Bezpieczne zakupy w internecie

Interaktywna checklista zakupowa dla seniorów — krok po kroku

Jak korzystać z tej checklisty?

1. Otwórz plik w programie do czytania PDF (np. Adobe Reader) i klikaj pola wyboru — możesz też wydrukować checklistę i odhaczać punkty długopisem.
2. Przechodź przez kroki w kolejności: od weryfikacji ceny aż do odbioru paczki.
3. Jeśli w którymkolwiek punkcie pojawi się „STOP" — przerwij zakupy i poproś o pomoc osobę, której ufasz. Uczciwy sklep nie znika z dnia na dzień.

Zakup, który sprawdzam:

Adres sklepu (np. www.sklep.pl): _____

Data zakupu: _____ Kwota (zł): _____

1 Czy to naprawdę okazja?

Zanim klikniesz „kupuję" — sprawdź cenę i pełny koszt zakupu

- ☐ Cena: Porównałem/am cenę w co najmniej 3 innych sklepach, które znam lub które sprawdziłem/am.
- ☐ Cena nie jest podejrzanie niska — nie jest o połowę niższa niż w innych sklepach. Skrajnie niska cena to najczęstsza przynęta fałszywych sklepów.
- ☐ Sprawdziłem/am, ile produkt kosztował przed wyprzedażą. Sklep ma obowiązek podać najniższą cenę z 30 dni przed obniżką.
- ☐ Znam pełny koszt zakupu: cena + dostawa + VAT — bez ukrytych opłat doliczanych dopiero przy płatności.
- ☐ Nie podejmuję decyzji pod presją: liczniki „tylko dziś", wyskakujące okienka i reklamy w mediach społecznościowych to częsta manipulacja.
- ☐ Znalazłem/am sklep samodzielnie (np. wpisując adres w przeglądarce), a nie tylko przez reklamę na Facebooku czy Instagramie.

ZŁOTA ZASADA

Prawdziwa okazja poczeka jeden dzień. Jeśli ktoś wywiera na Tobie presję czasu — to sygnał ostrzegawczy, nie okazja.

1. CERT Polska, „Bezpieczne zakupy w internecie" cert.pl/falszywe-sklepy/
2. UOKiK, „Zakupy wysokiego ryzyka" uokik.gov.pl/zakupy-wysokiego-ryzyka-falszywe-sklepy-udawane-polskie-marki-nieuc...

2 Czy sklep jest legalny?

Sprawdź, od kogo naprawdę kupujesz — wolno Ci o to dopytać sklep

- [ ] Dane firmy: Sklep publikuje pełne dane firmy: nazwa, adres siedziby, NIP lub KRS, e-mail i numer telefonu.
- [ ] Sprawdziłem/am firmę bezpłatnie w rejestrach państwowych: CEIDG (firma jednoosobowa) lub KRS (spółka) — dane zgadzają się z tymi na stronie.
- [ ] Sprawdziłem/am status NIP na stronie podatki.gov.pl — numer jest ważny i aktywny.
- [ ] Regulamin, polityka zwrotów i dane sprzedawcy są czytelne. Sklep musi podać te informacje jeszcze przed złożeniem zamówienia.
- [ ] Sklep ma numer telefonu — i udało mi się z nim skontaktować. Brak telefonu powinien wzbudzić wątpliwości.
- [ ] Adres strony wygląda poprawnie: jest kłódka (https), nazwa nie zawiera literówki znanej marki, nie ma dziwnych końcówek typu .xyz, .top, .lol.
- [ ] Opinie o sklepie znalazłem/am w niezależnych źródłach (wyszukiwarka, fora) — nie tylko na stronie sklepu, bo tam właściciel decyduje, co publikuje.
- [ ] Wiem, na jaki adres odesłałbym towar przy zwrocie — i nie jest to odległy kraj azjatycki bez wyjaśnienia.

PROSTA METODA

Nazwę firmy i NIP ze sklepu wklej do wyszukiwarki razem ze słowem „opinie” lub „oszustwo”. Kilka minut czytania może uratować Twoje pieniądze.

3. CERT Polska, „Poradnik zakupowy” cert.pl/uploads/docs/CERT_poradnik_zakupowy.pdf
4. UOKiK — Prawa konsumenta, obowiązki informacyjne sklepu prawakonsumenta.uokik.gov.pl/pytania-i-odpowiedzi/obowiaz...
5. Wyszukiwarka CEIDG aplikacja.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx
6. Sprawdź status NIP — podatki.gov.pl sprawdznip.podatki.gov.pl/
7. Ministerstwo Cyfryzacji i NASK — fałszywe sklepy gov.pl/web/cyfryzacja/uwaga-na-falszywe-sklepy-online--ostrzega-mi...

3 Bezpieczna płatność

Wybierz metodę, która Cię chroni — i nikomu nie podawaj kodów

- ☐ Metoda płatności: Wybieram bezpieczne metody płatności: BLIK, karta płatnicza, płatność za pobraniem albo przez platformę zakupową (np. serwis z ochroną kupującego).
- ☐ Nie płacę zwykłym przelewem na prywatne konto osoby, którą poznałem/am tylko przez internet — taki przelew nie daje żadnej ochrony.
- ☐ Nigdy nikomu nie podaję kodów z SMS-ów, kodów BLIK, pełnego numeru karty, kodu CVV ani PESEL — ani „bankowi", ani „policji", ani „kurierowi".
- ☐ Sprawdziłem/am w aplikacji banku kwotę, tytuł i dane odbiorcy — zanim zatwierdziłem/am płatność.
- ☐ Płacę tylko na stronie sklepu lub w aplikacji banku — nie klikam w linki do płatności przesłane SMS-em ani e-mailem.
- ☐ Jeśli płacę kartą — mam włączoną weryfikację 3-D Secure (kod SMS lub powiadomienie push od banku).

NAJWAŻNIEJSZE OSTRZEŻENIE

Żaden bank, policja ani kurier nigdy nie poprosi Cię o kod BLIK, kod z SMS-a ani hasło. Jeśli o to proszą — to na pewno oszuści. Odkładaj słuchawkę.

8. CERT Polska — bezpieczne metody płatności cert.pl/falszywe-sklepy/
9. Policja — ostrzeżenie przed fałszywymi SMS-ami podkarpacka.policja.gov.pl/rze/aktualnosci/151554,Policja-ostrzega-przed...

4 Czerwone flagi oszustów

Zaznaczoną choć jedną „czerwoną flagę"? STOP — rezygnuj z zakupu

UWAGA — TO NAJCZĘSTSZE PUŁAPKI

Każdy punkt poniżej to znany schemat oszustwa. Jeśli rozpoznajesz sytuację ze swojej transakcji — zaznacz „STOP", przerwij zakupy i poproś o pomoc osobę, której ufasz.

- ☐ STOP, gdy: SMS o dopłacie do paczki — nawet 1 zł lub 50 gr. Kurierzy i Poczta Polska nie wysyłają SMS-ów z linkami do opłat.
- ☐ Presja czasu: „ostatnia sztuka", „promocja kończy się za 5 minut", „zostało 2 sztuki".
- ☐ Sprzedawca z portalu ogłoszeniowego chce płatności poza platformą — prosi o przelew na prywatne konto.
- ☐ „Bank" albo „policja" dzwoni i prosi o pieniądze, dane lub kody — to zawsze oszuści.
- ☐ Sklep przyjmuje wyłącznie kartę lub szybki przelew — nie ma opcji płatności za pobraniem.
- ☐ Znaczki „Bezpieczne zakupy", „Sprawdzony sklep", „Gwarancja zwrotu pieniędzy" — to tylko grafiki, łatwe do skopiowania.
- ☐ Na stronie są duże błędy językowe, nielogiczne zdania i treści skopiowane z innych sklepów.
- ☐ „Syn" albo „córa" pisze z nowego numeru telefonu i prosi o pilny przelew pieniędzy.

10. Policja — metoda „na paczkę" malopolska.policja.gov.pl/krk/aktualnosci/aktualnosci/53465,Metoda-na-paczke-Uwaga-na...
11. UOKiK — sygnały ostrzegawcze uokik.gov.pl/zakupy-wysokiego-ryzyka-falszywe-sklepy-udawane-polskie-marki-nieuc...

5 Finalizacja i odbiór

Zamówienie złożone — dopilnuj, by nic Cię nie zaskoczyło

- ☐ Potwierdzenie: Dostałem/am e-mail z potwierdzeniem zamówienia — i zapisałem/am jego treść oraz numer zamówienia.
- ☐ Zapisałem/am potwierdzenie płatności, np. zrzut ekranu z aplikacji banku lub e-mail od sklepu.
- ☐ Znam przewidywany termin dostawy oraz numer śledzenia przesyłki.
- ☐ Status paczki sprawdzam wyłącznie na oficjalnej stronie przewoźnika — numer przesyłki wpisuję ręcznie, nie z linku z SMS-a.
- ☐ Przy odbiorze zwracam uwagę na stan opakowania — uszkodzoną paczkę mogę otworzyć przy kurierze i spisać protokół.
- ☐ Wiem, że mam 14 dni na odstąpienie od umowy bez podawania przyczyny — i zachowuję dowód zakupu (potwierdzenie, faktura).

TWOJE PRAWO

Towar kupiony przez internet możesz zwrócić w ciągu 14 dni od jego otrzymania — bez tłumaczenia się. Sprzedawca musi zwrócić wszystkie płatności, w tym koszt najtańszej dostawy.

WSZYSTKIE POLA ZAZNACZONE?

Jeśli tak — możesz bezpiecznie sfinalizować zakup. Jeśli jakiekolwiek pole sprawia Ci wątpliwości, poproś o pomoc bliską osobę lub rzecznika konsumentów.

12. Konsument.gov.pl — zakupy na odległość, 14 dni na odstąpienie konsument.gov.pl/zakupy-na-odleglosc-prawa-konsume...
13. UOKiK — zwrot towaru kupionego przez internet uokik.gov.pl/download/15712

Gdy coś pójdzie nie tak

Numery i strony, które pomogą — zapisz je w telefonie

Podejrzany SMS z paczki lub dopłatą?
Prześlij go bez zmian na bezpłatny numer 8080 (CERT Polska). Nie klikaj w link.

Podejrzana strona lub sklep?
Sprawdź ją na cert.pl/lista-ostrzezen — tam znajdziesz aktualną listę ostrzeżeń.

Ktoś poznał Twoje dane lub karty?
Natychmiast zadzwoń do swojego banku (infolinia jest na karcie lub w aplikacji) i zablokuj kartę oraz konto.

Zniknęły pieniądze?
Zgłoś oszustwo Policji: telefon 112 lub najbliższa jednostka. Zabierz ze sobą dowody.

Sklep nie odpowiada lub nie zwraca pieniędzy?
Zadzwoń do rzecznika konsumentów: 801 440 220 lub 22 266 76 76 (pn.–pt.).

ZŁOTA ZASADA NA KONIEC

Masz wątpliwości? Odczekaj jeden dzień i porozmawiaj z kimś zaufanym. Uczciwy sklep nie zniknie, a oszust nie lubi czekać — i właśnie po tym go poznasz.

Źródła — gdzie sprawdzić samodzielnie

- CERT Polska — bezpieczne zakupy w internecie
  https://cert.pl/falszywe-sklepy/
- CERT Polska — poradnik zakupowy (PDF)
  https://cert.pl/uploads/docs/CERT_poradnik_zakupowy.pdf
- CERT Polska — lista ostrzeżeń przed niebezpiecznymi stronami
  https://cert.pl/lista-ostrzezen/
- UOKiK — zakupy wysokiego ryzyka, fałszywe sklepy
  https://uokik.gov.pl/zakupy-wysokiego-ryzyka-falszywe-sklepy-udawane-polskie-marki-nieuczciwi-posrednicy
- UOKiK — pomoc dla konsumentów
  https://uokik.gov.pl/pomoc-dla-konsumentow
- Konsument.gov.pl — zakupy na odległość i prawo do odstąpienia
  https://konsument.gov.pl/zakupy-na-odleglosc-prawa-konsumenta/
- Wyszukiwarka CEIDG — darmowa weryfikacja firm
  https://aplikacja.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx
- Sprawdź status NIP — podatki.gov.pl
  https://sprawdznip.podatki.gov.pl/
- Ministerstwo Cyfryzacji i NASK — jak rozpoznać fałszywy sklep
  https://www.gov.pl/web/cyfryzacja/uwaga-na-falszywe-sklepy-online--ostrzega-ministerstwo-cyfryzacji-i-nask
- Policja — ostrzeżenie przed fałszywymi SMS-ami kurierów
  https://podkarpacka.policja.gov.pl/rze/aktualnosci/151554,Policja-ostrzega-przed-falszywymi-SMS-ami.html

14. CERT Polska — zgłaszanie podejrzanych SMS-ów (8080) cert.pl/lista-ostrzezen/
15. UOKiK — pomoc dla konsumentów uokik.gov.pl/pomoc-dla-konsumentow