikacja banku i można pomóc tylko kodem BLIK.
- Prośba o zachowanie tajemnicy.
- To samo konto zaczyna pisać do wielu osób.

Co zrobić?

1. Zawsze sprawdź, czy to na pewno Twój znajomy – zadzwoń na znany numer telefonu.
2. Nigdy nie podawaj kodu BLIK, nawet znajomym.
3. Nie działaj pod presją czasu.
4. Sprawdź, czy wiadomość nie zawiera błędów lub nietypowych sformułowań.
5. Jeśli masz wątpliwości, skontaktuj się z innym członkiem rodziny lub wspólnym znajomym.

Jeśli podałeś już kod BLIK lub wysłałeś pieniądze

1. Jak najszybciej skontaktuj się z bankiem i zgłoś nieautoryzowaną transakcję.
2. Zgłoś sprawę na policję (numer 112).
3. Poinformuj znajomego, którego konto zostało przejęte.
4. Zachowaj całą korespondencję (i zrzuty ekranu wiadomości).
5. Zgłoś incydent do administratora serwisu (np. Facebooka) – konto może być zablokowane.

8. FAŁSZYWE INWESTYCJE I OBIETNICE SZYBKIEGO ZYSKU

Szybki zysk? To może być oszustwo!

Oszuści obiecują wysokie zyski i wykorzystują zaufanie oraz emocje.

Fałszywe inwestycje mogą dotyczyć różnych produktów: kryptowalut, akcji, złota, ropy, a także rzekomych projektów energetycznych czy nieruchomości. Oszuści wykorzystują reklamy w internecie, mediach społecznościowych i kontakt telefoniczny.

1 Pan Jan widzi atrakcyjną reklamę



2 Pan Jan wypełnia formularz



3 Telefon od „doradcy inwestycyjnego"



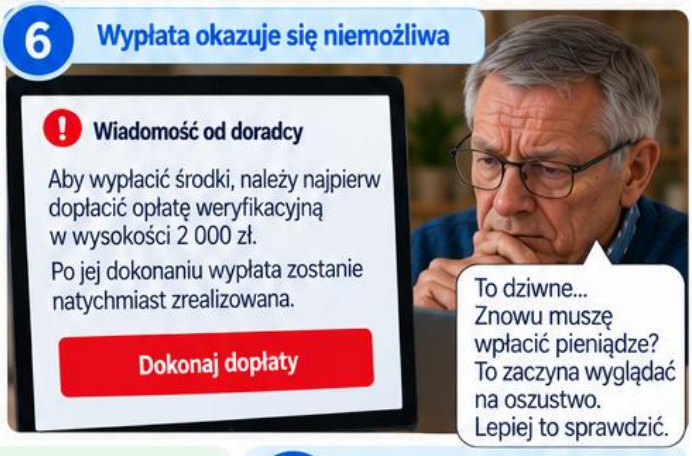
4 Pan Jan wpłaca pierwsze pieniądze



5 Na platformie pojawiają się „zyski"



6 Wypłata okazuje się niemożliwa



Sygnały ostrzegawcze

- Obietnice wysokich i szybkich zysków (np. 10–20% miesięcznie).
- Informacja „bez ryzyka" – każda inwestycja wiąże się z ryzykiem.
- Reklamy z wizerunkiem znanych osób bez ich rzeczywistej zgody.
- Nacisk na szybką decyzję.
- Konieczność wpłaty zaliczki lub kolejnych „opłat" (np. weryfikacyjnej, podatku).
- Kontakt tylko przez telefon, komunikatory lub e-mail – brak spotkania na żywo.
- Przelew na konto zagraniczne lub do firmy o niejasnej siedzibie.
- Brak możliwości wypłaty środków lub ciągłe żądanie dodatkowych wpłat.

Co zrobić?

1. Sprawdź, czy firma ma zezwolenie KNF – lista ostrzeżeń na stronie **knf.gov.pl**.
2. Zweryfikuj opinie o firmie w niezależnych źródłach (nie tylko na stronie firmy).
3. Nie ufaj obietnicom szybkiego zysku – każda inwestycja wiąże się z ryzykiem.
4. Nie instaluj żadnych aplikacji do zdalnego dostępu na prośbę „doradcy".
5. Nie udostępniaj swoich danych osobowych, danych do logowania ani danych karty płatniczej.
6. Skonsultuj się z zaufaną osobą z rodziny lub doradcą finansowym, zanim wpłacisz pieniądze.

Jeśli już zainwestowałeś pieniądze

1. Jak najszybciej skontaktuj się z bankiem i sprawdź, czy można zatrzymać przelew.
2. Zgłoś sprawę na policję (numer 112).
3. Zawiadom KNF, korzystając z formularza na stronie **knf.gov.pl** (w sekcji „Zgłoś nieprawidłowości").
4. Zachowaj całą korespondencję, umowy, potwierdzenia przelewów i zrzuty ekranu.
5. Ostrzeż rodzinę i znajomych, aby nie padli ofiarą podobnego oszustwa.

9. FAŁSZYWY KONSULTANT TECHNICZNY

Twój komputer ma wirusa!

Przestępcy dzwonią lub wyświetlają fałszywe komunikaty, podając się za pracowników znanych firm (np. Microsoft, Apple) lub Twojego dostawcę internetu. Twierdzą, że na Twoim komputerze jest wirus i trzeba go pilnie usunąć. Proszą o zainstalowanie programu do zdalnego dostępu.

Oszuści podszywają się pod pracowników znanych firm i próbują uzyskać zdalny dostęp do Twojego urządzenia.

1 Pan Jan widzi niepokojący komunikat



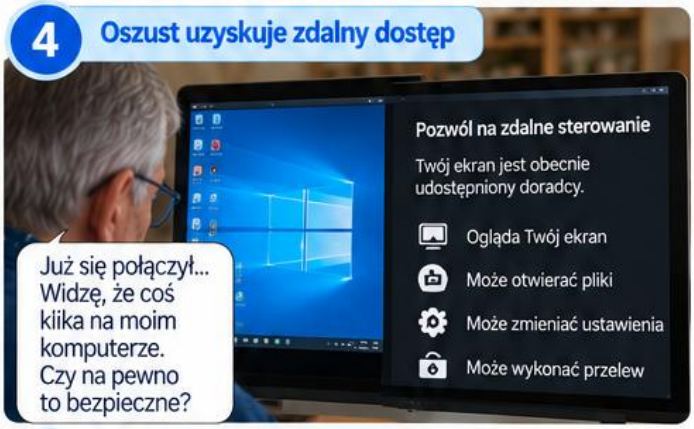
2 Dzwoni fałszywy konsultant



3 Prośba o instalację programu



4 Oszust uzyskuje zdalny dostęp



5 Próba wyłudzenia pieniędzy



6 Pan Jan przerywa i sprawdza



Sygnały ostrzegawcze

- Nagły komunikat o wirusach na ekranie.
- Telefon od osoby podającej się za pracownika znanej firmy (np. Microsoft, Apple, operator internetu).
- Prośba o zainstalowanie programu do zdalnego dostępu (np. AnyDesk, TeamViewer).
- Twierdzenie, że trzeba szybko działać, bo dane są zagrożone.
- Żądanie opłaty za „naprawę", licencję antywirusową lub „odblokowanie" komputera.
- Próba uzyskania danych karty płatniczej lub wykonania przelewu.

Co zrobić?

1. Nie ufaj komunikatom o wirusach ani telefonom od rzekomych konsultantów.
2. Nie instaluj żadnych programów do zdalnego dostępu na prośbę nieznajomej osoby.
3. Nie podawaj danych karty, numerów kont ani kodów do płatności.
4. Samodzielnie sprawdź, czy Twój komputer rzeczywiście ma problemy (np. użyj zaktualizowanego programu antywirusowego).
5. W razie wątpliwości skontaktuj się z rodziną lub znajomym, który zna się na komputerach.
6. Pamiętaj: prawdziwe firmy nie dzwonią i nie proszą o zdalny dostęp ani o płatność za „usunięcie wirusa".

Jeśli uzyskałeś dostęp lub podałeś dane

1. Natychmiast odłącz komputer od internetu (Wi-Fi i kabel).
2. Zmień wszystkie hasła (poczta e-mail, bank, media społecznościowe).
3. Skontaktuj się z bankiem, jeśli podałeś dane karty lub wykonałeś przelew.
4. Zgłoś sprawę na policję (numer 112).
5. Zrób zrzuty ekranu komunikatów i zachowaj całą korespondencję.
6. Przeskanuj komputer programem antywirusowym lub poproś zaufaną osobę o pomoc.

10. FAŁSZYWE NAGRANIA, GŁOSY AI I DEZINFORMACJA

To wygląda i brzmi prawdziwie? Uważaj!



Dzięki sztucznej inteligencji oszuści mogą tworzyć bardzo wiarygodne nagrania – głosy bliskich osób, fałszywe filmy znanych osób, informacje o rzekomych zagrożeniach czy pilnych okazjach. Sprawdzaj źródła i nie działaj pod wpływem emocji.

Oszuści wykorzystują sztuczną inteligencję do tworzenia fałszywych nagrań, głosów i wiadomości.

1 Pan Jan ogląda nagranie w internecie



2 Fałszywy głos bliskiej osoby



3 Fałszywa wiadomość w mediach społecznościowych



4 Pan Jan sprawdza źródło



5 Pan Jan nie działa pod wpływem emocji



6 Pan Jan rozmawia z rodziną i zgłasza próbę oszustwa



Sygnały ostrzegawcze

- Nagrania znanych osób zachęcające do inwestycji lub zakupów.
- Glos bliskiej osoby proszącej o pilne pieniądze.
- Informacje o rzekomych nowych opłatach, podatkach lub zagrożeniach.
- Wiadomości, które wywołują silne emocje (strach, radość, pośpiech).
- Nietypowy numer telefonu, z którego dzwoni znajomy.
- Prośba o zachowanie tajemnicy.
- Podejrzane profile w mediach społecznościowych utworzone niedawno.
- Błędy w tekście, dziwne adresy stron, brak oficjalnych źródeł.

Co zrobić?

1. Zachowaj spokój i nie działaj pod wpływem emocji.
2. Zweryfikuj informację w oficjalnych źródłach (np. strony rządowe, znane media: TVP, Polsat, RMF, PAP).
3. Skontaktuj się z bliską osobą na znany numer telefonu, aby potwierdzić, czy to prawda.
4. Sprawdź profil w mediach społecznościowych (kiedy został utworzony, ile ma obserwujących, czy są wcześniejsze posty).
5. Nie klikaj w podejrzane linki i nie pobieraj plików.
6. Jeśli masz wątpliwości, zapytaj kogoś zaufanego – rodzinę, znajomych lub lokalne służby.

Jeśli dałeś się oszukać

1. Jeśli przelałeś pieniądze – natychmiast skontaktuj się z bankiem i spróbuj zatrzymać przelew.
2. Zgłoś sprawę na policję (numer 112).
3. Zachowaj wszystkie dowody: nagrania, wiadomości, linki, zrzuty ekranu, numery telefonu.
4. Poinformuj rodzinę i znajomych, aby ostrzec ich przed podobnym oszustwem.
5. Zgłoś fałszywe treści w serwisach społecznościowych (np. Facebook, YouTube, TikTok).

11. BEZPIECZNY TELEFON I OCHRONA DANYCH

Twój telefon – Twoje bezpieczeństwo

Smartfon to bardzo przydatne narzędzie, ale też cel dla oszustów. Warto odpowiednio go zabezpieczyć i korzystać z niego świadomie.

Dobrze zabezpieczony telefon chroni Twoje dane, pieniądze i prywatność.

1 Pan Jan ustawia blokadę ekranu



2 Pan Jan dba o aktualizacje



3 Pan Jan uważa na podejrzane wiadomości



4 Pan Jan kontroluje uprawnienia aplikacji



5 Pan Jan korzysta z bezpiecznych aplikacji



6 Pan Jan bezpiecznie korzysta z bankowości



Sygnały ostrzegawcze

- Wiadomości z nieznanych numerów z linkami (np. o dopłatach, paczkach, winach, zwrotach podatku).
- Prośby o instalację aplikacji spoza oficjalnego sklepu.
- Aplikacje żądające zbyt wielu uprawnień (np. dostępu do kontaktów, SMS-ów, lokalizacji).
- Nagłe komunikaty o konieczności aktualizacji z podejrzanych stron.
- Nieznane połączenia z sugestią „pomocy technicznej".
- Nietypowe zachowanie telefonu (np. szybkie rozładowywanie baterii, dziwne reklamy).

Co zrobić?

1. Ustaw blokadę ekranu (kod PIN, hasło lub odcisk palca).
2. Regularnie aktualizuj system i aplikacje.
3. Pobieraj aplikacje tylko z oficjalnych sklepów (Google Play, App Store).
4. Sprawdzaj opinie o aplikacjach i liczbę pobrań.
5. Kontroluj uprawnienia aplikacji i wyłącz te, które są niepotrzebne.
6. Nie klikaj w linki z podejrzanych wiadomości.
7. Korzystaj z aplikacji bankowej – nigdy nie loguj się przez linki z wiadomości.
8. W razie wątpliwości skontaktuj się z bliską osobą lub infolinią instytucji.

Dodatkowe wskazówki

1. Włącz funkcję „Znajdź moje urządzenie" (na Androidzie lub iPhonie).
2. Używaj silnego kodu PIN (nie 1234 ani daty urodzenia).
3. Włącz uwierzytelnianie dwuskładnikowe tam, gdzie to możliwe.
4. Nie zapisuj haseł w notatkach w telefonie.
5. Uważaj na otwarte sieci Wi-Fi – nie loguj się do banku w miejscach publicznych.
6. Regularnie sprawdzaj listę zalogowanych urządzeń w banku, poczcie e-mail i mediach społecznościowych.
7. W przypadku zgubienia lub kradzieży telefonu – jak najszybciej zdalnie go zablokuj i zmień hasła do ważnych kont.

12. FAŁSZYWE WIADOMOŚCI Z URZĘDÓW, BANKÓW I FIRM

Wygląda prawdziwie, ale to może być oszustwo!

Oszuści podszywają się pod znane instytucje, aby wyłudzić Twoje dane lub pieniądze.

Instytucje publiczne i banki zazwyczaj nie proszą o podanie haseł, kodów SMS ani danych karty w wiadomościach e-mail lub SMS.

1 Fałszywa wiadomość z urzędu skarbowego



2 Fałszywy e-mail z banku



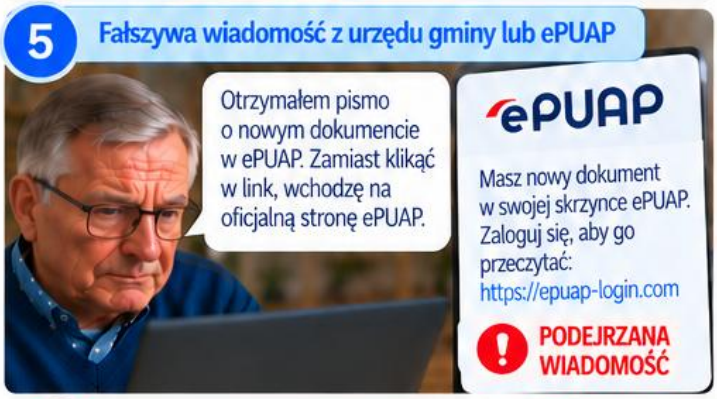
3 Fałszywa wiadomość od firmy kurierskiej



4 Fałszywa wiadomość z ZUS



5 Fałszywa wiadomość z urzędu gminy lub ePUAP



6 Fałszywa oferta od znanej firmy



Sygnały ostrzegawcze

- Wiadomości o pilnej zapłacie, blokadzie konta, świadczeniu lub zwrocie pieniędzy.
- Prośba o podanie danych osobowych, kodów SMS, haseł, numeru karty.
- Linki w SMS lub e-mailu prowadzące do nieznanych stron.
- Błędy językowe, dziwne sformułowania i nacisk na szybkie działanie („tylko dziś").
- Oferty zbyt atrakcyjne (np. bardzo tanie produkty).
- Nadawcy podszywający się pod instytucje, banki, firmy kurierskie lub znane sklepy.
- Załączniki w e-mailach, których się nie spodziewasz.
- Nieoczekiwane informacje o zaległościach, zwrotach podatków, dopłatach lub nowych dokumentach.

Co zrobić?

1. Nie klikaj w linki w podejrzanych wiadomościach.
2. Nie podawaj danych osobowych, kodów ani haseł.
3. Sprawdź informacje na oficjalnej stronie instytucji lub w aplikacji.
4. Jeśli masz wątpliwości, zadzwoń na oficjalną infolinię (użyj numeru ze strony instytucji).
5. Porównaj adres strony internetowej – oszuści często używają podobnych, ale fałszywych adresów.
6. Nie otwieraj podejrzanych załączników.
7. Zgłoś podejrzaną wiadomość do instytucji, pod którą ktoś się podszywa.

Przykłady oficjalnych kontaktów

gov.pl	**www.gov.pl** (portal rządowy)
ZUS	**www.zus.pl** infolinia: 22 560 16 00
KAS	**Krajowa Administracja Skarbowa** **www.podatki.gov.pl** infolinia: 22 330 03 30
ePUAP	**www.epuap.gov.pl** infolinia: 42 253 54 50
Twój bank	Zawsze korzystaj z oficjalnej strony lub aplikacji swojego banku
Policja	**112** (w sytuacji oszustwa)
CERT Polska	**https://incydent.cert.pl** (zgłoszenie podejrzanych wiadomości)

13. HASŁA, BEZPIECZNE LOGOWANIE I OCHRONA PESEL

Silne hasła, większe bezpieczeństwo

Jedno hasło to duże ryzyko. Chroń swoje konta i zastrzeż PESEL.

Dobre hasła, dodatkowa weryfikacja logowania i zastrzeżony PESEL utrudniają oszustom dostęp do Twoich danych i pieniędzy.

1 Pan Jan używa jednego hasła do wielu kont



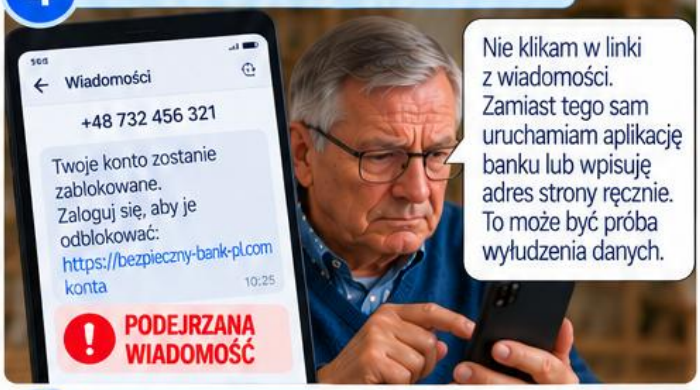
2 Pan Jan tworzy mocne, unikalne hasła



3 Pan Jan włącza dodatkowe zabezpieczenie logowania



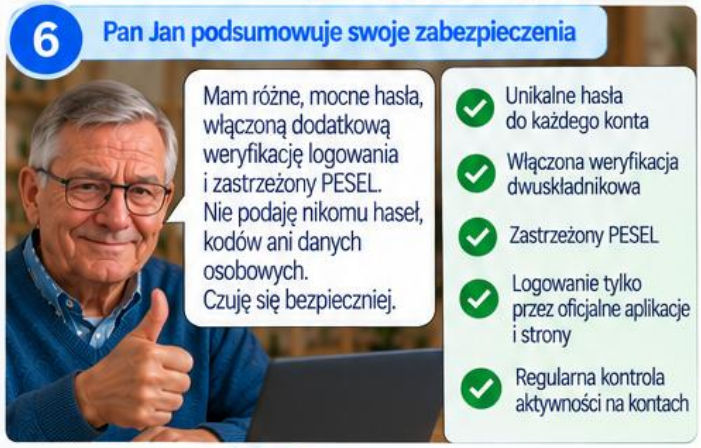
4 Pan Jan otrzymuje podejrzaną wiadomość



5 Pan Jan zastrzega swój numer PESEL



6 Pan Jan podsumowuje swoje zabezpieczenia



Sygnały ostrzegawcze

- Prośby o podanie hasła, kodu SMS lub kodu z aplikacji.
- Wiadomości z linkami do „logowania", „odblokowania konta" lub „aktualizacji danych".
- Informacje o nietypowej aktywności na Twoim koncie.
- Strony logowania o podejrzanym adresie internetowym (np. literówki, dodatkowe znaki).
- Prośby o zdalny dostęp do komputera lub telefonu w celu „naprawy konta".
- Wykorzystanie Twoich danych, np. próba zaciągnięcia kredytu lub umowy na Twoje nazwisko.

Co zrobić?

1. Używaj długich i unikalnych haseł do każdego konta.
2. Włącz uwierzytelnianie dwuskładnikowe (2FA) tam, gdzie to możliwe.
3. Loguj się tylko przez oficjalne aplikacje i strony (wpisuj adres ręcznie lub korzystaj z zapisanych zakładek).
4. Regularnie sprawdzaj aktywność na swoich kontach i listę zalogowanych urządzeń.
5. Zastrzeż numer PESEL w aplikacji mObywatel, na gov.pl lub w urzędzie gminy.
6. Nie podawaj haseł, kodów ani numeru PESEL przez telefon, e-mail ani w wiadomościach.
7. Rozważ korzystanie z menedżera haseł.

Jeśli ktoś poznał Twoje dane

1. Natychmiast zmień hasło do zagrożonego konta (poczta, bank, media społecznościowe).
2. Sprawdź i zakończ aktywne sesje logowania na wszystkich urządzeniach.
3. Włącz weryfikację dwuskładnikową, jeśli nie była włączona.
4. Skontaktuj się z bankiem, jeśli istnieje ryzyko utraty pieniędzy lub nieautoryzowanych transakcji.
5. Sprawdź status zastrzeżenia PESEL i historię wykorzystania swoich danych (mObywatel lub gov.pl).
6. Zgłoś sprawę na policję (numer 112), jeśli doszło do wyłudzenia danych lub straty finansowej.

14. CO ZROBIĆ, GDY PADNIESZ OFIARĄ OSZUSTWA?

Działaj szybko – to może ograniczyć straty!

Jeśli podejrzewasz, że dałeś się oszukać, nie czekaj. Każda minuta jest ważna.

Nawet jeśli wstydzisz się, że dałeś się oszukać – zgłoś sprawę. To może pomóc Tobie i innym.

1 Pan Jan zauważa niepokojącą transakcje



2 Pan Jan kontaktuje się z bankiem



3 Zabezpiecza swoje konta i urządzenia



- Zmieniam hasła do najważniejszych kont (poczta, bank, media społecznościowe).
- Wylogowuję podejrzane sesje.
- Sprawdzam, czy w telefonie nie ma zainstalowanych nieznanych aplikacji.
- Aktualizuję system i programy.

4 Zgłasza sprawę na policję



5 Zgłasza incydent do odpowiednich instytucji



- CERT.PL — Zgłoś oszustwo internetowe: https://incydent.cert.pl
- U.KE — Zgłoś podejrzaną stronę lub firmę: https://uokik.gov.pl
- KNF — Sprawdź ostrzeżenia przed nieuczciwymi firmami: https://www.knf.gov.pl

6 Monitoruje sytuację



- Regularnie sprawdzam stan konta.
- Kontroluję, czy nie pojawiają się nowe, podejrzane transakcje.
- Sprawdzam, czy moje dane nie zostały wykorzystane (np. wnioski kredytowe).
- Rozważam zastrzeżenie numeru PESEL, jeśli istnieje ryzyko kradzieży tożsamości.

Sygnały ostrzegawcze
że mogło dojść do oszustwa

- Nie rozpoznajesz transakcji na koncie.
- Otrzymałeś wiadomość z prośbą o podanie kodu, hasła lub danych.
- Ktoś uzyskał zdalny dostęp do Twojego komputera lub telefonu.
- Twoje konto w mediach społecznościowych zostało przejęte.
- Otrzymujesz powiadomienia o logowaniu z nieznanych urządzeń.
- Zniknęły pieniądze lub ktoś złożył wniosek kredytowy na Twoje dane.
- Podejrzane połączenia, wiadomości lub aktywność na Twoich kontach.

Szybki plan działania
krok po kroku

1. Skontaktuj się z bankiem – zgłoś nieautoryzowaną transakcję i zablokuj kartę, dostęp do konta oraz bankowość internetową.
2. Zmień hasła do zagrożonych kont (poczta, bank, media społecznościowe).
3. Sprawdź i zabezpiecz swoje urządzenia (telefon, komputer).
4. Zgłoś sprawę na policję (numer 112 lub najbliższy komisariat).
5. Zgłoś incydent do CERT Polska: **https://incydent.cert.pl**
6. Sprawdź, czy Twoje dane nie zostały wykorzystane (np. BIK, zastrzeżenie PESEL).
7. Zachowaj wszystkie dowody (zrzuty ekranu, wiadomości, numery telefonów, potwierdzenia przelewów).

Ważne numery i linki

112	**Policja** (numer alarmowy)
800 302 302	**CERT Polska** (zgłaszanie incydentów)
800 120 226	**Zastrzeż PESEL** (infolinia gov.pl)
801 889 889	**BIK** (sprawdź, czy ktoś nie wziął kredytu na Twoje dane)

- **https://incydent.cert.pl** — Zgłoś oszustwo internetowe
- **https://www.knf.gov.pl** — Sprawdź ostrzeżenia KNF
- **https://uokik.gov.pl** — Zgłoś nieuczciwą firmę lub stronę
- **https://www.bik.pl** — Sprawdź, czy Twoje dane są wykorzystywane

15. DANE OSOBOWE I DOKUMENTY

Twoje dane są cenne – chroń je!

Nie udostępniaj swoich dokumentów, zdjęć ani danych w internecie i przez telefon, jeśli nie masz pewności, komu je przekazujesz.

PESEL, dowód osobisty, dane adresowe i inne informacje mogą zostać wykorzystane przez oszustów do zaciągania kredytów, wyłudzeń i kradzieży tożsamości.

1 Pan Jan poznaje, które dane są wrażliwe



2 Pan Jan nie udostępnia zdjęć dokumentów



3 Pan Jan uważa na podawanie danych w formularzach



4 Pan Jan zabezpiecza swoje dokumenty



5 Pan Jan korzysta z mObywatel i sprawdza swoje dane



6 Pan Jan jest ostrożny przy wysyłaniu danych



Sygnały ostrzegawcze

- Prośba o przesłanie zdjęcia dowodu osobistego, prawa jazdy lub paszportu przez e-mail, komunikator lub formularz.
- Formularze z prośbą o podanie PESEL, adresu, numeru telefonu lub danych karty.
- Obietnica nagrody, zwrotu podatku lub szybkiego kredytu w zamian za podanie danych.
- Podejrzane strony internetowe, które wyglądają jak oficjalne serwisy.
- Prośby o skan dokumentów „do weryfikacji" przez nieznane firmy lub osoby.
- Wyciek danych z serwisów internetowych (wiadomości o naruszeniu bezpieczeństwa).
- Nieoczekiwane informacje o zaciągnięciu kredytu, zakupach na Twoje dane lub otwarciu konta.

Co zrobić?

1. Nie udostępniaj swoich danych osobowych i dokumentów, jeśli nie masz pewności, komu je przekazujesz.
2. Nie wysyłaj zdjęć dowodu ani innych dokumentów e-mailem, przez komunikatory lub formularze w internecie.
3. Sprawdzaj status zastrzeżenia PESEL w aplikacji mObywatel lub na gov.pl.
4. Korzystaj tylko z oficjalnych stron instytucji i aplikacji.
5. Usuwaj niepotrzebne zdjęcia i skany dokumentów z telefonu, komputera i chmury.
6. Uważaj na oferty szybkich kredytów, pożyczek i nagród – może to być oszustwo.
7. Regularnie sprawdzaj, czy ktoś nie wykorzystał Twoich danych (np. w BIK).

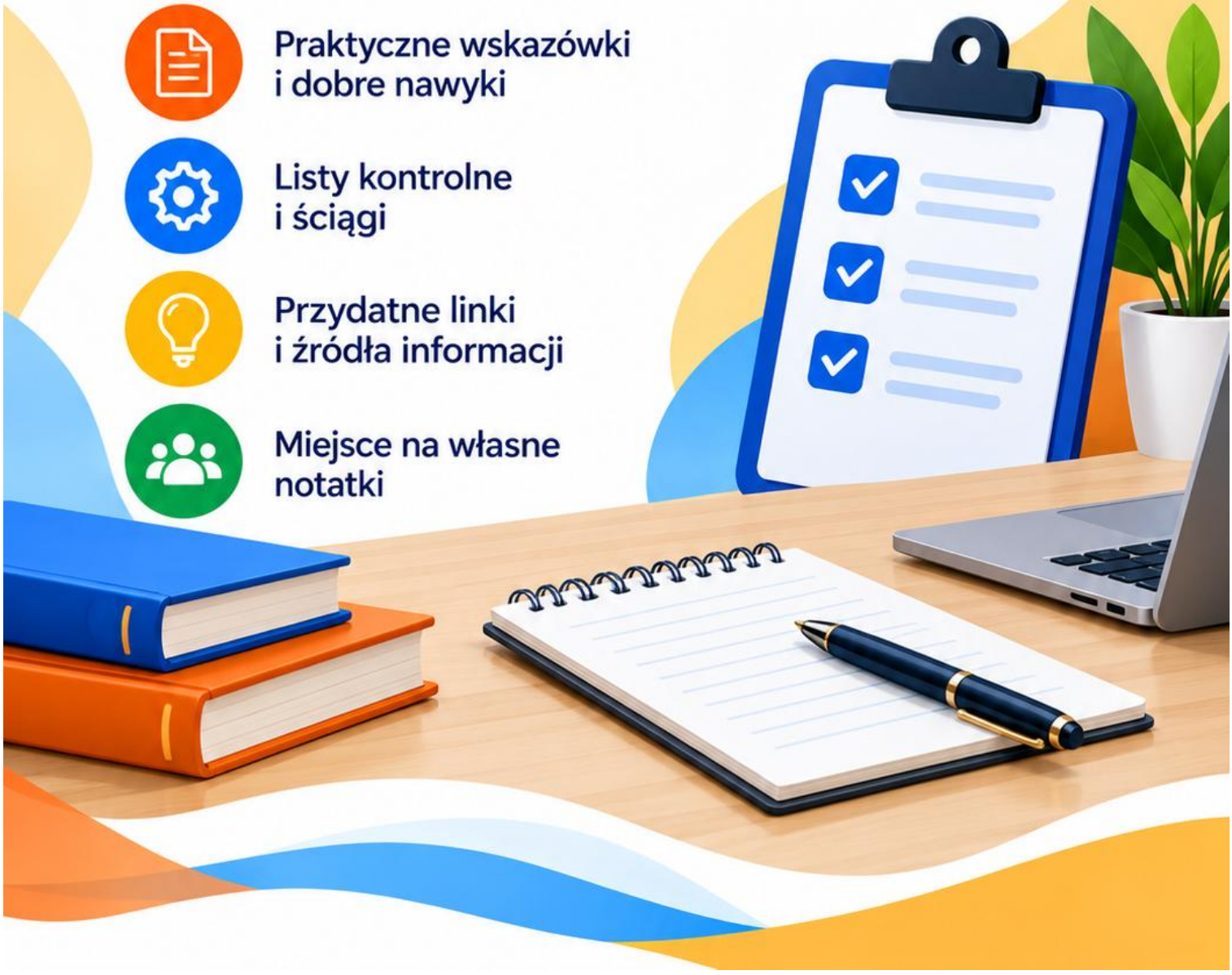
Dodatkowe wskazówki

1. Włącz powiadomienia w mObywatel o próbach użycia Twojego PESEL.
2. Sprawdzaj swoją historię w BIK (co 6 miesięcy możesz uzyskać darmowy raport).
3. Nie publikuj swoich danych (adresu, telefonu, daty urodzenia) w mediach społecznościowych.
4. Ustaw w telefonie blokadę ekranu (PIN, hasło lub odcisk palca).
5. Korzystaj z bezpiecznego, silnego hasła do poczty e-mail.
6. Po zakończeniu sprawy usuwaj kopie dokumentów ze swojego urządzenia.
7. W razie wątpliwości skontaktuj się bezpośrednio z urzędem, bankiem lub zaufaną instytucją.

Dodatki

Dodatkowe materiały, porady i przydatne informacje

- Praktyczne wskazówki i dobre nawyki
- Listy kontrolne i ściągi
- Przydatne linki i źródła informacji
- Miejsce na własne notatki



17. ĆWICZENIE – OSZUSTWO CZY PRAWDZIWA WIADOMOŚĆ?

Sprawdź swoją czujność

Przeczytaj poniższe wiadomości i zdecyduj, czy to oszustwo, czy prawdziwa wiadomość. Po każdym przykładzie znajdziesz krótkie wyjaśnienie na dole strony.

Nie każda wiadomość w internecie jest oszustwem. Zawsze jednak warto ją sprawdzić i dobrze się zastanowić, zanim klikniesz w link lub podasz swoje dane.

1 SMS o wygranej w konkursie



☐ To oszustwo ☐ To prawdziwa wiadomość

2 Wiadomość od operatora o przerwie technicznej



☐ To oszustwo ☐ To prawdziwa wiadomość

3 E-mail o zablokowaniu konta społecznościowego



☐ To oszustwo ☐ To prawdziwa wiadomość

4 Potwierdzenie wizyty w przychodni



☐ To oszustwo ☐ To prawdziwa wiadomość

5 Wiadomość od znajomego z prośbą o głosowanie



☐ To oszustwo ☐ To prawdziwa wiadomość

6 E-mail o zaległej fakturze za prąd



☐ To oszustwo ☐ To prawdziwa wiadomość

Rozwiązanie i wyjaśnienia

1. **Oszustwo** – nieoczekiwana nagroda, konieczność wpłaty niewielkiej kwoty i podejrzany link. To próba wyłudzenia danych i pieniędzy.
2. **Prawdziwa wiadomość** – informacja o planowanej przerwie technicznej od znanego operatora. Nie zawiera prośby o podanie danych ani płatności. Można ją potwierdzić w aplikacji operatora.
3. **Oszustwo** – groźba zablokowania konta, presja czasu i prośba o podanie danych. Link prowadzi do fałszywej strony.
4. **Prawdziwa wiadomość** – potwierdzenie wizyty, którą Pan Jan wcześniej umówił. Bez linków do płatności. W razie wątpliwości można skontaktować się z przychodnią.
5. **Oszustwo** – prośba o głosowanie może prowadzić do przejęcia konta. Najpierw skontaktuj się ze znajomą innym kanałem (telefonicznie).
6. **Oszustwo** – groźba odłączenia prądu, bardzo krótki termin i płatność przez link. Sprawdź rachunek w oficjalnym serwisie dostawcy energii.

Na co zwrócić uwagę?

- ☐ Czy wiadomość pasuje do Twojej sytuacji?
- ☐ Czy nadawca jest znany i wiarygodny?
- ☐ Czy nie ma presji czasu („tylko dziś", „w ciągu godzin")?
- ☐ Czy nie prosi o podanie danych osobowych, haseł, kodów SMS lub płatności?
- ☐ Czy link prowadzi do oficjalnej strony? Sprawdź dokładny adres.
- ☐ Czy wiadomość zawiera błędy językowe lub dziwne sformułowania?
- ☐ Jeśli masz wątpliwości, skontaktuj się z nadawcą innym kanałem (telefon, oficjalna strona lub aplikacja).

Pamiętaj!

1. Nie klikaj w linki z nieznanych wiadomości.
2. Nie podawaj swoich danych osobowych, kodów SMS ani haseł.
3. Zawsze sprawdzaj informacje na oficjalnych stronach i w aplikacjach.
4. Jeśli wiadomość dotyczy pieniędzy, skontaktuj się bezpośrednio z daną firmą lub instytucją.
5. Oszuści często wykorzystują emocje – radość, strach, presję czasu.
6. Lepiej poświęcić kilka minut na sprawdzenie, niż później żałować.

18. MOJA LISTA BEZPIECZEŃSTWA – DO SAMODZIELNEGO SPRAWDZENIA

Zadbaj o swoje bezpieczeństwo w internecie

Przejdź przez listę, zaznacz wykonane punkty i stosuj te zasady na co dzień. To proste działania, które naprawdę chronią Twoje dane, pieniądze i spokój.

Nie musisz znać wszystkiego od razu. Wystarczy, że zaczniesz od kilku najważniejszych rzeczy i stopniowo będziesz je wdrażać.

1 Zabezpieczam telefon i komputer



- ☐ Używam blokady ekranu (np. kod, PIN, odcisk palca).
- ☐ Regularnie instaluję aktualizacje systemu i aplikacji.
- ☐ Pobieram aplikacje tylko z oficjalnych sklepów (Google Play, App Store).
- ☐ Usuwam nieużywane i nieznane aplikacje.

2 Dbam o hasła i konta



- ☐ Używam silnych, unikalnych haseł do każdego konta.
- ☐ Korzystam z menedżera haseł lub zapisuję hasła w bezpiecznym miejscu (nie na kartce przy komputerze).
- ☐ Włączam dodatkowe zabezpieczenie logowania (np. kod SMS lub aplikację autoryzacyjną).
- ☐ Regularnie sprawdzam powiadomienia o logowaniach do swoich kont.

3 Chronię swoje dane osobowe



- ☐ Sprawdzam status zastrzeżenia PESEL w aplikacji mObywatel lub na stronie gov.pl.
- ☐ Nie udostępniam zdjęć dowodu osobistego ani innych dokumentów w internecie.
- ☐ Uważam, komu podaję swój adres, numer telefonu, e-mail.
- ☐ Nie publikuję w sieci informacji o swoich planach wyjazdowych ani o większych zakupach.

4 Sprawdzam, zanim kliknę



- ☐ Nie klikam w linki z nieznanych wiadomości (SMS, e-mail, komunikatory).
- ☐ Nie podaję kodów SMS, kodów z aplikacji ani danych karty płatniczej.
- ☐ Sprawdzam informacje na oficjalnej stronie instytucji lub w aplikacji (wpisując adres samodzielnie).
- ☐ W razie wątpliwości pytam zaufaną osobę (np. rodzinę, znajomego).

5 Wiem, gdzie szukać pomocy



- ☐ Mam zapisany numer infolinii swojego banku.
- ☐ Wiem, jak skontaktować się z policją w razie oszustwa (112).
- ☐ Znam stronę CERT Polska, na której można zgłosić podejrzaną wiadomość.
- ☐ Wiem, do kogo z rodziny lub znajomych mogę zwrócić się o pomoc.

6 Regularnie sprawdzam i porządkuję



- ☐ Co jakiś czas sprawdzam, czy moje dane i hasła nie wyciekły do internetu.
- ☐ Usuwam stare konta, których już nie używam.
- ☐ Przeglądam uprawnienia aplikacji w telefonie (np. dostęp do aparatu, lokalizacji).
- ☐ Rozmawiam z rodziną o zasadach bezpieczeństwa w internecie.

Ważne kontakty – miej pod ręką

Policja	**112** (w sytuacji zagrożenia) lub **997**
CERT Polska	**https://incydent.cert.pl** zgłoszenie podejrzanych wiadomości, stron internetowych i oszustw online
Twój bank	Numer infolinii znajdziesz na oficjalnej stronie banku lub w aplikacji mobilnej.
mObywatel	Aplikacja **mObywatel** do zastrzeżenia PESEL i zarządzania dokumentami.

Dodatkowe narzędzia do sprawdzania

Have I Been Pwned?
https://haveibeenpwned.com
sprawdź, czy Twój e-mail pojawił się w wyciekach danych.

Google – Sprawdzenie haseł
https://passwords.google.com
sprawdź, czy Twoje hasła nie są znane w wyciekach.

Firefox Monitor
https://monitor.firefox.com
sprawdź, czy Twoje dane pojawiły się w wyciekach.

Czy mój PESEL jest bezpieczny?
https://www.gov.pl/web/numer-pesel
informacje o zastrzeżeniu PESEL i możliwości jego ochrony.

Pamiętaj!

1. Zatrzymaj się, pomyśl, nie działaj pod presją.
2. Zawsze sprawdzaj informacje na oficjalnych stronach.
3. Nie podawaj swoich danych osobowych, kodów ani haseł.
4. Używaj silnych, unikalnych haseł.
5. Regularnie aktualizuj system i aplikacje.
6. W razie wątpliwości skontaktuj się z bankiem, rodziną lub policją.

Zatrzymaj się. Sprawdź. Dopiero potem działaj.

Małe działania dają dużą ochronę!

POJĘCIA, KTÓRE WARTO ZNAĆ

Ważne pojęcia z cyberbezpieczeństwa

Proste wyjaśnienia, które pomogą Ci rozpoznać zagrożenia

1 Deepfake – fałszywy obraz lub głos

Deepfake to nagranie, zdjęcie lub wypowiedź stworzone albo przerobione przy użyciu sztucznej inteligencji tak, aby wyglądały lub brzmiały jak prawdziwe. Przestępcy mogą wykorzystywać takie materiały, aby udawać członka rodziny, znajomego lub osobę publiczną i w ten sposób wyłudzać pieniądze lub rozpowszechniać fałszywe informacje.

Przykład

Otrzymujesz wiadomość wideo lub telefon, w którym głos przypomina głos syna, który pilnie prosi o pieniądze.

Jak się chronić?

- Zawsze sprawdzaj taką prośbę innym kanałem, np. oddzwoń na znany numer.
- Nie podejmuj pochopnych decyzji pod presją czasu.



2 Malware – złośliwe oprogramowanie

Malware to ogólna nazwa programów stworzonych po to, aby wyrządzić szkodę użytkownikowi, urządzeniu lub jego danym. Może kraść informacje, śledzić aktywność, wyświetlać niechciane reklamy albo umożliwiać przestępcy dostęp do telefonu lub komputera. Takie oprogramowanie może dostać się na urządzenie np. przez podejrzany załącznik, fałszywą aplikację lub niebezpieczną stronę internetową.

Przykład

Instalujesz aplikację z nieznanego źródła, a ona potajemnie uzyskuje dostęp do Twoich danych.

Jak się chronić?

- Instaluj aplikacje tylko ze sprawdzonych źródeł.
- Aktualizuj telefon i komputer.
- Nie otwieraj podejrzanych załączników i linków.



3 Phishing – wyłudzanie danych

Phishing to metoda oszustwa, w której przestępca podszywa się pod zaufaną instytucję lub firmę, np. bank, pocztę, urząd albo firmę kurierską. Wysyła fałszywą wiadomość e-mail lub SMS, która ma skłonić Cię do kliknięcia w link, otwarcia załącznika lub podania poufnych informacji, takich jak hasło do bankowości internetowej, dane karty płatniczej lub inne dane osobowe.

Przykład

Otrzymujesz SMS z informacją o niedopłacie za przesyłkę. Po kliknięciu linku trafiasz na fałszywą stronę płatności.

Jak się chronić?

- Nie klikaj w linki z wiadomości.
- Sprawdzaj informacje na oficjalnej stronie lub w aplikacji instytucji.
- Nigdy nie podawaj haseł ani danych karty w odpowiedzi na SMS lub e-mail.



4 Uwierzytelnianie dwuskładnikowe (2FA) – dodatkowa ochrona konta

Uwierzytelnianie dwuskładnikowe to sposób **zabezpieczenia konta**, w którym samo hasło nie wystarcza do zalogowania się. Potrzebne jest również drugie potwierdzenie tożsamości, np. kod z aplikacji uwierzytelniającej, zatwierdzenie logowania w aplikacji lub klucz bezpiecceństwa.

Przykład

Ktoś zdobył Twoje hasło, ale podczas logowania system prosi jeszcze o kod z aplikacji. Jeśli to nie Ty się logujesz, odrzuć prośbę.

Jak się chronić?

- Włącz 2FA na poczcie elektronicznej i kontach finansowych.
- Nie przekazuj nikomu kodów i nie zatwierdzaj nieznanych prób logowania.



Pamiętaj!

Znajomość tych pojęć pomaga szybko rozpoznać zagrożenia. Gdy masz wątpliwości – nie działaj pochopnie. Zatrzymaj się, sprawdź informację i w razie potrzeby skonsultuj się z bliskimi lub z instytucją.

KROK PO KROKU

Jak zainstalować i uruchomić aplikację mObywatel



Dzięki aplikacji **mObywatel** możesz mieć w telefonie m.in. mDowód, swoje dokumenty, sprawdzić informacje o PESEL i skorzystać z wielu usług publicznych.

1 Pobierz aplikację mObywatel

- Otwórz sklep z aplikacjami w swoim telefonie:
  - **Google Play** (Android)
  - **App Store** (iPhone)
- W wyszukiwarce wpisz: **mObywatel**
- Wybierz oficjalną aplikację z logo Orła i zainstaluj ją na swoim telefonie.



2 Otwórz aplikację

- Po zakończeniu instalacji kliknij **„Otwórz”**.
- Na ekranie powitalnym wybierz **„Rozpocznij”**.



3 Wybierz sposób logowania

- Aplikacja zaproponuje dwa sposoby logowania:
  - **Profil Zaufany** jeśli już go masz,
  - lub **bank/inni dostawcy** (np. bankowość elektroniczna), jeśli chcesz założyć Profil Zaufany podczas logowania.



4 Zaloguj się

- Jeśli wybierzesz Profil Zaufany – wpisz swój login i hasło.
- Jeśli wybierzesz bank – wybierz swój bank i postępuj zgodnie z instrukcjami na ekranie.
- Po poprawnym zalogowaniu zostaniesz przekierowany z powrotem do aplikacji mObywatel.



5 Ustal kod PIN

- Po pierwszym logowaniu aplikacja poprosi o ustalenie kodu PIN (najczęściej 6-cyfrowego).
- Ten kod będziesz później wpisywać przy każdym uruchomieniu aplikacji.
- Wpisz kod PIN, a następnie potwierdź go.



6 Włącz dodatkowe zabezpieczenia

- W ustawieniach aplikacji możesz włączyć dodatkowe zabezpieczenia, np.:
  - odblokowanie biometrią (odciskiem palca lub twarzą),
  - możliwość szybkiego logowania.



7 Gotowe! Korzystaj z mObywatela

- Po zakończeniu konfiguracji zobaczysz główny ekran aplikacji.
- Teraz możesz korzystać z dostępnych usług, m.in.:
  - **mDowód**,
  - **informacje o PESEL**,
  - inne dokumenty i usługi publiczne.



Pamiętaj!

- Pobieraj aplikację tylko z oficjalnych sklepów (Google Play lub App Store).
- Sprawdzaj, czy wydawcą aplikacji jest Ministerstwo Cyfryzacji.
- Nie udostępniaj swojego kodu PIN nikomu.
- Korzystaj z dodatkowych zabezpieczeń, np. odcisku palca lub rozpoznawania twarzy.
- Regularnie aktualizuj aplikację.

CYBERBEZPIECZEŃSTWO NA CO DZIEŃ

Jak zastrzec numer PESEL w aplikacji mObywatel?

Krok po kroku – prosta instrukcja

mObywatel

Zastrzeżenie PESEL utrudnia oszustom zaciągnięcie kredytu, zakup na raty lub założenie konta na Twoje dane.

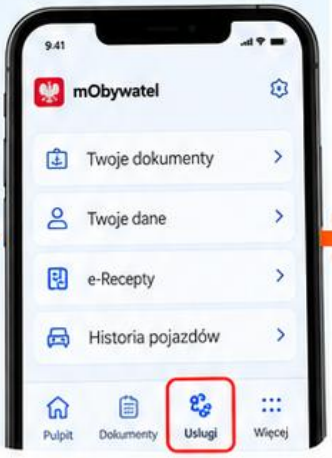
1 Zaloguj się do aplikacji mObywatel

Otwórz aplikację **mObywatel** i zaloguj się wybraną metodą (np. hasło, profil zaufany lub bank).



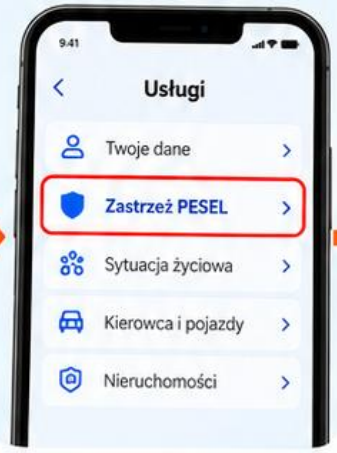
2 Przejdź do zakładki „Usługi"

Na dolnym pasku menu wybierz zakładkę **„Usługi"**.



3 Wybierz „Zastrzeż PESEL"

Na liście usług znajdź i wybierz pozycję **„Zastrzeż PESEL"**.



4 Zapoznaj się z informacją

Przeczytaj krótkie informacje o tym, co oznacza zastrzeżenie numeru PESEL i jak działa ta usługa. Następnie kliknij **„Dalej"**.



5 Zastrzeż swój PESEL

Kliknij przycisk **„Zastrzeż PESEL"**.



6 Potwierdź operację

Aplikacja poprosi Cię o potwierdzenie decyzji, np. kodem PIN, hasłem lub metodą logowania.



7 PESEL został zastrzeżony

Po potwierdzeniu zobaczysz komunikat, że Twój numer PESEL jest zastrzeżony.



8 Sprawdź status w każdej chwili

W usłudze „Zastrzeż PESEL" możesz zobaczyć aktualny status (zastrzeżony / niezastrzeżony), historię operacji oraz w razie potrzeby cofnąć zastrzeżenie.



Ważne!

- Zastrzeżenie PESEL jest bezpłatne.
- Możesz je w każdej chwili cofnąć w aplikacji mObywatel.
- Po cofnięciu zastrzeżenia numer PESEL znów będzie aktywny (np. do zaciągnięcia kredytu).
- Zastrzeżenie PESEL nie wpływa na korzystanie z usług publicznych (np. w przychodni, urzędzie, wyborach).
- Warto regularnie sprawdzać status PESEL w aplikacji.

Pamiętaj!

- Nie udostępniaj nikomu swoich danych do logowania do aplikacji mObywatel.
- Korzystaj z silnego hasła i – jeśli to możliwe – z uwierzytelniania dwuskładnikowego (2FA).
- Zastrzeżenie PESEL utrudnia oszustom wykorzystanie Twoich danych do wyłudzeń.

16. GDZIE SZUKAĆ POMOCY? – PRZYDATNE KONTAKTY I NARZĘDZIA

Nie jesteś sam – tutaj znajdziesz pomoc

Jeśli podejrzewasz oszustwo, padłeś ofiarą cyberprzestępstwa lub chcesz sprawdzić, czy Twoje dane lub hasła wyciekły do internetu – skorzystaj z poniższych kontaktów i narzędzi.

Działaj szybko!
Im szybciej zgłosisz problem i zabezpieczysz swoje konta, tym większa szansa na ograniczenie strat.

1 Skontaktuj się z bankiem



- Zadzwoń na numer infolinii swojego banku (z listy na stronie banku lub aplikacji).
- Poproś o zablokowanie dostępu do konta, karty i bankowości internetowej.
- Zapytaj o możliwość cofnięcia nieautoryzowanej płatności.

2 Zgłoś sprawę na policję



Policja 112 (w sytuacji zagrożenia) lub 997

- Zgłoś sprawę na najbliższym komisariacie.
- Zabierz wydruki lub zrzuty ekranu wiadomości, numeru telefonu, przelewów.
- Poproś o potwierdzenie zgłoszenia.

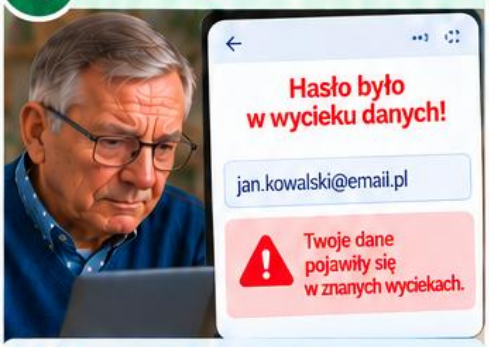
3 Zgłoś incydent online



CERT Polska https://incydent.cert.pl zgłoszenie podejrzanych wiadomości, stron internetowych i oszustw online.

- Możesz anonimowo zgłosić podejrzaną stronę, wiadomość e-mail, SMS lub oszustwo.
- CERT Polska analizuje zagrożenia i ostrzega innych użytkowników.

4 Sprawdź, czy Twoje dane wyciekły



Have I Been Pwned?
https://haveibeenpwned.com

Sprawdź, czy Twój adres e-mail lub numer telefonu pojawił się w znanych wyciekach danych z różnych serwisów.

5 Sprawdź, czy Twoje hasła wyciekły



Google – Sprawdzenie haseł
https://passwords.google.com

Jeśli używasz konta Google, sprawdź, czy Twoje zapisane hasła nie znalazły się w wyciekach danych.

6 Zastrzeż PESEL i sprawdź jego status



Aplikacja mObywatel
Zastrzeż swój numer PESEL, aby utrudnić oszustom zaciąganie kredytów na Twoje dane. Możesz też sprawdzić status zastrzeżenia.

Przydatne kontakty

gov.pl	www.gov.pl – oficjalny portal rządowy
Policja	112 (w sytuacji zagrożenia) 997
CERT Polska	https://incydent.cert.pl – zgłoszenie podejrzanych wiadomości
NASK	NASK – Dyżurnet.pl dyzurnet.pl – zgłaszanie nielegalnych treści w internecie
UOKiK	uokik.gov.pl – zgłaszanie nieuczciwych praktyk firm
KNF	www.knf.gov.pl – informacje dla konsumentów usług finansowych

Inne narzędzia do sprawdzania

HAVE I BEEN PWNED?	https://haveibeenpwned.com – sprawdź wycieki danych (adres e-mail, telefon)
Firefox Monitor	https://monitor.firefox.com – sprawdź, czy Twoje dane pojawiły się w wyciekach
Password Checkup	https://passwords.google.com – sprawdź swoje hasła (wymaga konta Google)
Czy mój PESEL jest bezpieczny?	https://www.gov.pl/web/numer-pesel – informacje o zastrzeżeniu PESEL i możliwościach jego ochrony

Co przygotować przy zgłoszeniu?

1. Zrzuty ekranu wiadomości, stron internetowych lub rozmów.
2. Numer telefonu nadawcy i adres e-mail.
3. Daty i godziny zdarzeń.
4. Potwierdzenia przelewów i inne dowody (np. faktury, ogłoszenia).
5. Opis sytuacji – co się wydarzyło i jakie dane zostały przekazane.

Pamiętaj!

- Zawsze sprawdzaj adres strony – wpisuj go samodzielnie.
- Nie podawaj danych przez linki z wiadomości.
- Używaj silnych i różnych haseł.
- Włącz dodatkowe zabezpieczenia (np. weryfikacja dwuetapowa).
- Regularnie sprawdzaj, czy Twoje dane nie wyciekły.

Moje notatki

Miejsce na ważne informacje, pomysły i własne zapiski

Ważne informacje

Do zrobienia

- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

Kontakty i numery

Wskazówki i pomysły

Inne notatki

Pamiętaj!

Zapisuj tu swoje pytania, pomysły i ważne informacje. Te notatki pomogą Ci wrócić do najważniejszych spraw po zakończeniu lektury poradnika.

Moje notatki

