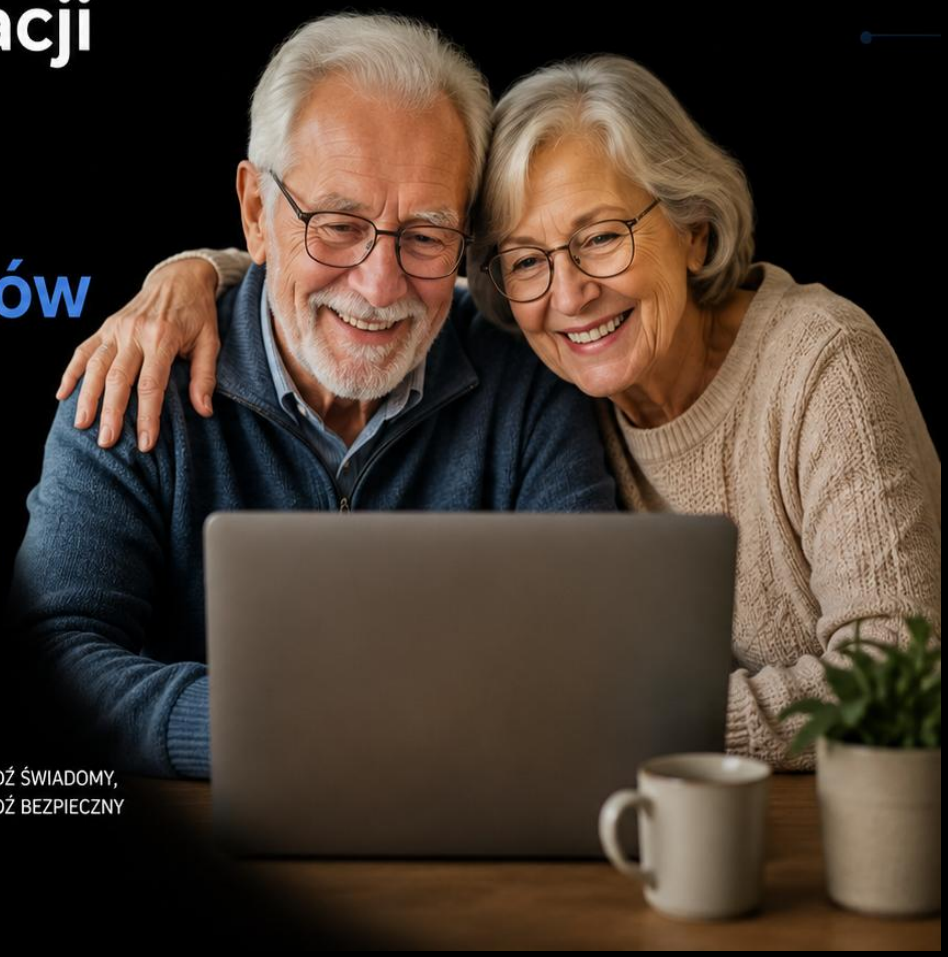
Przedstawienie informacji na temat cyberbezpieczeństwa i bezpieczeństwa seniorów w internecie

HASŁO:
JAK SIĘ NIE DAĆ OSZUSTWOM
W ŚWIECIE NOWYCH TECHNOLOGII



CHROŃ SWOJE DANE | NIE DAJ SIĘ OSZUKAĆ | DBAJ O SWOJE BEZPIECZEŃSTWO | BĄDŹ ŚWIADOMY, BĄDŹ BEZPIECZNY

Dlaczego ten temat jest ważny dla seniorów?

- Coraz więcej spraw załatwiamy **online**
- Seniorzy są **częstym celem oszustów**
- Oszuści wykorzystują **emocje i pośpiech**

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści nie łamią drzwi – oni zdobywają Twoje zaufanie.

Działają według schematu: EMOCJE → PRESJA → BŁĄD → STRATA PIENIĘDZY

PAMIĘTAJ!
Przestępcy są świetnymi psychologami. Wykorzystują Twoje emocje, zaufanie i pośpiech. Ich cel jest jeden – Twoje pieniądze.

1. EMOCJE

Budzą silne uczucia, aby przejąć nad Tobą kontrolę.

- Strach: „Twoje konto zostanie zablokowane."
- Nadzieja: „Wygrałeś dużą kwotę!"
- Zaufanie: „Jestem z banku/policji/prokuratury."
- Współczucie: „Pomóż mi, jestem w trudnej sytuacji."

2. PRESJA

Nie dają czasu na zastanowienie.

- Działają szybko, wprowadzają pośpiech.
- Dzwonią, piszą, nalegają.
- Grożą konsekwencjami: „Jeśli nie zrobisz teraz, stracisz pieniądze/zostaniesz ukarany."

3. BŁĄD

W chwili słabości podejmujesz złą decyzję.

- Klikasz w link.
- Podajesz dane logowania, kody BLIK, PIN, PESEL.
- Wykonujesz przelew „na bezpieczne konto".
- Umożliwiasz zdalny dostęp do swojego komputera.

4. STRATA PIENIĘDZY

Pieniądze znikają w kilka minut.

Odzyskanie pieniędzy jest bardzo trudne lub niemożliwe.

CO ZROBIĆ, ABY SIĘ NIE DAĆ?

ZATRZYMAJ SIĘ
Nie działaj pod wpływem emocji i presji. Weź głęboki oddech, policz do 10.

SPRAWDŹ
Zweryfikuj informacje w oficjalnych źródłach. Zadzwoń do banku domyślnie – użyj numeru z oficjalnej strony.

SKONSULTUJ
Porozmawiaj z kimś bliskim. Druga osoba pomoże spojrzeć trzeźwo na sytuację.

NIE UDOSTĘPNIAJ
Nikomu nie podawaj kodów, loginów, PIN-ów, danych dowodu osobistego ani dostępu do komputera.

BĄDŹ CZUJNY
Instytucje nigdy nie proszą o pieniądze, kody BLIK ani zdalny dostęp do Twoich urządzeń.

ZGŁOŚ PODEJRZANE SYTUACJE
Zgłoś na Policję (112) lub na infolinię swojego banku. Twoje zgłoszenie może uchronić innych.

TWOJE BEZPIECZEŃSTWO JEST NAJWAŻNIEJSZE!
Świadomy senior to bezpieczny senior.

Nie jesteś sam!
Pytaj, sprawdzaj, nie działaj pochopnie.

WAŻNE NUMERY

- Policja: 112
- Infolinia dla Seniorów: 22 505 11 11 (czynna 7 dni w tyg. 8:00–20:00)
- CERT Polska (incydenty w internecie): 8080 (bezpłatnie)

OSZUSTWO NA WNUCZKA

Nie daj się oszukać – chroń siebie i swoich bliskich!

PAMIĘTAJ!
Policja, prokuratura ani żaden urzędnik **NIGDY** nie proszą o pieniądze przez telefon!

JAK DZIAŁA OSZUST?

Podszywa się pod rodzinę
Dzwoni i udaje wnuczka, dziecka lub innego bliskiego – zna Twoje dane i wzbudza zaufanie.

Tworzy presję czasu
Mówi o nagłej sytuacji: wypadek, zatrzymanie przez policję, pilna operacja – potrzebuje pieniędzy „już teraz".

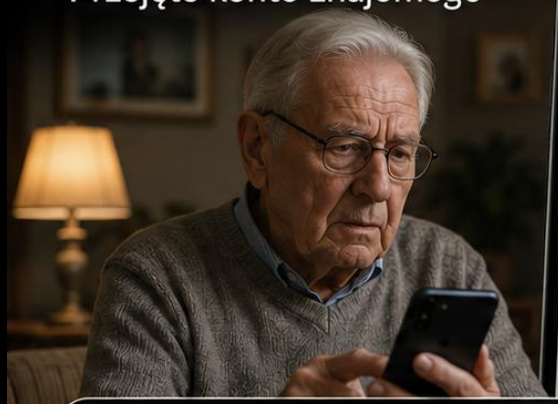
Prosi o pieniądze
Prosi o gotówkę, przelew lub przekazanie pieniędzy nieznanej osobie (np. kurierowi, znajomemu).

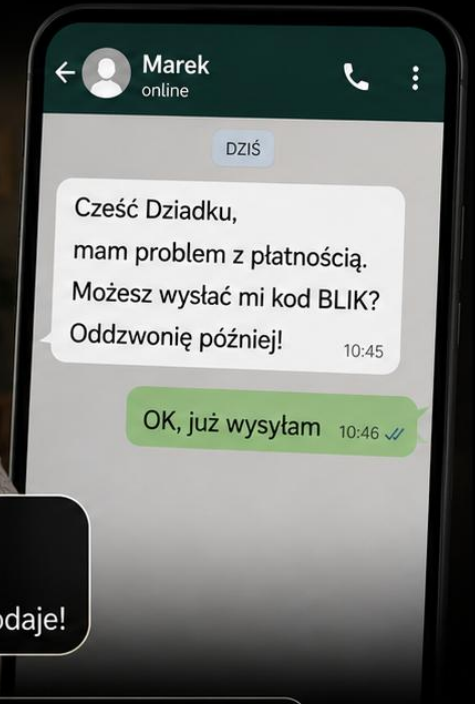
CO MOŻESZ ZROBIĆ?

- **Zachowaj spokój** – nie działaj pod presją.
- Zawsze **oddzwoń** do bliskiego na znany Ci numer telefonu i sprawdź, czy wszystko w porządku.
- **Nie przekazuj pieniędzy** nieznanym osobom, nie wykonuj przelewów pod wpływem emocji.

OSZUSTWO NA BLIK

Przejęte konto znajomego





PAMIĘTAJ!
Nie każdy, kto pisze,
jest tym, za kogo się podaje!

Zasada nr 1:
Zawsze weryfikuj telefonicznie!

JAK DZIAŁA OSZUST?

Przejmuje konto znajomego
Oszust włamuje się na konto w mediach społecznościowych lub komunikatorze.

Wysyła wiadomość
Pisze z prośbą o kod BLIK, tłumacząc się pilną sytuacją (np. problem z płatnością, zakup, zwrot pieniędzy).

Wyłudza pieniądze
Dzięki kodowi BLIK wypłaca pieniądze z Twojego konta.

CO ZROBIĆ W TAKIM PRZYPADKU?

- **Nie wysyłaj** kodu BLIK nikomu!
- **Zadzwoń do znajomego** i upewnij się, że to on naprawdę prosi o pomoc.
- **Zgłoś sprawę** swojemu bankowi i zmień hasło do konta.

PAMIĘTAJ!
Oszust wykorzystuje zaufanie – **nie daj się oszukać!**

OSZUSTWO NA ZNAJOMOŚĆ!

Oszuści budują relację, zdobywają zaufanie i proszą o pieniądze.
Nie daj się zwieść emocjom – chroń swoje serce i swoje pieniądze!

JAK SIĘ BRONIĆ PRZED OSZUSTAMI?

WERYFIKUJ TOŻSAMOŚĆ
Sprawdź profil, zdjęcia i informacje.
Szukaj w wyszukiwarce grafiki (Google Lens).
Prawdziwi ludzie mają historię i ślady w sieci.

NIE UFAJ ZBYT SZYBKO
Oszuści szybko okazują uczucia i mówią o miłości, ale jeszcze Cię nie znają.

NIE WYSYŁAJ PIENIĘDZY
To najczęstszy cel oszustów. Zawsze znajdą „pilny powód" – bilet, operacja, długi, inwestycja.

ROZZMAWIAJ Z BLISKIMI
Zanim podejmiesz decyzję, porozmawiaj z kimś z rodziny lub zaufaną osobą.

ZGŁASZAJ PODEJRZANE SYTUACJE
Zgłoś oszustwo na Policję (112 lub 997) lub do administratora portalu.

PAMIĘTAJ!
Oszuści grają na Twoich emocjach, pragnieniu bliskości i pomocy.
Nie działaj pod wpływem uczuć – działaj z rozwagą!

NIE KAŻDY W INTERNECIE JEST TYM, ZA KOGO SIĘ PODAJE.
Zachowaj ostrożność i chroń swoje dane oraz pieniądze.

GDZIE SZUKAĆ POMOCY?

- Policja – 112 lub 997
- Infolinia dla Seniorów – 22 505 11 11 (czynna 7 dni w tyg. 8:00–20:00)
- CERT Polska – 8080 (bezpłatna infolinia)

FAŁSZYWY ZUS LUB URZĄD SKARBOWY
NIE DAJ SIĘ OSZUKAĆ!

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

JAK DZIAŁAJĄ OSZUŚCI?

PODSZYWAJĄ SIĘ
Podają się za pracownika ZUS lub Urzędu Skarbowego.

WYSYŁAJĄ FAŁSZYWE WIADOMOŚCI
E-maile lub SMS-y z informacją o zaległościach, zwrocie podatku lub konieczności dopłaty.

CHCĄ WYŁUDZIĆ DANE LUB PIENIĄDZE
Proszą o kliknięcie w link, otwarcie załącznika lub podanie danych logowania i danych karty.

PODEJRZANE E-MAILE – NA CO UWAŻAĆ?

- Naciskają na Ciebie – grożą karą, zajęciem konta, wezwaniem do zapłaty.
- Zawierają linki – prowadzą do fałszywych stron łudząco podobnych do prawdziwych.
- Fałszywe załączniki – mogą zawierać wirusy lub kraść Twoje dane.
- Podejrzany nadawca – dziwny adres e-mail, literówki, brak oficjalnej domeny.
- Nieproszone wiadomości – nie odpowiadaj na nie i nie klikaj w nic.

CO ZROBIĆ, GDY DOSTANIESZ TAKĄ WIADOMOŚĆ?

ZATRZYMAJ SIĘ
Nie działaj pod wpływem emocji i presji.

SPRAWDŹ
Nie klikaj w linki ani nie otwieraj załączników.

ZWERYFIKUJ
Skontaktuj się z instytucją oficjalnym numerem telefonu (z oficjalnej strony).

USUŃ
Usuń wiadomość i nie odpowiadaj na nią.

CHROŃ SWOJE DANE
Nigdy nie podawaj danych logowania, numeru PESEL, danych karty ani kodów SMS.

JAK ROZPOZNAĆ FAŁSZYWE INFORMACJE?

- Sprawdź adres e-mail nadawcy – czy to oficjalna domena np. @zus.pl lub @mf.gov.pl?
- Zwróć uwagę na błędy językowe i literówki.
- Prawdziwe instytucje nie proszą o dane przez e-mail lub SMS.
- Wejdź na oficjalną stronę ZUS lub Urzędu Skarbowego ręcznie – nie przez link.
- W razie wątpliwości zapytaj bliską osobę.

PAMIĘTAJ!
Twoje dane są cenne. Chroń je tak, jak swoje oszczędności.

WAŻNE NUMERY
- ZUS: 22 560 16 00
- Urząd Skarbowy – infolinia KAS: 22 330 03 30

BEZPIECZNY SENIOR = SPOKOJNY SENIOR
Bądź czujny i nie daj się oszukać!

OSZUSTWO NA PRACOWNIKA BANKU

Oszuści podszywają się pod pracowników banku,
aby ukraść Twoje dane i pieniądze.

Nie daj się oszukać – bądź czujny i świadomy!

NA CO UWAŻAĆ?

KONTO ZAGROŻONE
Dostajesz informację, że Twoje konto jest zagrożone lub ktoś próbuje się na nie włamać.

FAŁSZYWY KONSULTANT
Dzwoni lub pisze rzekomy pracownik banku. Brzmi profesjonalnie i wzbudza zaufanie.

BANK NIE PROSI O HASŁA!
Proszą o kod BLIK, dane do logowania, hasła, instalację aplikacji lub przelanie pieniędzy na „bezpieczne konto".

JAK SIĘ CHRONIĆ?

BANK NIGDY NIE PROSI O:
hasła, kodów BLIK, kodów SMS, danych do logowania ani instalacji aplikacji.

ROZŁĄCZ SIĘ I ZADZWOŃ DO BANKU
Jeśli masz wątpliwości – rozłącz się i zadzwoń na oficjalny numer banku z jego strony internetowej.

NIE KLIKAJ W LINKI
Nie otwieraj linków i załączników w wiadomościach e-mail i SMS, nawet jeśli wyglądają wiarygodnie.

NIE DZIAŁAJ POD PRESJĄ
Oszuści wywołują stres i pośpiech, abyś nie zdążył się zastanowić. Zatrzymaj się i sprawdź!

CHROŃ SWOJE DANE
Nie udostępniaj nikomu swoich danych osobowych, numerów kart, kodów i haseł.

CO ZROBIĆ, GDY PODEJRZEWASZ OSZUSTWO?

1. **ZATRZYMAJ SIĘ** – Nie działaj pochopnie. Weź głęboki oddech.
2. **ZWERYFIKUJ** – Skontaktuj się z bankiem korzystając z oficjalnego numeru telefonu.
3. **NIE PODAWAJ DANYCH** – Nie podawaj haseł, kodów, danych kart ani kodów BLIK nikomu – nigdy!
4. **POROZMAWIAJ Z BLISKIMI** – Skonsultuj się z kimś z rodziny lub zaufaną osobą.
5. **ZGŁOŚ OSZUSTWO** – Zgłoś sprawę w banku oraz na Policji (112 lub 997).

WAŻNE NUMERY

- **POLICJA:** 112 lub 997
- **INFOLINIA DLA SENIORÓW:** 22 505 11 11 (czynna 7 dni w tyg. 8:00–20:00)
- **CERT POLSKA** (incydenty w internecie): 8080 (bezpłatnie infolinia)

PAMIĘTAJ!

Bank dba o Twoje bezpieczeństwo, ale Ty musisz dbać o swoje dane!

Twoje pieniądze są cenne. Nie ryzykuj!

Zaufanie jest dobre, ale ostrożność – jeszcze lepsza!

Bezpieczny senior = spokojny senior. Bądź czujny!

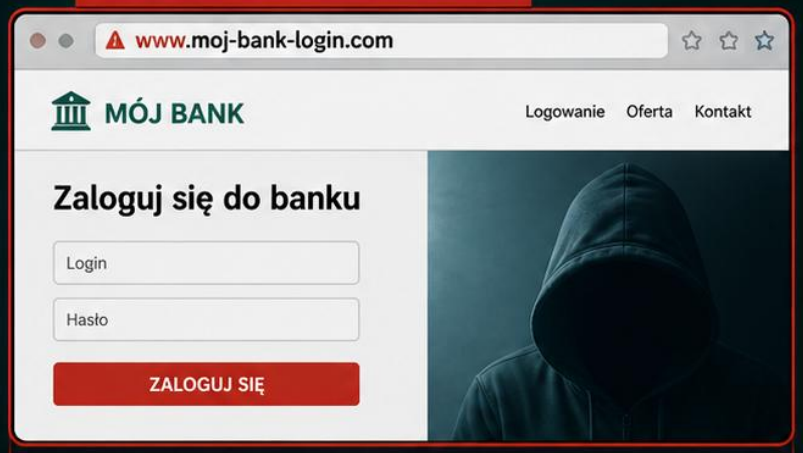
NIE DAJ SIĘ OSZUKAĆ!

Świadomość to najlepsza ochrona.

NIE DAJ SIĘ OSZUKAĆ – SPRAWDŹ STRONĘ WWW

Porównanie fałszywej i prawdziwej strony banku

FAŁSZYWA STRONA



- **Podejrzany adres strony**
  Adres nie pasuje do oficjalnej strony banku.
- **Brak kłódki lub niebezpieczne połączenie**
  Strona może nie mieć certyfikatu SSL (brak kłódki) lub używać http zamiast https.
- **Błędy językowe i stylistyczne**
  Literówki, dziwne sformułowania, nieprofesjonalny wygląd.
- **Nietypowy wygląd strony**
  Strona może wyglądać inaczej niż zwykle, mieć inne logo lub układ.
- **Prośba o dane wrażliwe**
  Bank nigdy nie prosi o podanie loginu, hasła ani kodów w emailu lub przez formularz.
- **Brak danych kontaktowych lub fałszywe dane**
  Brak adresu, telefonu lub podane dane są nieprawdziwe.

PRAWDZIWA STRONA

- **Poprawny adres strony**
  Adres strony zgadza się z oficjalną domeną banku.
- **Bezpieczne połączenie (https)**
  Widoczna kłódka i adres zaczynający się od https.
- **Profesjonalny wygląd i poprawny język**
  Brak błędów, strona wygląda spójnie i profesjonalnie.
- **Znane elementy strony**
  Układ, logo i grafiki są zgodne z oficjalną stroną banku.
- **Brak próśb o dane wrażliwe**
  Bank nie prosi o login, hasło ani kody przez stronę lub email.
- **Dane kontaktowe są dostępne**
  Adres, telefon i inne dane kontaktowe są podane i prawdziwe.

PAMIĘTAJ!

- **Nie klikaj w linki** w wiadomościach e-mail od nieznanych nadawców.
- **Zawsze wpisuj adres** strony banku ręcznie w przeglądarkę.
- **W razie wątpliwości** skontaktuj się z bankiem korzystając z oficjalnych numerów.
- **Nie podawaj nikomu** swoich danych logowania ani kodów.

DEEP FAKE – NIE DAJ SIĘ OSZUKAĆ!

Przestępcy mogą wykorzystywać wizerunek i głos znanych osób, aby nakłonić Cię do inwestycji i wyłudzić Twoje pieniądze.

PRZYKŁAD: FAŁSZYWY FILM LUB REKLAMA

Pamiętaj: **To może być oszustwo!**
Nie każda rekomendacja znanej osoby jest prawdziwa.

JAK ROZPOZNAĆ DEEP FAKE?

Nienaturalny wygląd twarzy
Sztywna mimika, rzadkie mruganie, nienaturalne ruchy ust lub twarzy.

Nienaturalny głos
Monotonny, robotyczny, bez emocji lub z dziwnymi przerwami.

Podejrzana treść
Obietnice szybkiego zysku, brak ryzyka, presja czasu, „tylko dziś", „nie przegap".

Nieznane linki i źródła
Klikanie w podejrzane linki może prowadzić do stron oszustów.

Sprawdź w innych źródłach
Poszukaj informacji w oficjalnych kanałach danej osoby lub instytucji.

CO ZROBIĆ?

Zachowaj ostrożność
Nie powierzaj pieniędzy na podstawie nagrań lub reklam z internetu.

Zweryfikuj informacje
Skontaktuj się bezpośrednio z firmą lub osobą, której wizerunek został użyty.

Nie klikaj, nie wpłacaj
Nie klikaj w linki i nie dokonuj przelewów, jeśli coś budzi Twoje wątpliwości.

Porozmawiaj z bliskimi
Skonsultuj podejrzane treści z rodziną lub zaufaną osobą.

PAMIĘTAJ!
Przestępcy wykorzystują nowe technologie, ale Twoja czujność jest najlepszą ochroną.

ZASADY BEZPIECZEŃSTWA SENIORA

Chron swoje dane
Nie udostępniaj danych osobowych ani danych do logowania.

Korzystaj z oficjalnych źródeł
Loguj się do banku tylko przez znaną stronę lub aplikację.

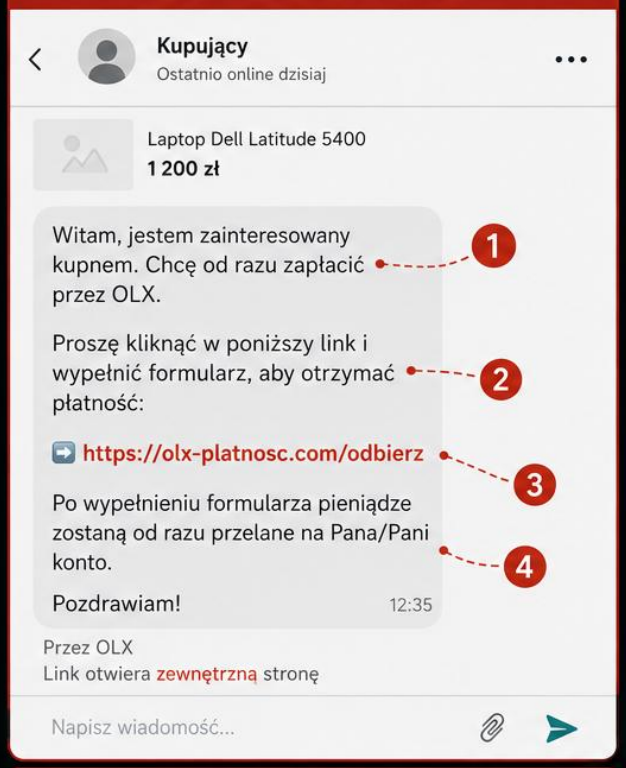
Bądź czujny wobec promocji
Jeśli oferta wydaje się zbyt dobra, by była prawdziwa – prawdopodobnie jest fałszywa.

W razie wątpliwości – zadzwoń
Skontaktuj się z bankiem lub infolinią i zapytaj o podejrzaną sytuację.

FAŁSZYWA WIADOMOŚĆ OLX – JAK JĄ ROZPOZNAĆ?

Uważaj na oszustów! Sprawdź, zanim klikniesz.

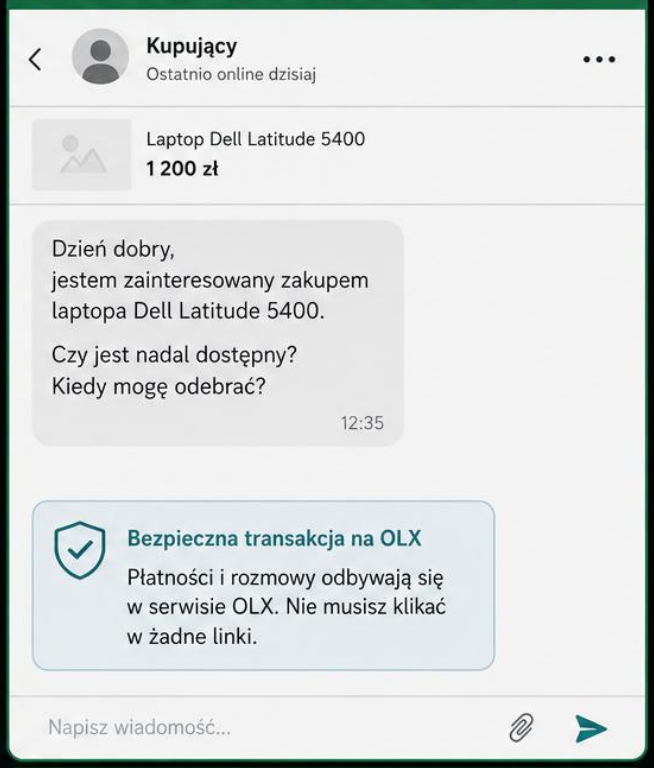
FAŁSZYWA WIADOMOŚĆ



JAK ROZPOZNAĆ FAŁSZ?

1. **PODEJRZANE LINKI**
   Fałszywe wiadomości zawierają linki do stron, które nie są domeną OLX (np. olx-platnosc.com).
2. **PRESJA CZASU I SZYBKOŚĆ**
   Oszust chce, abyś działał szybko i nie miał czasu na zastanowienie.
3. **OGÓLNE POWITANIA**
   Brak Twojego imienia, ogólne sformułowania (np. „Witam").
4. **POZA SERWISEM OLX**
   Prawdziwe płatności i rozmowy odbywają się tylko na OLX. Nie ma potrzeby klikania w linki.
5. **BŁĘDY JĘZYKOWE**
   Często występują literówki, dziwne sformułowania lub brak polskich znaków.

PRAWDZIWA WIADOMOŚĆ OLX



NIE KLIKAJ W LINKI I NIE PODAWAJ DANYCH!
OLX nigdy nie prosi o płatności poza serwisem ani nie wysyła linków do formularzy.

PAMIĘTAJ!
W razie wątpliwości skontaktuj się z pomocą OLX lub zaufaną osobą.

BEZPIECZNIE!
Prawdziwa wiadomość jest krótka, konkretna i nie zawiera linków do zewnętrznych stron.

ZASADY BEZPIECZEŃSTWA NA OLX

- Korzystaj z Bezpiecznych Płatności OLX.
- Nie klikaj w linki przesyłane przez innych użytkowników.
- Nie podawaj danych osobowych, danych karty ani kodów.
- W razie wątpliwości – nie podejmuj działania.

CHROŃ SWOJE DANE W INTERNECIE

PROSTE ZASADY DLA KAŻDEGO SENIORA

Twoje dane są cenne – chroń je tak, jak swoje oszczędności i dokumenty.

10 ZASAD OCHRONY TWOICH DANYCH

1 CHROŃ SWÓJ PESEL

Nie podawaj numeru PESEL przez telefon, e-mail ani w formularzach internetowych, chyba że masz pewność, komu go udostępniasz.

2 UŻYWAJ SILNYCH HASEŁ

Twórz hasła z liter, cyfr i znaków specjalnych. Nie używaj łatwych haseł jak „123456" czy „hasło". Nie używaj tego samego hasła do różnych kont.

3 WŁĄCZ WERYFIKACJĘ DWUETAPOWĄ

Jeśli to możliwe, włącz dodatkową ochronę konta (kod SMS lub aplikacja uwierzytelniająca). To skutecznie chroni Twoje konto.

4 UWAŻAJ NA WIADOMOŚCI

Nie klikaj w linki i nie otwieraj załączników w wiadomościach od nieznanych nadawców. To może być próba oszustwa (np. wyłudzenia danych lub pieniędzy).

5 KORZYSTAJ TYLKO ZE SPRAWDZONYCH STRON

Sprawdzaj adres stron (czy zaczyna się od https://) i unikaj podejrzanych witryn. Nie podawaj danych na stronach, których nie znasz.

6 UWAŻAJ W PUBLICZNYCH SIECIACH WI-FI

Nie loguj się do banku i nie podawaj wrażliwych danych w otwartych sieciach Wi-Fi, np. w kawiarniach czy na dworcach.

7 AKTUALIZUJ SYSTEM I APLIKACJE

Aktualizacje poprawiają bezpieczeństwo. Włącz automatyczne aktualizacje, jeśli to możliwe.

8 OGRANICZ UDOSTĘPNIANIE DANYCH O SOBIE

Nie udostępniaj w internecie informacji o swoim wieku, adresie, numerze telefonu, stanie majątkowym czy planach podróży.

9 ZABEZPIECZ DOKUMENTY

Nie wysyłaj zdjęć dokumentów tożsamości (dowód osobisty, paszport) osobom, którym nie ufasz.

10 KORZYSTAJ Z ZAUFANYCH ŹRÓDEŁ

Załatwiaj sprawy online tylko na stronach urzędów, banków i znanych firm. Nie korzystaj z podejrzanych ofert, które wydają się „zbyt dobre, by być prawdziwe".

PAMIĘTAJ!

- Banki i urzędy NIGDY nie proszą o podanie danych osobowych przez telefon ani e-mail.
- Jeśli masz wątpliwości – zapytaj bliską osobę.
- Lepiej zapobiegać niż żałować – dbaj o swoje dane tak, jak o swoje oszczędności.

BEZPIECZEŃSTWO ZACZYNA SIĘ OD CIEBIE

Stosując te proste zasady, chronisz siebie i swoje pieniądze przed oszustami. W razie wątpliwości – skonsultuj się z rodziną lub zadzwoń do banku.

BĄDŹ CZUJNY

Zawsze sprawdzaj i nie działaj pochopnie.

ZADZWOŃ I ZAPYTAJ

W razie wątpliwości skontaktuj się z bankiem lub zaufaną osobą.

CHROŃ SWOJE DANE

Twoje dane to klucz do Twojego bezpieczeństwa.

DBAJ O SIEBIE

Bezpieczny senior to spokojny senior.

GDZIE ZGŁASZAĆ OSZUSTWA
I W JAKI SPOSÓB?

Reaguj – Twoje zgłoszenie może uchronić Ciebie i innych przed stratą.

GDZIE MOŻESZ ZGŁOSIĆ OSZUSTWO?

1. NA POLICJĘ

Zgłoś oszustwo osobiście w najbliższej jednostce Policji lub telefonicznie – 112 w nagłych wypadkach.

POLICJA 112

2. DO BANKU

Jeśli padłeś ofiarą oszustwa finansowego (np. przelew na fałszywe konto) – jak najszybciej skontaktuj się ze swoim bankiem.

INFOLINIA BANKU

3. DO CERT POLSKA

Zgłoś podejrzane strony internetowe, fałszywe sklepy, oszustwa w internecie.

www.incydent.cert.pl

4. DO UOKiK

Zgłoś nieuczciwe praktyki firm, fałszywe sklepy internetowe, oszustwa przy zakupach.

www.inokik.gov.pl

5. NA OLX I INNE PORTALE

Użyj formularza „Zgłoś naruszenie" dostępnego na stronie danego portalu (np. OLX, Vinted itp.).

POMOC OLX

JAK ZGŁOSIĆ? – KROK PO KROKU

1. Opisz sytuację – co się stało, kiedy i w jaki sposób.
2. Podaj wszystkie znane informacje – stronę www, numer telefonu, e-mail, nick, numer konta (jeśli dotyczy).
3. Dołącz dowody – zrzuty ekranu, wiadomości, e-maile, potwierdzenia przelewów.
4. Przekaż zgłoszenie odpowiedniej instytucji.
5. Zachowaj potwierdzenie zgłoszenia – może być potrzebne w przyszłości.

DLACZEGO WARTO ZGŁASZAĆ?

- Pomagasz chronić siebie i innych przed oszustwami.
- Twoje zgłoszenie pomaga służbom szybciej reagować i zatrzymywać oszustów.
- Zwiększasz bezpieczeństwo w internecie.

PAMIĘTAJ!

- Nigdy nie jest za późno na zgłoszenie – nawet jeśli strata już się wydarzyła.
- Nie wstydź się zgłaszać – oszuści są coraz bardziej podstępni, każdy może paść ofiarą.
- Nie odpowiadaj na podejrzane wiadomości po zgłoszeniu – odetnij kontakt z oszustem.

PRZYDATNE NUMERY

- Policja (w razie zagrożenia) – 112
- Infolinia dla Seniorów – 22 505 11 11 (czynna 7 dni w tygodniu 8:00–20:00)
- CERT Polska – 8080 (bezpłatna infolinia bezpieczeństwa)

3 PROSTE ZASADY BEZPIECZEŃSTWA W INTERNECIE

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

Kilka sekund ostrożności może uchronić Ciebie i Twoje dane przed oszustwem.

1 ZATRZYMAJ SIĘ

Zanim klikniesz, pomyśl!

- Nie działaj pod presją czasu.
- Uważaj na podejrzane wiadomości, linki i oferty „zbyt piękne, by były prawdziwe".
- Chroń swoje dane – nie podawaj ich nikomu, kto o nie prosi.

2 SPRAWDŹ

Upewnij się, że to bezpieczne.

- Sprawdź adres strony – czy zaczyna się od https:// i ma kłódkę.
- Zweryfikuj nadawcę wiadomości lub oferty.
- W razie wątpliwości – zapytaj bliską osobę.

3 DZIAŁAJ

Bezpiecznie i świadomie.

- Korzystaj z zaufanych stron i aplikacji.
- Zgłaszaj podejrzane sytuacje odpowiednim instytucjom.
- Dbaj o aktualizacje systemu i programów.

PAMIĘTAJ!

- Twoje dane są cenne. Chroń je każdego dnia.
- W razie wątpliwości zapytaj rodzinę lub znajomych.
- Bezpieczeństwo w internecie zaczyna się od Ciebie!

BĄDŹ OSTROŻNY. BĄDŹ ŚWIADOMY. BĄDŹ BEZPIECZNY. KAŻDEGO DNIA.