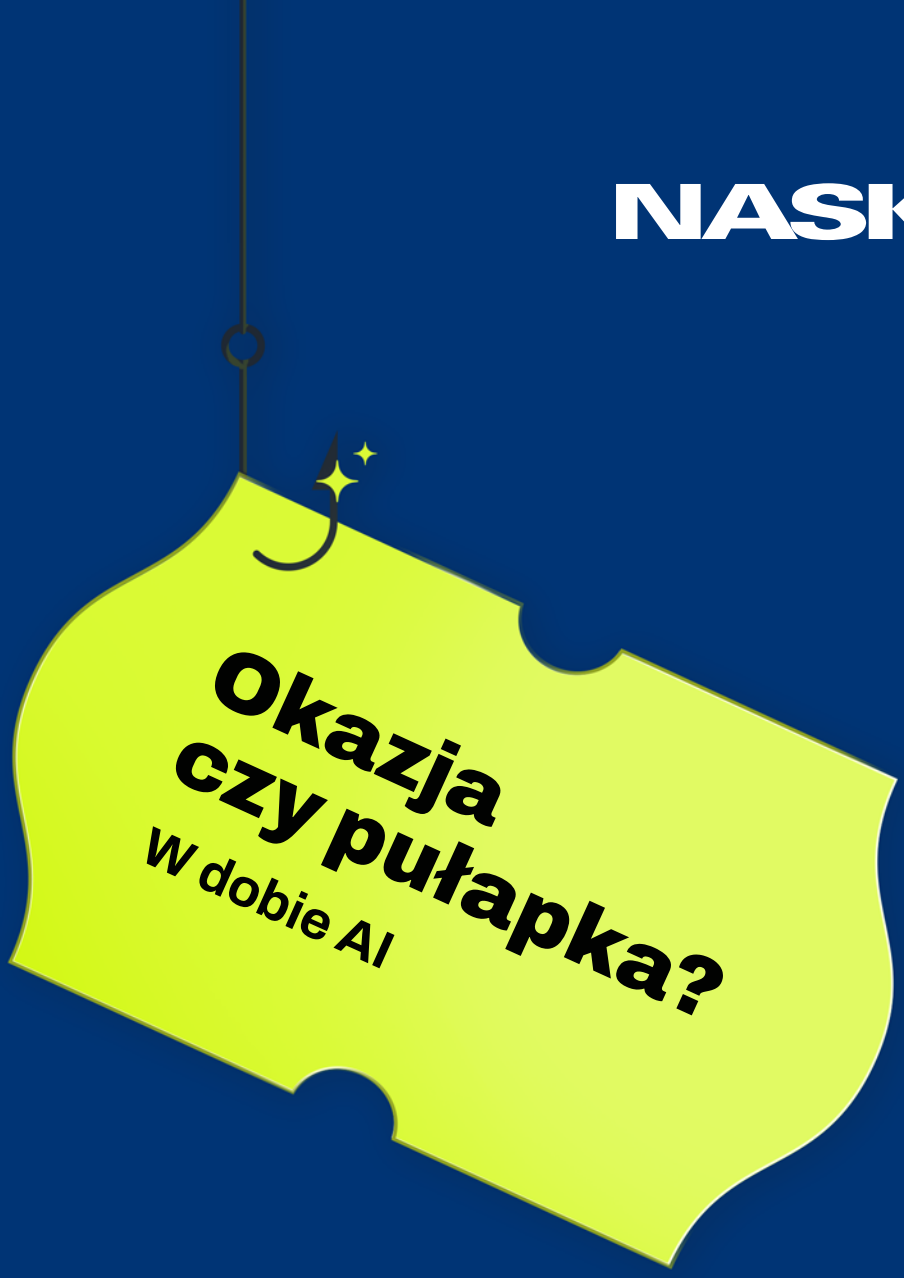
NASK



Część II poradnika
o bezpiecznych
zakupach online

TYTUŁ

Okazja czy pułapka? W dobie AI

Część II poradnika o bezpiecznych zakupach online

AUTORZY

Katarzyna Grabowska (red.), Agnieszka Wrońska, Sylwia Adamczyk, Karol Bojke

KOMENTARZE EKSPERCKIE

st. asp. Monika Przestrzelska, p.o. Rzecznika Prasowego Komendanta CBZC

dr Anna Mlostoń-Olszewska, radca prawny, Pełnomocnik Terenowy Rzecznika Finansowego w Łodzi

Paweł Rodziewicz, Miejski Rzecznik Konsumentów w Elblągu

Wojciech Szczerba, Koordynator Projektu ECK Polska

Andrzej Janyszko, Departament Komunikacji UOKiK

WSPARCIE MERYTORYCZNE

Olga Zabolewicz

REDAKCJA JĘZYKOWA I KOREKTA

Łukasz Szczęsny, Katarzyna Nakonieczna

PROJEKT GRAFICZNY

NASK – PIB

Publikacja jest rozpowszechwniana na zasadach licencji Creative Commons
Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe

ISBN 978-83-68356-91-5

2026

NASK – Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

www.nask.pl









PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Ministra Cyfryzacji.

Spis treści

3 Wstęp

8 Fałszywe sklepy internetowe tworzone przy użyciu AI

13 Manipulacja opiniami o produktach przy użyciu sztucznej inteligencji

17 Oszustwa związane z płatnościami

21 Fałszywe oferty zakupowe w mediach społecznościowych

24 Dezinformacja i fałszywe autorytety w reklamach

28 Fałszywe aplikacje zakupowe

31 Oszustwa związane z przesyłkami i śledzeniem paczek

35 Sklepy sezonowe

39 Oznaczanie treści wygenerowanych przy pomocy AI – prawo i zagrożenia

42 Komentarze eksperckie dot. ochrony konsumentów

Wstęp

Zakupy online stały się już niemal nieodłącznym elementem codziennego życia. Internet daje dostęp do ogromnej liczby produktów, atrakcyjnych cen, promocji oraz możliwości porównywania ofert bez wychodzenia z domu. Wraz z rozwojem handlu elektronicznego rośnie jednak także liczba zagrożeń. Cyberprzestępcy doskonale wiedzą, że konsumenci poszukują okazji cenowych, kierują się opiniami innych użytkowników i często podejmują decyzje pod wpływem emocji czy presji czasu. Dlatego coraz częściej wykorzystują stworzone przy użyciu sztucznej inteligencji fałszywe sklepy internetowe, fikcyjne promocje, zmanipulowane opinie i reklamy. W efekcie nawet doświadczeni użytkownicy internetu mogą mieć trudność z oceną, czy mają do czynienia z autentycznym sprzedającym.

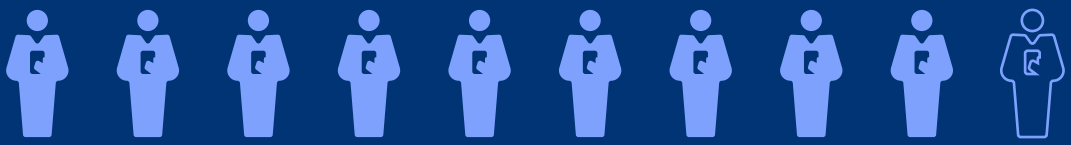
Poradnik, który oddajemy w Państwa ręce, stanowi drugą część publikacji o bezpieczeństwie zakupów online „Okazja czy pułapka? Poradnik o bezpiecznych zakupach online" i opisuje obserwacje dotyczące metod oszustów oraz oferuje praktyczne wskazówki pomagające unikać internetowych pułapek. Szczególną uwagę poświęcono nowym wyzwaniom związanym ze sztuczną inteligencją, która coraz częściej wykorzystywana jest do tworzenia fałszywych sklepów, opinii, reklam oraz innych treści wpływających na decyzje zakupowe konsumentów.

Poradnik został również wzbogacony o porady ekspertów z różnych instytucji, którzy dzielą się swoją wiedzą i doświadczeniem w zakresie ochrony konsumentów.

Mamy nadzieję, że zawarte w tej publikacji informacje pomogą Państwu dokonywać bardziej świadomych decyzji zakupowych, skuteczniej rozpoznawać zagrożenia i bezpieczniej korzystać z możliwości, jakie oferuje współczesny handel elektroniczny. W świecie, w którym coraz trudniej odróżnić prawdziwe oferty od fałszywych, wiedza i ostrożność pozostają najlepszą ochroną przed oszustami.

Kupujemy online często i coraz wygodniej

Zakupy internetowe stały się codziennością. W 2026 roku aż 93% polskich internautów odwiedzało strony i aplikacje zakupowe, a ponad połowa (53%) robiła to codziennie. Potwierdza to również częstotliwość zakupów online – 79% kupujących deklarowało, że zrealizowało je w ciągu ostatniego miesiąca, podczas gdy tylko 3% wskazało, że ich ostatni zakup miał miejsce dawniej niż rok temu[1].



93% polskich internautów odwiedzało strony i aplikacje zakupowe.

Smartfon króluje podczas zakupów

Coraz częściej zakupy robimy za pomocą telefonu. Polscy internauci korzystają ze sklepów internetowych przede wszystkim na swoich smartfonach (w 2026 r. liczba użytkowników to średnio 14 mln dziennie), rzadziej zaś na komputerach (3 mln)[1].



Dla współczesnych konsumentów ważna jest nie tylko cena. Coraz większe znaczenie mają wiarygodność sprzedawcy, bezpieczeństwo zakupów oraz autentyczność opinii [2].

Co buduje zaufanie do sklepu internetowego?



Sztuczna inteligencja coraz częściej pomaga w zakupach

Tylko **8%** konsumentów preferuje kontakt z chatbotem.

Narzędzia AI stają się integralną częścią procesu robienia zakupów online. **Ponad połowa klientów e-commerce korzysta z rozwiązań opartych na sztucznej inteligencji**, np. podczas wyszukiwania czy uzyskiwania informacji o ofercie lub jako źródło rekomendacji. Jednocześnie konsumenci nadal preferują kontakt z człowiekiem[2].

AI tak, zakupy bez nadzoru nie

Mimo że duża część konsumentów (65%) korzysta z narzędzi AI, 71% nie chciałoby powierzyć sztucznej inteligencji samodzielnego dokonania zakupu[1].





Coraz bardziej świadomi konsumenci

Kupujący stają się coraz ostrożniejsi i bardziej wymagający. Rośnie znaczenie zweryfikowanych opinii, rzetelnych informacji o produktach oraz transparentności sprzedawców[2].



Fałszywe sklepy internetowe tworzone przy użyciu AI

Po czym rozpoznać fałszywy sklep internetowy?

Jeszcze kilka lat temu można było wskazać kilka sygnałów ostrzegawczych:

- strona internetowa zawierała błędy językowe;
- zamieszczone zdjęcia były słabej jakości;
- nie podawano informacji o sprzedającym lub były niekompletne.

A dziś?
Sytuacja wygląda zupełnie inaczej

Rozwój sztucznej inteligencji sprawił, że tworzenie różnego rodzaju treści stało się nie tylko dużo prostsze i szybsze. Dodatkowo współczesne modele generują materiały praktycznie pozbawione wymienionych wcześniej cech i coraz trudniej jest na pierwszy rzut oka stwierdzić, że mamy do czynienia z dziełem oszustów. Przestępcy wykorzystują AI do tworzenia zwodniczych wizualizacji nieistniejących produktów i szaty graficznej całych sklepów internetowych.

W reklamach wygenerowanych dzięki narzędziom sztucznej inteligencji spotkasz np.:

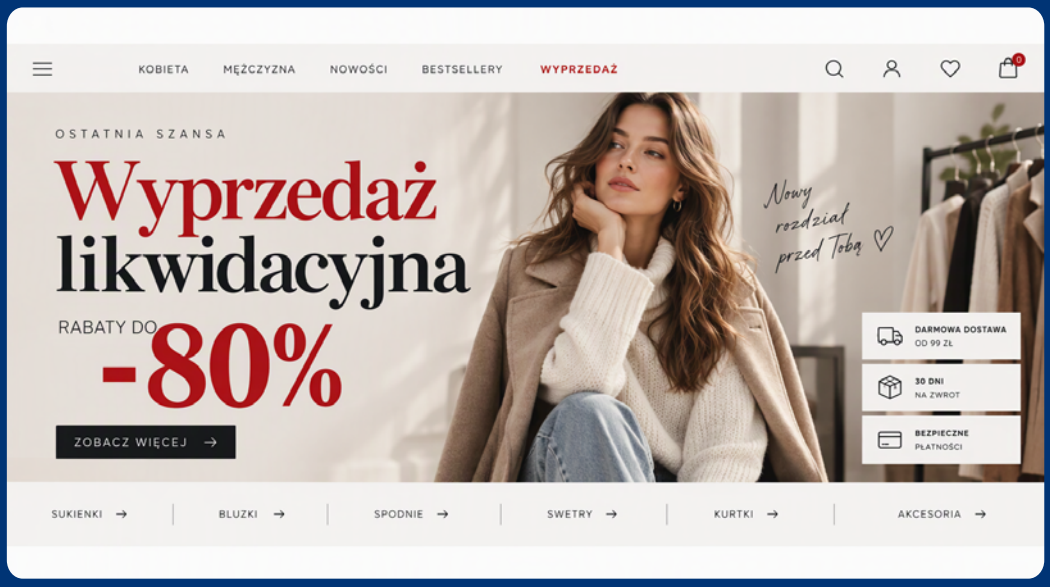
- „zdjęcia" produktów, które w rzeczywistości nie istnieją,
- wizerunki rzekomych klientów prezentujących produkty lub efekty ich działania,
- fikcyjne opinie i recenzje,
- fałszywe zdjęcia magazynów, pracowników czy siedziby firmy,
- filmy prezentujące produkt, który po zakupie okazuje się wyglądać zupełnie inaczej lub nigdy nie zostaje dostarczony.

Profesjonalnie wyglądająca witryna internetowa – czy to prawdziwy sklep?

Zakupy online dają możliwość m.in. wyszukania produktu w okazyjnej cenie. Wystarczy, że wpiszesz w przeglądarce internetowej interesujący cię przedmiot, by już po chwili mieć przed sobą listę stron oferujących to, czego szukasz. Jedno kliknięcie i przenosisz się do internetowej witryny sklepowej. Bywa jednak, że sklep, do którego trafiasz, nie jest uczciwym przedsiębiorstwem, a serwisem próbującym wyłudzić twoje pieniądze lub dane.

Wczytana po otwarciu odnośnika, podszywająca się pod sklep, strona może wyglądać bardzo wiarygodnie. Najczęściej są na niej zdjęcia produktów z poprawnymi językowo opisami, opinie klientów, regulamin a nawet chatbot, gotów odpowiedzieć ci w czasie rzeczywistym na wszystkie pytania. Na pierwszy rzut oka nic nie wzbudza podejrzeń. Co więcej, wymienione elementy budują zaufanie i mogą uśpić twoją czujność. Problem ujawni się dopiero po przekazaniu danych i/lub zakończeniu płatności.

PRZYKŁAD: STRONA FAŁSZYWEGO SKLEPU Z ODZIEŻĄ*



*przykładowa witryna wygenerowana za pomocą AI.

PRZYKŁAD: STRONA FAŁSZYWEGO SKLEPU Z ODZIEŻĄ*



*przykładowa witryna wygenerowana za pomocą AI.

W ofercie fałszywego sklepu mogą znaleźć się setki produktów, często przecenionych nawet o kilkaset złotych. Nagłówki kuszą rzekomą „wyprzedażą likwidacyjną". Zdarza się, że cała historia o zamknięciu biznesu służy jedynie uwiarygodnieniu oszustwa. Rzekome zdjęcia zadowolonych klientek mogą okazać się obrazami wygenerowanymi dzięki narzędziom AI.

Sprawdź, zanim kupisz

Profesjonalnie wyglądająca strona może okazać się dobrze przygotowaną mistyfikacją. Na co więc zwracać uwagę, zanim zdecydujesz się na zakup? Jest kilka elementów, od których dobrze zacząć.

https://twojpolskisklep.pl/pozostala/czesc/adresu

adres strony / domena

Adres strony

To pierwsza rzecz, której warto się przyjrzeć. Trzeba jednak zaznaczyć, że adres strony może być łudząco podobny do znanej nazwy sklepu – może różnić się w prawie niezauważalny sposób, np. duża litera *I* (i) zostaje podmieniona na małą literę *l* (L) lub podwójne *v* zastępuje *w*. Może się też zdarzyć, że pierwszy raz kupujesz w jakimś sklepie i po prostu nie wiesz, jak powinien brzmieć adres jego strony. Dlatego podczas zakupów online zawsze należy mieć odruch weryfikowania sprzedawcy i innych elementów znajdujących się na stronie.

Informacje o sprzedającym

Na stronie internetowej sklepu powinny znaleźć się informacje o jego właścicielu. Warto porównać je z ogólnodostępnymi rejestrami KRS lub CEIDG. Brak adresu siedziby, numeru kontaktowego czy informacji o sprzedającym to oznaki, które należy potraktować jako sygnał ostrzegawczy.

Dostępne formy płatności

Jeśli sklep oferuje ograniczony wybór form płatności (np. tylko przelew na konto, tylko płatność kartą), powinna zapalić ci się czerwona lampka. Bywa też tak, że na stronie sklepu widzisz różne formy płatności: płatność kartą, płatność mobilna, gotówka przy odbiorze czy tradycyjny przelew, ale przy finalizacji zakupu dostępna jest tylko jedna z nich, np. płatność kartą. Brak możliwości skorzystania z innych, ogólnodostępnych form płatności to także sygnał ostrzegawczy, który może świadczyć, że masz doczynienia z oszustwem.

Cena produktu i presja czasu

Zawsze porównuj cenę danego produktu z cenami oferowanymi przez sprzedawców na innych stronach. Jeśli jest wyraźnie niższa od cen rynkowych, może to oznaczać, że masz do czynienia z oszustwem. Dodatkowo zwracaj uwagę, czy sprzedający nie wywiera presji czasu poprzez komunikaty typu: „ostatnia sztuka", „promocja ważna tylko do północy" czy zegary odliczające czas do zakończenia promocji. Poczucie przemijającej okazji może potęgować chęć jak najszybszej finalizacji zakupu.

Polityka prywatności

Mało kto zagląda do tego dokumentu, choć jego dostępność podczas przetwarzania danych w celu sprzedaży internetowej jest wymagana prawnie. Przestępcy często podchodzą do niego po macoszemu – albo przycisk kierujący do stosownej podstrony nie działa, albo w treści polityki roi się od błędów, najczęściej w wyniku tłumaczenia maszynowego.

Opinie

Dobrym wyznacznikiem wiarygodności sklepu internetowego są opinie wystawiane przez klientów. Czasem mogą cię uchronić przed nieuczciwym sprzedawcą lub niskiej jakości towarem. Opinie najlepiej sprawdzać bezpośrednio w wyszukiwarce internetowej i na dedykowanych temu portalach. Trzeba jednak uważać na fałszywe wpisy, które mogli spreparować sami przestępcy lub wykupione przez nich boty.

Manipulacja opiniami o produktach przy użyciu sztucznej inteligencji



Od lat to opinie klientów należą do najważniejszych czynników wpływających na decyzje zakupowe. Aż 90,2% kupujących deklaruje, że zwraca uwagę na recenzje pochodzące od innych użytkowników, a wśród osób w wieku 18–29 lat odsetek ten wynosi 96%[3]. Oceny i komentarze stały się jednym z kluczowych źródeł informacji przy wyborze produktów i sprzedawców. Dla 43% konsumentów są one jednym z najważniejszych czynników wpływających na zaufanie do e-sklepu[4]. Klienci przywiązują również coraz większe znaczenie do aktualności recenzji i są świadomi, że liczy się ich autentyczność. Około trzy czwarte kupujących online zwraca uwagę na to, czy opinie są nowe, a niemal 60% przedstawicieli pokolenia Z deklaruje, że zetknęło się z fałszywymi lub manipulacyjnymi recenzjami[2].

Dlaczego fałszywe opinie są niebezpieczne?

Rozwój sztucznej inteligencji sprawił, że tworzenie fałszywych opinii stało się łatwiejsze, tańsze i bardziej wydajne. Fałszywa opinia wygenerowana przy pomocy AI może przybrać postać recenzji produktu, usługi czy sklepu, która wygląda jak relacja zadowolonego klienta, choć w rzeczywistości nie stoi za nią żadna osoba mająca kontakt z produktem. Co więcej, gdy widzimy wiele pozytywnych ocen i pochlebnych komentarzy, naturalnie zakładamy, że inni klienci są zadowoleni z zakupu, a produkt lub sprzedawca zasługują na zaufanie. To właśnie ten mechanizm wykorzystują oszuści oraz nieuczciwi sprzedawcy. Tworząc fałszywe opinie i recenzje, próbują wywołać wrażenie, że dany produkt cieszy się dużym uznaniem i został sprawdzony przez wielu zadowolonych klientów. Niestety podobne praktyki stosują czasem również legalnie działające sklepy czy sprzedawcy, którym wydaje się, że sztuczne poprawianie ocen pozwoli szybko zwiększyć sprzedaż.



★★★★☆

Susan W.

Jakość na najwyższym poziomie. Efekty już pierwszego dnia. Nie wyobrażam sobie bez niego funkcjonowania. Wsyscy moi znajomi już kupili



★★★★★

Anna

Słuchawki oferują bardzo dobrą jakość dźwięku oraz wygodę użytkowania. Bateria pozwala na długie korzystanie bez konieczności częstego ładowania. Produkt wyróżnia się korzystnym stosunkiem jakości do ceny i spełnia oczekiwania nawet bardziej wymagających użytkowników.



★★★★★

Karol Kotowski

Jestem bardzo zadowolony z zakupu. Produkt wyróżnia się wysoką jakością wykonania oraz intuicyjną obsługą. Spełnia wszystkie oczekiwania, a nawet je przewyższa. Korzystam z niego codziennie i mogę z pełnym przekonaniem polecić go każdemu, kto szuka niezawodnego rozwiązania w rozsądnej cenie. Dodatkowym atutem jest świetny stosunek jakości do ceny.



★★★★★

Piotr lat 65

To zdecydowanie najlepszy suplement, jaki kiedykolwiek stosowałem. Już po kilku dniach zauważyłem ogromną poprawę samopoczucia, więcej energii i lepszą koncentrację. Produkt działa dokładnie tak, jak obiecuje producent. Polecam każdemu, kto chce zadbać o swoje zdrowie i dobre samopoczucie.

Przykładowa ilustracja

Powyższe opinie wyglądają podejrzanie, ponieważ są bardzo ogólne, nie zawierają konkretnych informacji dotyczących rzeczywistego użytkowania produktu, nie wskazują ani żadnej wady i sa bardzo entuzjastyczne. Sformułowania takie jak: „bardzo dobra jakość

dźwięku", „korzystny/świetny stosunek jakości do ceny", „spełnia oczekiwania wymagających użytkowników", „niezawodne rozwiązanie w rozsądnej cenie", „działa dokładnie tak, jak obiecuje producent" są typowymi frazami marketingowymi, które mogą pasować do niemal każdego produktu i nie brzmią jak wyraz czyichś osobistych odczuć.

Jak rozpoznać fałszywe recenzje?

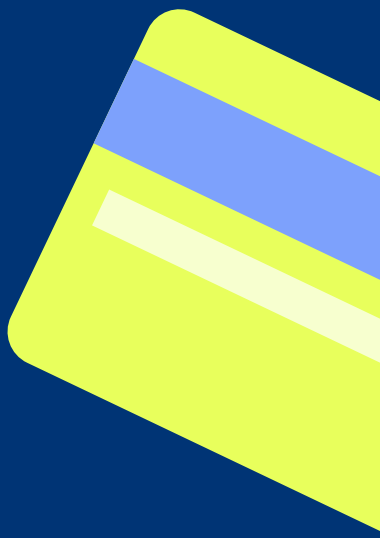
Choć nie ma jednej cechy pozwalającej z całkowitą pewnością wskazać fałszywą opinię, zwracaj uwagę na kilka sygnałów ostrzegawczych.

- **Zbyt ogólnikowe komentarze**, w których brakuje konkretnych informacji o użytkowaniu produktu, np. „Świetny produkt, polecam!", „Najlepszy zakup w życiu!".
- **Przesadnie entuzjastyczny ton**, np. „Ten blender zmienił moje życie! Każdy powinien go kupić!".
- **Powtarzające się sformułowania w wielu opiniach**, czyli sytuacja, gdy wiele recenzji używa niemal identycznych zwrotów. Może to oznaczać, że zostały napisane przez jedną osobę lub wygenerowane automatycznie.
- **Język przypominający reklamę**, np. „Innowacyjne rozwiązanie gwarantujące najwyższą jakość i niezrównaną satysfakcję użytkownika".
- **Nagły „wysyp" opinii.** Jeżeli przez wiele miesięcy produkt miał niewiele ocen, a nagle w ciągu kilku dni pojawia się kilkadziesiąt lub kilkaset i to wyłącznie pozytywnych recenzji, może to świadczyć o sztucznym generowaniu komentarzy. Sprawdzaj daty publikacji. Wiele podobnych opinii z krótkiego okresu może budzić wątpliwości.
- **Same zachwyty i brak wad.** Żaden produkt nie jest idealny dla wszystkich użytkowników. Czytaj zarówno opinie pozytywne, jak i negatywne. Brak krytycznych ocen może być sygnałem ostrzegawczym. Porównuj informacje w różnych źródłach, weryfikuj opinie także poza sklepem internetowym.

Jeśli opinie, sprzedawca lub sam produkt budzą jakiekolwiek wątpliwości, poświęć kilka minut na dodatkową weryfikację informacji. W erze AI zdrowy sceptycyzm staje się równie ważny jak porównywanie cen czy parametrów technicznych różnych produktów przed transakcją. Świadome korzystanie z recenzji wystawianych przez innych użytkowników nie gwarantuje udanych zakupów, ale zmniejsza ryzyko podjęcia decyzji pod wpływem manipulacji, marketingowych sztuczek czy fałszywych recenzji.

Oszustwa związane z płatnościami



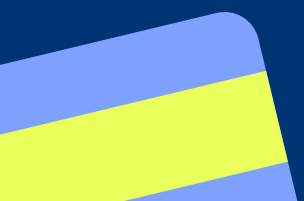


Zakupy internetowe są wygodne także dlatego, że umożliwiają dokonywanie płatności online. Dzięki nim wiele spraw można załatwić „od ręki”, szybko i bezgotówkowo. Wygodę tę doceniają kupujący, ale i wykorzystują cyberprzestępcy, którzy nieustannie poszukują sposobów na wyłudzenia danych (w tym finansowych) oraz samych pieniędzy.

Oszuści wykorzystują profesjonalnie wyglądające strony i generują treści z wykorzystaniem AI, za pomocą których mogą starać się przekonać cię, że to, co widzisz, jest prawdą.

Oszustwa płatnicze

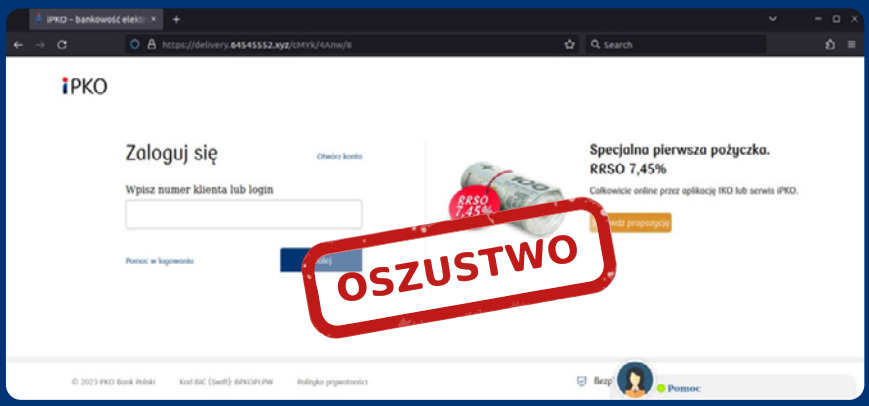
Celem oszustów jest nakłonienie cię do przekazania swoich danych logowania do kont bankowych, podania numerów kart płatniczych czy kodów autoryzacyjnych. W ten sposób mogą uzyskać dostęp nie tylko do twoich danych, ale i pieniędzy. Aby osiągnąć ten cel wykorzystują preteksty takie jak np. sprawiające wrażenie pilnych komunikaty, informacje o rzekomych problemach z płatnościami lub obietnice atrakcyjnych promocji. Wywierając presję czasu i próbując wzbudzić emocje, liczą na twoją nieuwagę.





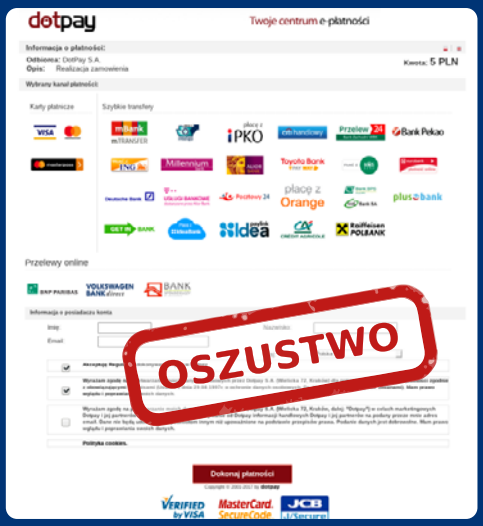
Fałszywa strona banku

Oszuści, podszywając się pod uznane i rozpoznawalne instytucje, tworzą strony internetowe wykorzystujące łudząco podobną do oryginału szatę graficzną, logotypy i układ treści. Co więcej, adres strony może różnić się jedynie nieznacznie od prawdziwej, dobrze znanej domeny banku. Podanie loginu i hasła na takiej stronie skutkuje przekazaniem danych logowania oszustom, co mogą oni wykorzystać do przejęcia konta bankowego.



Źródło: CERT Polska/CSIRT NASK

Fałszywa bramka płatności



Bramki płatnicze to mechanizm pośredniczący pomiędzy sprzedawcą a kupującym, umożliwiający szybkie przesyłanie pieniędzy podczas zakupów online. Fałszywa bramka może łudząco przypominać prawdziwego operatora i tak samo oferować różne metody płatności, które w rzeczywistości przekierowują na fałszywe strony kontrolowane przez oszustów, przez co wprowadzone tam dane trafiają prosto w ręce cyberprzestępców.

Źródło: CERT Polska/CSIRT NASK

Prawdziwa płatność, nieistniejący produkt

Atrakcyjne oferty sprzedaży mogą pojawić się na prawdziwych stronach internetowych, w mediach społecznościowych, popularnych serwisach ogłoszeniowych czy aukcyjnych. Oszuści działają także tam, kusząc kupujących niskimi cenami. Zakup bez wcześniejszej weryfikacji czy choćby wnikliwego wczytania się w opis oferty może okazać się szybką ścieżką do straty pieniędzy, gdyż zakupione dobra nigdy nie zostają wysłane.

Oszustwo na kody do płatności mobilnych

Oszustwa związane z płatnościami to nie tylko fałszywe strony czy aplikacje. To również próby wyłudzenia kodów do płatności mobilnych poprzez przejęte konta w mediach społecznościowych. Przestępcy, podszywając się pod znajomych, piszą do osób z listy kontaktów przejętego konta z prośbą o kod, tłumacząc się np. rzekomym brakiem gotówki przy kasie i pilną potrzebą zapłacenia za zakupy.

Sprawdź, zanim zapłacisz



Link w wiadomości
Przed przekazaniem jakichkolwiek informacji zwracaj uwagę na adres strony. Sprawdź, czy jesteś we właściwym miejscu.



Prośba o podanie danych karty
Przestępcy mogą próbować wywrzeć presję komunikatami typu: „Konieczna weryfikacja karty”, „Płatność nie powiodła się, zweryfikuj dane, inaczej zamówienie zostanie anulowane”. Jeśli coś wzbudza twoje wątpliwości, nie podawaj danych kart płatniczych.



Prośba od znajomego
Jeśli ktoś ze znajomych lub rodziny niespodziewanie prosi cię o kod do płatności mobilnych, może to być próba oszustwa. Taką prośbę najlepiej zweryfikuj innym kanałem, np. zadzwoń na numer tej osoby i potwierdź, że wiadomość faktycznie pochodzi od niej.

O czym warto pamiętać?

Zawsze stosuj zasadę ograniczonego zaufania. Nawet jeśli strona czy wiadomość na pierwszy rzut oka wygląda prawidłowo, zweryfikuj ją dokładnie. Przed dokonaniem jakiejkolwiek płatności zawsze sprawdzaj rodzaj transakcji, odbiorcę i kwotę. Nie udostępniaj kodów do płatności mobilnych, dopóki nie upewnisz się, że prośba pochodzi rzeczywiście od osoby, za którą podaje się rozmówca. Oszuści liczą na pośpiech i działanie pod wpływem chwili.

Fałszywe oferty zakupowe w mediach społecznościowych



Platformy społecznościowe są chętnie wykorzystywane do reklamowania sklepów internetowych czy konkretnych produktów. Niestety korzystają z nich także oszuści, którzy tworzą fałszywe profile i reklamy, by wyłudzić pieniądze lub dane osobowe.

Bywa, że fałszywe oferty pojawiają się na profilach, które od jakiegoś czasu obserwujesz, wpisują się w ich temat i dodatkowo kuszą ograniczoną liczbą produktów, krótkim czasem trwania wyjątkowej oferty cenowej czy promocją dla wybranych. Chcą skłonić cię do zakupu, zanim zdążysz spokojnie sprawdzić sprzedawcę i warunki transakcji.

Zagrożeniem są również reklamy prowadzące do stron, które wyglądają jak prawdziwe witryny sklepów lub znanych marek.

Jakie oszustwa mogą pojawiać się w mediach społecznościowych?



Fałszywe wyprzedaże likwidacyjne
Reklamy informują o rzekomym zamknięciu sklepu lub likwidacji magazynu, oferując produkty przecenione nawet o 70–90%. Po dokonaniu zakupu możesz nie otrzymać zamówienia lub dostać produkt o znacznie niższej jakości niż deklarowana. Podchodź z rezerwą do wyjątkowo dużych obniżek cen.



Podszywanie się pod znane marki
Oszuści kopiują logo, zdjęcia oraz wygląd oficjalnych stron internetowych, zmieniając jedynie szczegóły adresu URL. Jeśli reklama dotyczy znanego sklepu lub serwisu, najlepiej wejdź na jego oficjalną stronę internetową lub skorzystaj z aplikacji, wyszukaj reklamowany produkt i sprawdź, czy jego cena jest taka sama. Dokonuj zakupów pod adresem lub w aplikacji, które znasz.



Towar niezgodny z reklamą
Zdjęcia i filmy prezentują produkt wysokiej jakości w wyjątkowo atrakcyjnej cenie, a po otrzymaniu przesyłki okazuje się, że to tania podróbka, produkt o zupełnie innych parametrach lub przedmiot nieprzypominający tego z reklamy. Zaskakująco niska cena produktu zawsze powinna skłonić cię do dokładnej weryfikacji sklepu.

Deepfake w reklamach zakupowych

Do oszustw w mediach społecznościowych wykorzystywane są także materiały typu deepfake.

Deepfake to wygenerowany przez sztuczną inteligencję fałszywy materiał audio lub wideo. Przykładem może być zmanipulowane nagranie przedstawiające osobę wypowiadającą słowa, które w rzeczywistości nigdy nie padły z jej ust. Za sprawą tej technologii możesz zobaczyć znanego aktora, dziennikarza, influencera czy eksperta, który poleca określony produkt, choć tak naprawdę nigdy tego nie zrobił.

Takie materiały są szczególnie niebezpieczne, ponieważ wykorzystują twoje zaufanie do rozpoznawalnych osób. Jeśli ktoś, kogo znasz z telewizji, internetu lub mediów społecznościowych, osobiście rekomenduje produkt, łatwiej jest uznać ofertę za wiarygodną. Tymczasem sam film może być całkowicie wygenerowany lub zmodyfikowany przez sztuczną inteligencję.

Nie zakładaj, że film jest prawdziwy tylko dlatego, że występuje w nim znana osoba. Jeśli lubiany lub szanowany przez ciebie celebryta, ekspert lub influencer zachęca w internecie do zakupu produktu, zweryfikuj tę informację. Możesz na przykład zajrzeć na oficjalny profil tej osoby.

O czym warto pamiętać?

- Weź pod uwagę, że obecność reklamy na popularnej platformie społecznościowej nie jest gwarancją wiarygodności sprzedawcy.
- Zachowaj ostrożność wobec wyjątkowo atrakcyjnych promocji.
- Nie ufaj bezkrytycznie zdjęciom i nagraniom na platformach społecznościowych. Materiały publikowane w reklamach mogą być wygenerowane lub zmodyfikowane przez narzędzia sztucznej inteligencji, dlatego warto szukać dodatkowych informacji o produkcie i sprzedawcy.
- Poświęć kilka minut na weryfikację oferty – może cię to uchronić przed utratą pieniędzy lub danych.

Traktuj reklamy prezentujące produkty wyglądające wręcz zbyt idealnie jako sygnał ostrzegawczy. Zdjęcia mogą być bardzo efektowne, ale jednocześnie sprawiać wrażenie sztucznych. Nie ufaj bezkrytycznie samemu obrazowi. Gdy reklama wydaje się zbyt atrakcyjna, wstrzymaj się z zakupami i poszukaj informacji na temat danego sklepu lub produktu w innych źródłach. Wyrób w sobie nawyk wpisywania adresu nieznanego sklepu w wyszukiwarkę internetową i sprawdzania opinii o nim.

Dezinformacja i fałszywe autorytety w reklamach

Internet pełen jest reklam obiecujących szybkie rozwiązania problemów zdrowotnych, finansowych czy życiowych. Jednak bardzo często nie stoją za nimi przełomowe produkty czy usługi, lecz dezinformacja i różnorodne techniki manipulacji.

Dezinformacja to fałszywa bądź wprowadzająca w błąd treść, która jest tworzona lub rozpowszechniana celowo, z zamiarem oszukania odbiorców bądź pozyskania określonych korzyści.

W obszarze medycyny niesie ona szczególnie duże ryzyko, bo może wpływać na decyzje dotyczące leczenia lub profilaktyki i w efekcie skutkować pogorszeniem stanu zdrowia, opóźnianiem właściwej diagnozy, a w skrajnych przypadkach nawet zagrożeniem życia.

Dezinformacja zdrowotna może przybierać formę fałszywych porad medycznych i treści podważających bezpieczeństwo lub skuteczność sprawdzonych metod leczenia, ale także promowania i sprzedaży leków, suplementów, diet czy terapii o rzekomym „cudownym” działaniu.

Zachowaj szczególną czujność, jeśli reklama:

- gwarantuje pewne wyleczenie choroby;
- obiecuje natychmiastowe efekty;
- sugeruje, że lekarze ukrywają skuteczną metodę leczenia;
- zachęca do odstawienia terapii zaleconej przez specjalistę;
- powołuje się na anonimowych ekspertów;
- posługuje się presją czasu.

Fałszywe autorytety

Osoby, które głoszą w internecie rzekomo przełomowe sposoby leczenia i sprzedają własne produkty paramedyczne, suplementy, diety czy usługi, w rzeczywistości mogą nie mieć żadnych kwalifikacji. W sieci możesz natrafić na armię fałszywych ekspertów, którzy podważają sens badań naukowych, krytykują konwencjonalną medycynę, propagują teorie spiskowe na temat koncernów farmaceutycznych oraz zachwalają „naturalne" i „alternatywne" metody leczenia. Robią to najczęściej dla zarobku. Nie wszyscy ci fałszywi eksperci istnieją w rzeczywistości, często popularnością cieszą się profile (np. lekarzy) wygenerowane w całości dzięki narzędziom sztucznej inteligencji.

Miej na uwadze, że internetowi szarlatani mogą sprzedawać produkty nieprzebadane lub mające wprost szkodliwe działanie. Suplementy, zioła i inne preparaty reklamowane jako „cudowne środki" mogą być nie tylko nieskuteczne, ale wręcz powodować niepożądane skutki lub wchodzić w interakcje z lekami przepisanymi przez lekarzy. Równie groźne może być konsultowanie stanu zdrowia z osobami, które nie mają do tego odpowiednich uprawnień – a zdarza się, że fałszywi eksperci udzielają płatnych porad.

Pamiętaj, że popularność danego „eksperta" nie świadczy o jego kompetencjach – bywa, że szkodliwe profile w internecie gromadzą setki tysięcy obserwujących. Na platformach społecznościowych popularność często wynika z atrakcyjnej formy przekazu, umiejętności wzbudzania emocji i prezentowania sensacyjnych treści, a nie z rzeczywistych kompetencji.

Gdy natrafiasz na profil obserwowany przez tysiące osób, łatwo może być ci założyć, że jego autor to ekspert. Odpowiada za to tzw. efekt społecznego dowodu słuszności, czyli nasza skłonności do uznawania informacji za prawdziwe, jeśli wydają się akceptowane przez wiele innych osób. Tymczasem liczba obserwatorów i reakcji nie zastępuje kwalifikacji, wykształcenia ani dowodów naukowych.

O czym warto pamiętać?

- Nie ufaj obietnicom „cudownego" działania oferowanych produktów i weryfikuj informacje podawane przez sprzedawców.
- W sprawach dotyczących zdrowia zachowaj szczególną ostrożność i nie podejmuj decyzji pod wpływem emocji. Dotyczy to także wyboru i zakupu produktów oraz usług zdrowotnych. Strach, presja czasu czy obietnica szybkiego rozwiązania problemu mogą skłaniać do pochopnych decyzji – zanim coś kupisz lub zastosujesz, daj sobie czas na spokojną ocenę sytuacji.
- Weryfikuj kwalifikacje osób udzielających porad medycznych. To, czy posiadają prawo wykonywania zawodu lekarza, możesz sprawdzić w Centralnym Rejestrze Lekarzy Naczelnej Izby Lekarskiej (rejestr.nil.org.pl). Zwróć uwagę, czy nie widnieje tam adnotacja o jego zawieszeniu lub zrzeczeniu się go.
- Konsultuj się ze specjalistami – w sprawach zdrowia najpewniejszym źródłem informacji jest lekarz lub farmaceuta.

Udostępnianie informacji

Odpowiedzialne korzystanie z platform społecznościowych polega także na tym, by nie przyczyniać się do dalszego rozpowszechniania fałszywych treści. Zanim udostępnisz sensacyjną wiadomość, alarmujący wpis lub reklamę obiecującą spektakularne efekty, sprawdź ich wiarygodność. Zwróć uwagę na to, kim jest autor, poszukaj potwierdzenia informacji w innych rzetelnych źródłach i upewnij się, czy treść nie została już zidentyfikowana jako fałszywa lub wprowadzająca w błąd.

Pamiętaj, że każdym udostępnieniem zwiększasz zasięg publikacji – nawet jeśli robisz to w celu ostrzeżenia innych. W ten sposób możesz nieświadomie przyczynić się do rozpowszechniania fałszywych informacji. Jeśli nie masz pewności co do wiarygodności materiału, nie podawaj go dalej.

Widzisz? Reaguj!

Treści o charakterze dezinformacyjnym możesz zgłosić do Ośrodka Analizy Dezinformacji NASK przez formularz dostępny na stronie zglos-dezinformacje.nask.pl. Możesz zgłaszać je także bezpośrednio administracji platform, na których zostały opublikowane, korzystając z wbudowanych formularzy.

Fałszywe aplikacje zakupowe

Zakupy online pozwalają, za pomocą kilku kliknięć, szybko sfinalizować transakcję. Co więcej, nie trzeba korzystać wyłącznie ze strony internetowej. Wiele firm oferuje dziś wygodne aplikacje mobilne i zachęca klientów do ich zainstalowania, kusząc np. dodatkowym rabatem czy bezpłatną dostawą. Wystarczy smartfon z dostępem do internetu i aplikacja, a cała oferta sklepu jest na wyciągnięcie ręki, nic więc dziwnego, że wiele osób chętnie korzysta z tej formy robienia zakupów. Wiedzą o tym również cyberprzestępcy, którzy tworzą fałszywe aplikacje, często podszywające się pod te udostępniane przez znane marki.



Fałszywa aplikacja, realne zagrożenie

Rozpoznawalna nazwa sklepu, logotyp czy znajoma szata graficzna mogą sprawić, że uznasz aplikację za prawdziwą. Wszystko wygląda wiarygodnie: zdjęcia i opisy produktów, komentarze klientów, promocje. Pozory mogą mylić. Zainstalowanie fałszywej aplikacji może wiązać się z wieloma negatywnymi skutkami.

Przejęcie kontroli

Fałszywa aplikacja może mieć dostęp do wiadomości, kontaktów, kalendarza, zdjęć czy kamery i mikrofonu. Może zainfekować sprzęt złośliwym oprogramowaniem i w ten sposób pozyskiwać dane o urządzeniu i o tobie, a nawet aktywować płatne subskrypcje bez twojej wiedzy – opłaty mogą być naliczane zarówno poprzez płatne wiadomości SMS (SMS Premium), jak i doliczane do rachunku sieci komórkowej. Oszustwo polegające na aktywowaniu płatnych subskrypcji bez wiedzy użytkownika to tzw. *toll fraud*.

Kradzież danych

Podanie danych w fałszywej aplikacji sprawia, że wszystkie wprowadzone tam informacje trafiają w ręce przestępców. Mogą to być dane osobowe, loginy i hasła czy dane kart płatniczych. Uzyskane w ten sposób dane mogą zostać wykorzystane do przejęcia kont, wyłudzeń lub realizacji nieuprawnionych transakcji. Jeśli używasz jednego hasła do kilku kont, pamiętaj, że w przypadku wycieku danych inne konta także są zagrożone.

Utrata pieniędzy

Instalacja fałszywej aplikacji to także poważne ryzyko utraty pieniędzy, zarówno w wyniku działania płatnych subskrypcji, jak i przekazania danych kart płatniczych czy loginów i haseł do bankowości elektronicznej.

Sprawdź, zanim zainstalujesz

Zanim pobierzesz daną aplikację, sprawdź, co dokładnie i z jakiego źródła instalujesz na swoim urządzeniu.

Strona sklepu

Zobacz, czy na oficjalnej stronie sprzedawcy można znaleźć informację o aplikacji dla klientów, oraz czy znajdują się tam odsyłacze do jej pobrania z oficjalnych sklepów Google Play i App Store.

Wydawca aplikacji

Przed instalacją sprawdź, kto jest wydawcą aplikacji. Upewnij się, czy rzeczywiście została udostępniona przez dany sklep albo innego oficjalnego dostawcę.

Oceny i opinie użytkowników aplikacji

Zwróć uwagę na oceny i opinie użytkowników. Porównaj treść komentarzy, datę publikacji i zestaw to z informacjami, które można znaleźć w internecie.

Reklamy

Zachowaj ostrożność, gdy trafiasz na reklamę zachęcającą do instalacji aplikacji. Zawsze weryfikuj źródła i autora, nawet jeśli reklama prowadzi do prawdziwego sklepu z aplikacjami.

Pamiętaj!

Przed pobraniem i instalacją aplikacji warto poświęcić czas na weryfikację jej wiarygodności. Odpowiedz sobie na pytania: skąd o niej wiesz, kto jest jej wydawcą, jakie ma opinie oraz czy zawarta w niej oferta, zdjęcia i opisy produktów nie są wyidealizowane. Cyberprzestępcy mogą wykorzystywać narzędzia AI, by tworzyć atrakcyjne oferty i profesjonalnie wyglądające aplikacje, i niejednokrotnie posługują się nazwami znanych marek i rozpoznawalnymi logotypami. Dlatego ostrożność i weryfikacja są kluczowe.

Oszustwa związane z przesyłkami i śledzeniem paczek



Liczba produktów zamawianych przez internautów przekłada się bezpośrednio na liczbę paczek dostarczanych każdego dnia przez kurierów. Według raportu o stanie rynku pocztowego w 2025 r., wydanego przez Urząd Komunikacji Elektronicznej, w zeszłym roku firmy kurierskie działające na polskim rynku obsłużyły 1,37 miliarda przesyłek[5].

Popularność tej formy dostawy sprawiła, że jest ona często wykorzystywana przez cyberprzestępców jako pretekst do oszustw. Kampanie phishingowe o rzekomych dostawach paczek czy podszywanie się pod firmy kurierskie to częste sposoby działania cyberprzestępców.

Fałszywa przesyłka

Masz 24h na odbiór przesyłki.

Potwierdź dane żeby przesyłka została dostarczona.

Jeśli nie dopłacisz 1,25zł, paczka zostanie zwrócona do nadawcy.

Potwierdź dane, żeby przesyłka została dostarczona. Działania związane z oszustwami „na paczkę”



Fałszywa wiadomość o niewielkiej dopłacie do przesyłki
Nadawca wiadomości próbuje przekonać, że konieczne jest uiszczenie niewielkiego wyrównania opłaty za dostarczenie przesyłki. W przeciwnym razie paczka nie dotrze do celu. Wariantów oszustwa jest wiele, mogą pojawiać się wzmianki o należności za cło, zmianę adresu czy ponowną próbę doręczenia. Deklarowana kwota to zwykle zaledwie kilka złotych.

Tego typu wiadomości zawierają linki przekierowujące na fałszywe strony, po wejściu na które użytkownik zostaje poproszony o podanie danych osobowych i/lub karty płatniczej czy danych logowania do bankowości elektronicznej.



Fałszywa aplikacja
Śledzenie drogi przesyłki to usługa powszechnie oferowana przez firmy kurierskie i przewozowe, dostępna zarówno na ich stronach internetowych, jak i w aplikacjach mobilnych. Przestępcy wykorzystują popularność takich rozwiązań i potrafią je podrabiać. W wysyłanych wiadomościach mogą zachęcać do pobrania rzekomo dedykowanego oprogramowania. W rzeczywistości zainstalowanie niezweryfikowanej aplikacji może skutkować kradzieżą danych lub uzyskaniem przez osoby niepowołane dostępu do twojego urządzenia.



Fałszywy link do śledzenia paczki
Fałszywe wiadomości mogą zawierać też inne elementy, takie jak link, który rzekomo służy do śledzenia paczki. Po jego otwarciu strona często łudząco przypomina znaną witrynę firmy kurierskiej, zawiera rzekomą historię transportu paczki czy status przesyłki. Często po chwili pojawia się komunikat o konieczności potwierdzenia danych lub wniesienia dodatkowej opłaty.



Wiadomość o rzekomym uszkodzeniu paczki
W dobie sztuczne inteligencji łatwo jest wygenerować bardzo realistyczne zdjęcie obrazujące uszkodzenie przesyłki. Oszustwa z tym związane można podzielić na dwie kategorie. Pierwszą z nich jest wysyłanie do adresata zdjęć rzekomo uszkodzonej paczki, w celu skłonienia go do kliknięcia w link zawarty w wiadomości i podania danych osobowych, danych płatniczych lub uiszczenia dodatkowej opłaty, na przykład za ponowną dostawę. Drugą strategią jest podawanie się za niezadowolonego klienta i wysyłanie do firm kurierskich zdjęć obrazujących rzekomo uszkodzoną w trakcie dostawy paczkę, by wyłudzić odszkodowanie.

Sprawdź, zanim będzie za późno

Na co zwracać uwagę?

Weryfikuj otrzymaną informację

Jeśli otrzymasz wiadomość dotyczącą przesyłki, zawsze weryfikuj jej prawdziwość. Sprawdź na oficjalnej stronie przewoźnika, infolinii lub w aplikacji, czy to faktycznie paczka, na którą czekasz.

Uważaj na linki z wiadomości

Wiadomości od oszustów często zawierają linki, które mają rzekomo prowadzić do strony przewoźnika czy służyć do pobierania aplikacji umożliwiającej śledzenie paczki. Jeśli jesteś już na danej stronie, zweryfikuj jej adres i wszystkie zawarte na niej elementy. Nie pobieraj aplikacji z nieznanych źródeł. Nawet przeglądając programy w oficjalnym sklepie, sprawdź kto jest wydawcą aplikacji, jakie ma ona opinie i komentarze.

Chroń dane

Jeśli ktoś prosi o twoje dane osobowe lub o dane twojej karty płatniczej czy login i hasło, potraktuj to jako sygnał ostrzegawczy. Odbiór paczki albo niedopłata to częsty pretekst mający na celu wyłudzenie ważnych informacji.

Nie daj się presji czasu i emocjom

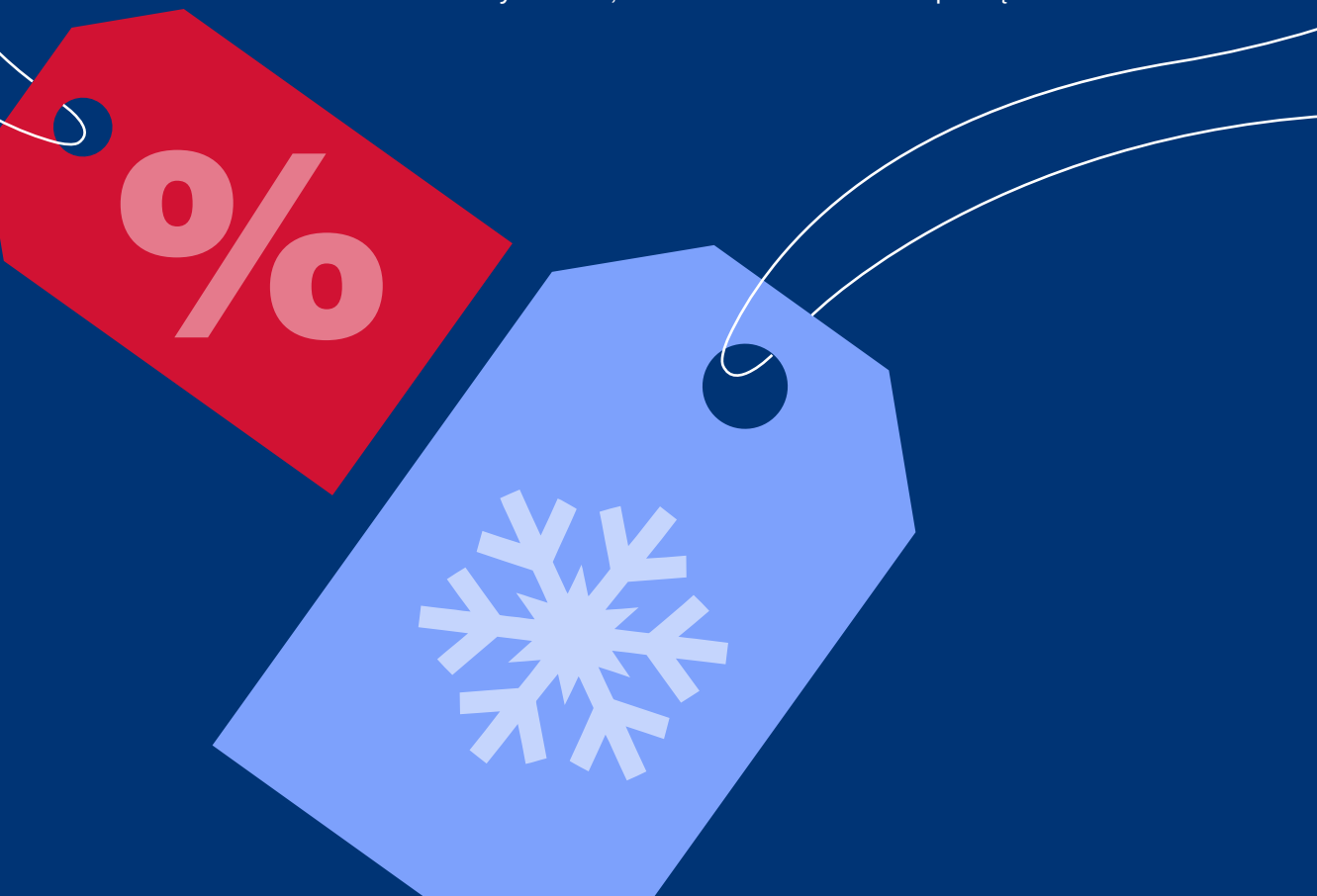
Zwracaj uwagę na komunikaty. Jeśli wiadomość wywołuje poczucie presji czasu bądź silne emocje, np. związane z niedostarczeniem paczki – uważaj, może to być oszustwo!

Przyglądaj się zdjęciom i dokumentom

Z pozoru realistycznie wyglądające zdjęcia przesyłki mogą okazać się wygenerowane za pośrednictwem sztucznej inteligencji. Zawsze weryfikuj otrzymany obraz: przyjrzyj się, czy nie ma na nim znaków wodnych, które są dodawane automatycznie przy generowaniu zdjęć, sprawdź metadane lub skorzystaj z ogólnodostępnych detektorów AI.

Sklepy sezonowe

Jak w „Porach roku” Vivaldiego zmienia się krajobraz cyberzagrożeń. Przestępcy bardzo chętnie nawiązują do sezonowych motywów, bieżących wydarzeń, popularnych tekstów kultury i wszelkich innych treści, które w danym okresie są interesujące dla użytkowników internetu. Wszystko po to, by przykuć twoją uwagę, uśpić czujność i wyłudzić to, co chcesz chronić – dane i pieniądze.





Źródło: CERT Polska/CSIRT NASK

Co roku, gdy nadchodzi zima, oszuści zalewają polski internet ofertami fałszywych sklepów z opałem. Węgiel, koks, ekogroszek – produkt nie ma znaczenia. Liczy się fakt dotarcia do odbiorcy, a to ułatwiają reklamy, które przestępcy masowo wykupują na platformach społecznościowych. Gdy algorytm profilujący użytkownika uzyska informację, że ten poszukuje opału na zimę, podsuwa mu takich ofert coraz więcej.

Jak rozpoznać fałszywą reklamę?

Z każdym rokiem jest to coraz trudniejsze. Oszuści weryfikują, jaki typ reklam przynosi im największe korzyści, skwapliwie wykorzystują również rosnące możliwości AI. Wygenerowanie interaktywnej strony sklepu (często wzorowanej na prawdziwej witrynie dystrybutora opału) zajmuje bardzo niewiele czasu. Przestępcy jednak często popełniają w tym procesie błędy, więc uważność może cię uchronić przed własną pomyłką. Dlatego zawsze przed zakupem zwróć uwagę na kilka czynników.

https://

Adres strony
Szczególnie w przypadku lokalnych dystrybutorów opału może zdarzyć się, że to fałszywa strona wyświetli się pierwsza w wynikach wyszukiwania. Jeśli widzisz kilka możliwości, warto zweryfikować je np. telefonicznie lub prewencyjnie zgłosić podejrzenie oszustwa do zespołu CERT Polska.

Polityka prywatności
Obecność i poprawność tej polityki sama w sobie nie świadczy jeszcze o rzetelności strony, ale jej brak powinien wzbudzać niepokój.

Dane sprzedawcy
Często zdarza się, że przestępcy świadomie kopiują prawdziwe dane istniejącej firmy. Dlatego wszystko, co wyświetla się na stronie, należy traktować z ograniczonym zaufaniem.



Dostępne metody płatności
W przypadku niektórych fałszywych sklepów dostępna bywa także metoda płatności kartami podarunkowymi (np. PaySafeCard). To jedna z ulubionych metod przestępców i choć jej obecność nie przesądza o tym, że strona jest nierzetelna, na pewno powinna wzbudzać czujność. Szczególnie, gdy do jej wykorzystania namawia „konsultant" lub za skorzystanie z niej jest oferowana dodatkowa promocja.



Opinie innych kupujących
Czasami warto wykorzystać media społecznościowe. Często gromadzą się tam osoby poszkodowane przez oszustów, więc wpisanie nazwy fałszywego sklepu może ujawnić grupę, która demaskuje proceder i np. organizuje pozew zbiorowy wobec właściciela-oszusta. Brak takich grup nie oznacza, że sklep jest rzetelny, ale jeśli istnieją, to lepiej uczyć się na cudzych błędach.



Ceny
Zbyt dobre okazje mogą szybko okazać się pułapką, która nieoczekiwanie pochłonie twoje oszczędności.



Presja czasu
Czasem 5 minut namysłu może uratować oszczędności życia – warto podejmować decyzje powoli.

Oszuści bardzo chętnie wykorzystują również inne tematy – niedawno w CERT Polska ostrzegaliśmy przed fałszywymi promocjami na paliwo, głośno było także o dystrybucji szkodliwego oprogramowania pod pozorem dostępu do nowej gry komputerowej. Wszelkie podejrzane treści w internecie możesz zgłaszać do zespołu CERT Polska za pomocą formularza na stronie incydent.cert.pl, w aplikacji mObywatel (usługa Bezpiecznie w sieci) lub – w przypadku fałszywych SMS-ów – przekazując je bez zmian pod darmowy numer 8080. Warto to robić również w przypadku, gdy samodzielnie rozpoznasz oszustwo, bo dzięki temu pomagasz chronić innych użytkowników internetu.

Co zrobić, gdy zakup został już opłacony?

Jeśli zamówiony produkt nie dotarł lub istnieje podejrzenie, że dane trafiły w ręce oszustów, jak najszybciej skontaktuj się z bankiem, aby ustalić możliwe sposoby działania. Im szybsza będzie twoja reakcja, tym większa szansa na odzyskanie pieniędzy. Podejrzenie przestępstwa warto zgłosić również na policję.

Zachęcamy, by link do fałszywego sklepu wysłać do zespołu CERT Polska, przez stronę incydent.cert.pl lub za pośrednictwem aplikacji mObywatel 2.0.

Warto także ostrzegać innych przed oszustwem, zostawiając wpisy w serwisach z opiniami czy na platformach społecznościowych.

Oznaczanie treści wygenerowanych przy pomocy AI – prawo i zagrożenia

Sztuczna inteligencja jest coraz częściej wykorzystywana w sprzedaży do tworzenia opisów, zdjęć, filmów czy rekomendacji i jako podstawa działania chatbotów odpowiadających na pytania klientów. Problem pojawia się jednak wtedy, gdy nie wiemy, że mamy do czynienia z treścią wygenerowaną lub zmodyfikowaną przez AI, a dany materiał wpływa na naszą decyzję zakupową. Ma to szczególne znaczenie w handlu internetowym, gdzie oceniamy produkty głównie na podstawie zdjęć, opisów, opinii i rekomendacji. Jeśli treści te zostały wygenerowane lub istotnie zmienione przez AI, mogą nie odzwierciedlać rzeczywistości.

Co na to prawo?

Najważniejszym unijnym aktem dotyczącym sztucznej inteligencji jest AI Act, czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689. Przepisy określają obowiązki dotyczące przejrzystości korzystania ze sztucznej inteligencji. Szczególnie ważny jest tutaj art. 50.

> Artykuł 50 unijnego Aktu w sprawie sztucznej inteligencji (AI Act) reguluje obowiązki w zakresie przejrzystości dla dostawców oraz podmiotów stosujących niektóre systemy AI.

W uproszczeniu chodzi o to, aby w określonych sytuacjach było dla ciebie jasne, że masz do czynienia z AI albo z materiałem sztucznie wygenerowanym lub zmodyfikowanym. Są to np. sytuacje, w których kontaktujesz się z chatbotami obsługującymi klientów, wirtualnymi asystentami, systemami prowadzącymi rozmowy głosowe czy narzędziami generującymi odpowiedzi na pytania. Jeżeli komunikujesz się z systemem sztucznej inteligencji, stosujące go podmioty powinny cię o tym poinformować, chyba że jest to dla ciebie oczywiste i jasno wynika z okoliczności. Szczególne wymagania dotyczą także tzw. deepfake'ów, czyli obrazów, nagrań audio lub filmów wygenerowanych albo zmienionych przez AI w taki sposób, że mogą sprawiać wrażenie autentycznych. Muszą one być opatrzone informacją o użyciu sztucznej inteligencji. Informacja ta powinna być jasna, widoczna i łatwa do odnalezienia. Twórca materiału nie może zmuszać cię do szukania jej w regulaminie, przypisach lub trudno dostępnych sekcjach strony internetowej. Celem tych wymogów jest umożliwienie ci rozpoznawania treści generowanych przez AI, świadomej oceny ich wiarygodność i przemyślanych decyzji zakupowych.

Czy każda treść stworzona przy pomocy AI musi być oznaczona?

Nie. To jeden z najważniejszych aspektów nowych przepisów, które trzeba podkreślić. Sam fakt, że firma wykorzystała sztuczną inteligencję, nie oznacza automatycznie, że przy każdym zdjęciu, tekście czy reklamie musi pojawić się wielki napis „wygenerowane przez AI".

Znaczenie ma przede wszystkim to, do czego AI została wykorzystane i jak bardzo zmieniło materiał, oraz czy ingerencja technologii może wpłynąć na ocenę autentyczności materiału przez odbiorcę. Jeżeli AI została użyta wyłącznie do technicznej obróbki zdjęcia, np. redukcji szumów, poprawienia oświetlenia, korekty kolorów, zmiany rozmiaru albo konwersji formatu, to nie ma obowiązku oznaczania takiego użycia. Informacja powinna pojawić się wtedy, gdy algorytm dodaje do zdjęcia elementy, których pierwotnie na nim nie było, zmienia cechy produktu albo tworzy realistyczną scenę, która nigdy nie miała miejsca.

Dla odbiorców kluczowe jest to, czy AI jedynie poprawia jakość materiału, czy też zmienia jego treść. Różnica jest istotna: czym innym jest poprawienie jakości zdjęcia kanapy, a czym wygenerowanie widoku luksusowego salonu i takie przedstawienia mebla, że wydaje się on większy, solidniejszy i wykonany z lepszego materiału i ogółem wygląda znacznie lepiej niż w rzeczywistości. Warto dodać, że wykorzystanie sztucznej inteligencji i oznaczenie tego faktu nie sprawia, że przedsiębiorca może uchylać się od odpowiedzialności za rzetelność przekazu. Nawet oznaczenie treści jako wygenerowanej przez AI nie usprawiedliwia wprowadzania klientów w błąd ani prezentowania oferty w sposób zniekształcający rzeczywisty obraz produktu.

Czy da się rozpoznać treść stworzoną przez AI?

Czasami jeszcze tak, ale coraz częściej – nie. Dziwne szczegóły na zdjęciu, nienaturalny głos, powtarzające się sformułowania lub brak źródeł mogą wzbudzić podejrzenia. Nie należy jednak zakładać, że zawsze uda się „wyłapać AI" na podstawie błędów w materiale. Technologia szybko się rozwija, a wygenerowane materiały są coraz bardziej realistyczne. **Najważniejsza zasada brzmi: nie pytaj tylko „czy to AI?", ale „czy mogę temu zaufać?".** W czasach generatywnej AI zasada „widzę, więc wierzę" przestaje być bezpieczna.

Sztuczna inteligencja może ułatwiać zakupy i dostęp do informacji, jednak jej wykorzystanie powinno być transparentne. Oznaczanie treści wygenerowanych lub zmodyfikowanych przez AI pomaga konsumentom świadomie oceniać prezentowane materiały. Jednocześnie cały czas kluczowe znaczenie ma zachowanie ostrożności i krytyczna analiza informacji przed podjęciem decyzji zakupowej.

Komentarze eksperckie dotyczące ochrony konsumentów

Świadomość zagrożeń ze strony cyberprzestępców stanowi jeden z głównych czynników wpływających na szeroko rozumiane bezpieczeństwo użytkowników. Drugi ważny aspekt to sposoby instytucjonalnej ochrony internautów. Uważność w osobistym korzystaniu z sieci powinna być połączona z wiedzą na temat działań różnych instytucji, które wspierają nas i dbają o nasze prawa na rynku e-commerce. W tej części poradnika eksperci z Centralnego Biura Zwalczania Cyberprzestępczości, biura Rzecznika Finansowego, Miejskiego Rzecznika Konsumentów, Europejskiego Centrum Konsumenckiego oraz Urzędu Ochrony Konkurencji i Konsumentów dzielą się wskazówkami, dzięki którym możemy skuteczniej dbać o swoje prawa jako konsumenci, a wedle potrzeby – wiedzieć, gdzie szukać pomocy.

Centralne Biuro Zwalczania Cyberprzestępczości

st. asp. Monika Przestrzelska
p.o. Rzecznika Prasowego Komendanta CBZC

Cyberprzestępczość stanowi jedno z największych i najszybciej rozwijających się zagrożeń dla bezpieczeństwa obywateli naszego kraju. Dlatego bardzo istotne jest, by śledzić aktualne zagrożenia w sieci. Warto pamiętać, że świadomy użytkownik cyberprzestrzeni ma duże szanse na to, że uniknie zagrożenia i nie da się oszukać.

Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) realizuje działania profilaktyczne ukierunkowane na zwiększenie świadomości, a co za tym idzie – bezpieczeństwa użytkowników sieci. W 17 Zarządach CBZC – po jednym w każdym województwie – służą funkcjonariusze, którzy na co dzień zajmują się cyberprofilaktyką. Jednak Biuro zwalcza przestępczość w internecie przede wszystkim poprzez wykrywanie, zapobieganie oraz ściganie sprawców przestępstw, a także wspiera w tym zakresie inne jednostki.

Konsekwencje nieuwagi podczas robienia zakupów online mogą być poważne – od utraty pieniędzy wskutek płatności za towar, który nie istnieje, po kradzież danych karty i związane z tym dalsze nieautoryzowane transakcje. W skrajnych przypadkach dochodzi nawet do kradzieży tożsamości. CBZC ma na swoim koncie wiele akcji, które poskutkowały wykryciem i zatrzymaniem osób zamieszczających w internecie fałszywe ogłoszenia sprzedażowe (na przykład prowadząc fikcyjne sklepy).

Przykłady:

luty 2026

Zatrzymano 12 osób podejrzanych o oszustwa pod pozorem sprzedaży różnych towarów w sieci. Sprawcy zakładali fałszywe sklepy internetowe i umieszczali oferty na jednym z popularnych serwisów aukcyjnych. Proceder odbywał się na szeroką skalę. Ustalono, że takich zakupów mogło dokonać ponad 1100 osób, a łączna suma strat wyniosła ok. 3 mln złotych.

(https://cbzc.policja.gov.pl/bzc/aktualnosci/807,26-zarzutow-karnych-cyberprzestepcy--zamieszczali-falszywe-ogloszenia-na-popularn.html)

czerwiec 2026

Zatrzymano ponad 20 osób podejrzanych o sprzedaż nieistniejącego towaru na fałszywych stronach sprzedażowych. Oszuści „sprzedawali" m.in. opał i elektronarzędzia. Wykorzystywane przez sprawców witryny łudząco przypominały prawdziwe sklepy internetowe i zachęcały atrakcyjną ceną. By klienci nie podejrzewali oszustwa, na stronie zamieszczono dane kontaktowe do sprzedawcy. Niestety oszuści stosowali podszywanie i podane przez nich dane należały do innego, prawdziwego sprzedawcy. Po złożeniu zamówienia i dokonaniu opłaty ofiary otrzymywały potwierdzenie zakupu na wskazany adres e-mail, co tym bardziej utwierdzało je w przekonaniu, że wszystko jest w porządku. Jednak gdy czas oczekiwania na otrzymanie przesyłki niepokojąco się wydłużał, kupujący nabierali podejrzeń i starali się kontaktować ze sprzedawcą telefonicznie. W tym momencie odkrywali, że doszło do oszustwa. Straty, jakie łącznie poniosły ofiary, to ponad 16,3 tys. złotych. Oszukano ponad 440 osób.

(https://cbzc.policja.gov.pl/bzc/aktualnosci/965,Zarabiali-na-fikcyjnych-sklepach-internetowych-oszukali-w-ten-sposob-ponad-440-o.html)

sierpień 2026

Zatrzymano 28-letniego mężczyznę podejrzanego o prowadzenie nielegalnego sklepu internetowego. Mężczyzna zajmował się sprzedażą wyrobów akcyzowych. Działał za pośrednictwem szyfrowanych komunikatorów oraz portali społecznościowych. Zabezpieczono wtedy około 12,5 tys. sztuk waporyzatorów bez wymaganych znaków akcyzy. Straty, jakie poniósłby Skarb Państwa, gdyby zabezpieczony towar trafił do obrotu, oszacowano na blisko 1,7 mln złotych.

(https://cbzc.policja.gov.pl/bzc/aktualnosci/1006,Nielegalny-sklep-internetowy-zlikwidowany-przez-CBZC-i-KAS.html)

Podane przykłady pochodzą tylko z ostatnich miesięcy. CBZC ujawnia i likwiduje o wiele więcej takich fikcyjnych sklepów internetowych. Często jest to bardzo żmudna, trudna, wielomiesięczna praca, ale dla funkcjonariuszy najważniejsze jest to, że przynosi efekty.

Pamiętaj!

Jeśli padniesz ofiarą oszusta, zawiadomienie o tym przyjmie policjant w najbliższej jednostce Policji – nie musisz specjalnie szukać Zarządu CBZC. Warto jednak odpowiednio przygotować się do zgłoszenia; w miarę możliwości zabezpiecz dane sklepu i wydruki z korespondencji bądź zrzuty ekranu, które mogą usprawnić i przyspieszyć działania policjantów.

Zakupy robione przez internet wymagają zachowania rozsądku i ostrożności, dlatego zawsze warto dać sobie chwilę, by zweryfikować najważniejsze informacje. Bądź krok przed oszustami – nie daj się oszukać!

Rzecznik Finansowy

dr Anna Mlostoń-Olszewska,
Radca prawny, Pełnomocnik Terenowy Rzecznika Finansowego w Łodzi

Co może zrobić klient, który zapłacił kartą za zakupy w internecie, ale nie otrzymał zamówionego towaru? Pomocna może być procedura chargeback. Pokazuje to sprawa kupującego, który zwrócił się o pomoc do Rzecznika Finansowego.

Do Rzecznika Finansowego zgłosił się klient, który zamówił biżuterię w sklepie internetowym. Mimo informacji, że produkt jest dostępny w magazynie, przesyłka nie dotarła na czas. Sprzedawca wyjaśnił, że doszło do opóźnienia logistycznego, ale nie podał nowego terminu dostawy.

Klient zwrócił się więc do swojego banku o zwrot pieniędzy w ramach tzw. chargebacku. Bank przyjął zgłoszenie, ale po otrzymaniu wyjaśnień sprzedawcy odmówił zwrotu środków. Uznał, że transakcja przebiegła prawidłowo, a zamawiający otrzymał towar. W rzeczywistości zamówienie do niego nie dotarło.

Klient nie zgodził się ze stanowiskiem banku i zwrócił się o pomoc do Rzecznika Finansowego. Po przeanalizowaniu sprawy eksperci Rzecznika podjęli interwencję. W jej wyniku klient odzyskał pieniądze w ramach chargebacku.

Zamówiłeś/zamówiłaś towar w internecie, ale sklep go nie dostarczył? Odesłałeś/odesłałaś zakupiony produkt, ale sprzedawca nie zwrócił ci pieniędzy? A może odwołano lot lub inną opłaconą już przez ciebie usługę? Jeżeli płatność została dokonana kartą, w takiej sytuacji może pomóc chargeback. To procedura, dzięki której można dochodzić zwrotu pieniędzy za określone transakcje bezgotówkowe.

Chargeback: co to właściwie jest?

Chargeback, czyli obciążenie zwrotne, to procedura oferowana przez organizacje płatnicze, takie jak Visa i Mastercard. **Dotyczy płatności kartą debetową, kredytową lub inną kartą płatniczą.** Może pomóc w odzyskaniu pieniędzy, gdy zapłaciłeś/zapłaciłaś kartą, ale sprzedawca albo usługodawca nie wywiązał się z umowy, na przykład nie dostarczył towaru albo nie zwrócił pieniędzy po anulowaniu zakupu towaru lub usługi.

Jeżeli twój zakup został opłacony zwykłym przelewem, gotówką lub kodem płatności mobilnych, chargeback nie będzie właściwą procedurą. Inaczej może być w przypadku płatności przez internetową bramkę płatniczą. Znaczenie ma to, czy ostatecznie została obciążona karta. Warto więc sprawdzić historię rachunku. Jeśli nie masz pewności, jak została rozliczona płatność, możesz zapytać o to bank.

Możliwość przeprowadzenia procedury chargeback nie wynika wprost z przepisów prawa. Jej zasady określają organizacje płatnicze, a zwrot środków jest realizowany za pośrednictwem banku, który wydał konkretną kartę.

Kiedy chargeback może pomóc?

O chargeback można zwrócić się do banku między innymi wtedy, gdy:

- zapłaciliśmy za towar, ale go nie otrzymaliśmy;
- odesłaliśmy towar, ale sklep nie zwrócił pieniędzy;
- otrzymaliśmy produkt uszkodzony lub istotnie niezgodny z opisem;
- zapłaciliśmy za usługę, która nie została wykonana;
- odwołano lot lub inną usługę, za którą zapłaciliśmy kartą, a nie otrzymaliśmy należnego zwrotu;
- sprzedawca zakończył działalność lub ogłosił upadłość, nie dostarczając opłaconego towaru albo usługi;
- karta została obciążona dwukrotnie za tę samą transakcję;
- pobrano inną kwotę niż ta, którą zaakceptowaliśmy;
- mimo anulowania subskrypcji z naszego konta nadal pobierana jest cykliczna opłata.

Każda sprawa jest oceniana indywidualnie, zgodnie z zasadami właściwej organizacji płatniczej.

Jak skorzystać z chargebacku?

W pierwszej kolejności złóż reklamację u sprzedawcy lub usługodawcy. Krótko opisz problem i wskaż, czego oczekujesz, na przykład dostarczenia towaru albo zwrotu pieniędzy.

Próba rozwiązania sporu bezpośrednio ze sprzedawcą jest istotna. Może być również wymagana do rozpoczęcia procedury chargeback.

Zachowaj przy tym całą dokumentację:

- potwierdzenie zamówienia,
- potwierdzenie płatności kartą,
- opis produktu lub usługi i regulamin zakupu,
- korespondencję ze sprzedawcą lub usługodawcą,
- złożoną reklamację i odpowiedź sprzedawcy lub usługodawcy,
- potwierdzenie zwrotu lub nadania przesyłki,
- informację o anulowaniu usługi lub odwołaniu lotu,
- zdjęcia uszkodzonego albo niezgodnego z opisem produktu,
- wyciąg lub historię rachunku pokazującą obciążenie karty.

Jeśli oferta zniknęła ze strony internetowej, przydatny może być również zapis lub zrzut ekranu przedstawiający jej treść.

Jeżeli sprzedawca odmówi spełnienia zgłoszonych roszczeń, nie odpowie albo nie zwróci pieniędzy w uzgodnionym terminie, nie czekaj – **jak najszybciej skontaktuj się z bankiem**, który wydał kartę, i zgłoś chęć skorzystania z procedury chargeback.

Pamiętaj!

W ramach procedur organizacji płatniczych obowiązują określone terminy graniczne na dokonanie zgłoszenia, które mogą zależeć od jego przyczyny, rodzaju transakcji oraz momentu, w którym towar lub usługa miały zostać dostarczone.

Najlepiej od razu zapytaj swój bank:

- jaki termin obowiązuje w danej sprawie;
- jakie dokumenty trzeba dostarczyć;
- czy zgłoszenie wymaga wypełnienia formularza;
- czy bank pobiera opłatę związaną z jego rozpatrzeniem.

Jak przebiega procedura?

1. Klient zgłasza bankowi problem dotyczący konkretnej transakcji kartą.
2. Bank sprawdza zgłoszenie i przekazane dokumenty.
3. Jeżeli spełnione są warunki procedury, bank kieruje sprawę dalej w ramach właściwej organizacji płatniczej.

4. Sprzedawca może przedstawić swoje stanowisko i dokumenty, na przykład dowód dostarczenia towaru.

5. Po analizie sprawy klient otrzymuje informację o wyniku.

Jeżeli zgłoszenie zostanie uwzględnione, pieniądze są zwracane. Jeżeli sprzedawca wykaże, że prawidłowo wykonał umowę, wniosek o chargeback może zostać odrzucony.

Co zrobić, gdy bank odmówi?

Jeżeli bank odmówi uruchomienia procedury rozpatrywania chargebacku albo zgłoszenie zakończy się odmową zwrotu pieniędzy, poproś o wyjaśnienie przyczyn. Złóż do banku reklamację. Opisz prostymi słowami:

- czego dotyczyła transakcja;
- co zrobił lub czego nie zrobił sprzedawca lub usługodawca;
- kiedy zwróciłeś/zwróciłaś się do banku;
- dlaczego nie zgadzasz się ze stanowiskiem banku;
- czego oczekujesz.

Jeżeli bank odrzuci reklamację, możesz zwrócić się po pomoc do Rzecznika Finansowego.

Jak Rzecznik Finansowy może pomóc w sprawie chargebacku?

Rzecznik Finansowy jest państwową instytucją, która pomaga klientom w sporach z podmiotami rynku finansowego, w tym m.in. z bankami. W sprawie dotyczącej chargebacku eksperci Rzecznika Finansowego mogą przeanalizować, czy bank prawidłowo rozpatrzył zgłoszenie i reklamację oraz czy odpowiednio uzasadnił swoje stanowisko. W ramach postępowania interwencyjnego Rzecznik może wystąpić do banku o wyjaśnienia i przedstawić argumentację przemawiającą za ponowną analizą sprawy.

Rzecznik Finansowy nie prowadzi procedury chargeback i nie może nakazać organizacji płatniczej zwrotu pieniędzy. Może jednak ocenić sposób działania banku i pomóc

klientowi, który sam nie jest w stanie przeanalizować skomplikowanych zasad lub uzasadnienia odmowy.

Rzecznik Finansowy – nie tylko chargeback

Chargeback to tylko jeden z wielu problemów, z którymi można zwrócić się do Rzecznika Finansowego. Zakres jego działalności obejmuje nie tylko kwestie obsługi klientów przez banki, ale także m.in. przez firmy ubezpieczeniowe i pożyczkowe czy towarzystwa emerytalne. Działania Rzecznika Finansowego obejmują udzielanie porad, prowadzenie postępowań interwencyjnych i polubownych, a w określonych przypadkach także pomoc na etapie postępowania sądowego. Pomoc prawna udzielana przez ekspertów Biura Rzecznika Finansowego jest bezpłatna.

Każdego dnia pomagamy konsumentom w sporach z bankami, ubezpieczycielami i innymi podmiotami rynku finansowego. Wiele osób zakłada, że odmowna odpowiedź na złożoną reklamację kończy sprawę. Nie zawsze tak jest. Jeżeli nie zgadzasz się ze stanowiskiem instytucji finansowej albo nie rozumiesz powodów odmowy, warto skorzystać z pomocy Rzecznika Finansowego. Nasi eksperci mogą przeanalizować sprawę i ocenić, czy stanowisko banku jest prawidłowe.

Miejski Rzecznik Konsumentów

Paweł Rodziewicz,
Miejski Rzecznik Konsumentów

Konsumentka przez kilka tygodni obserwowała profil sprzedawcy „La Butik" w serwisie społecznościowym Twarzokajet.pl. Z treści zamieszczanych na tym profilu wynikało, że prowadzi go przedsiębiorca posiadający sklep stacjonarny o tej samej nazwie, który znajduje się w sąsiednim mieście. Za pośrednictwem platformy właściciel sklepu udostępniał swoją ofertę i organizował transmisje na żywo, podczas których atrakcyjna pani prezentowała towary i zachęcała do ich kupna w promocyjnych cenach. Po obejrzeniu jednego z takich materiałów skontaktowała się za pomocą komunikatora z administratorem profilu „La Butik" i wyraziła chęć zakupienia kilku elementów garderoby. Uzgodniła cenę, formę płatności oraz sposób dostawy towaru. Żądaną kwotę uiściła BLIK-iem na wskazany numer telefonu. Nie uzgodniła jednak terminu dostawy. Po upływie tygodnia skontaktowała się ze sprzedawcą i poinformowała, że nie otrzymała jeszcze zamówionych rzeczy. Sprzedawca zapewnił, że ma małe opóźnienie i w przeciągu dwóch dni wyśle paczkę. Minął kolejny tydzień i straciła cierpliwość. Napisała do sprzedawcy wiadomość o treści: „Jesteście oszustami. Oddajcie mi moje pieniądze. Inaczej oddam sprawę na Policję i opiszę w internecie". W odpowiedzi otrzymała wiadomość o treści: „Paczka już jest w drodze". W opisie profilu „La Butik" znajdował się adres i numer telefonu do sprzedawcy. Konsumentka zadzwoniła pod ten numer i poinformowała, że odstępuje od umowy i nie ma zamiaru odbierać przesyłki. W odpowiedzi usłyszała, że nie może odstąpić od umowy przed otrzymaniem zamówionych ubrań, a na ich dostarczenie sprzedawca ma 30 dni. Kilka dni później odebrała przesyłkę od kuriera. Po jej rozpakowaniu obejrzała dokładnie zawartość i przymierzyła odzież. Ubrania nie przypadły jej do gustu, więc odesłała paczkę do sprzedawcy. Czekała na zwrot pieniędzy, jednak w ciągu kolejnych dwóch tygodni nie odnotowała żadnego wpływu na swoim koncie. Zasięgnęła opinii w internecie i wystosowała wezwanie do zapłaty. W odpowiedzi otrzymała pismo, w którym sprzedawca odmówił zwrotu pieniędzy, powołując się na art. 38 ust. 1 pkt 5 ustawy o prawach konsumenta i jako powód podał rozerwanie foliowych worków, w które odzież była zapakowana w celach higienicznych. Po otrzymaniu tej wiadomości rozeźlona udała się po pomoc do rzecznika konsumentów.

Działania podjęte przez rzecznika konsumentów

Porada prawna

Konsumentka została zaproszona na poradę prawną do biura rzecznika. [art. 42 ust. 1 pkt 1 u.o.k.i.k.]

W pierwszej kolejności rzecznik zweryfikował, czy zamieszkuje ona na terenie obejmującym funkcjonowanie samorządu, przez który jest zatrudniony. [art. 39 u.o.k.i.k.]

Następnie rzecznik zbadał status sprzedawcy pod kątem tego, czy prowadzi on działalność gospodarczą w zakresie obejmującym zawieranie umów sprzedaży odzieży, aby móc stwierdzić, czy strony łączy stosunek o charakterze konsumenckim. Paczka, w której sprzedawca dostarczył zakupiony towar, nie zawierała paragonu ani innego dokumentu fiskalnego, który określałby dane sprzedawcy. Profil „La Butik" zawierał dane (adres i numer telefonu) oraz asortyment tożsamy z działalnością gospodarczą widniejącą w rejestrze. [art. 431 k.c., art. 22^1 k.c., art. 62 k.k.s.]

Po dokładnym zweryfikowaniu właściwości miejscowej i rzeczowej rzecznik przeszedł do analizy okoliczności towarzyszących zawarciu umowy. Jego wątpliwości nie budził fakt, że umowa sprzedaży została skutecznie zawarta za pośrednictwem komunikatora internetowego. Z tego powodu zakwalifikował ją jako umowę zawartą na odległość. Na profilu „La Butik" sprzedawca nie zamieścił jednak żadnych dodatkowych informacji. Tymczasem na przedsiębiorcę zawierającego umowy na odległość ustawa o prawach konsumenta nakłada bardzo obszerny obowiązek informacyjny, który zazwyczaj realizowany jest poprzez wskazanie wymaganych informacji w regulaminie sklepu. [art. 2 pkt 1 u.p.k., art. 12 u.p.k.]

Konsumentka została poinformowana, że zawieranie umów na odległość z przedsiębiorcą, który nie dochowuje obowiązku informacyjnego, jest bardzo ryzykowne.

Zawierając umowę sprzedaży, sprzedawca zobowiązuje się przenieść na kupującego własność rzeczy i wydać mu rzecz, a kupujący zobowiązuje się zapłacić cenę. W przypadku, gdy termin wydania zakupionej rzeczy nie został wskazany w treści umowy (lub w regulaminie), towar powinien zostać wydany niezwłocznie, nie później niż w terminie 30 dni. [art. 535 k.c., art. 543^1 k.c.]

Rzecznik zwrócił konsumentce uwagę, aby w swoich opiniach unikała obraźliwych określeń lub oskarżeń, takich jak: „oszuści", „złodzieje" itp., ponieważ może to narazić ją na odpowiedzialność karną lub cywilnoprawną. Prawo do wyrażania opinii na temat towaru, sprzedawcy oraz sposobu obsługi klienta jest jednym z podstawowych praw konsumenta,

jednak trzeba uważać, aby tego prawa nie nadużyć i nie naruszyć praw przysługujących innym. [art.24 k.c., art. 212 k.k.]

Następnie rzecznik przeanalizował formę i treść oświadczenia, na podstawie którego konsumentka twierdziła, że odstąpiła od zawartej umowy. [art. 27–30 u.p.k.]

Od umowy sprzedaży zawartej na odległość oraz poza lokalem przedsiębiorstwa konsument może, w większości przypadków, odstąpić w ciągu 14 dni od dnia otrzymania towaru. Korzysta wtedy z tzw. prawa do namysłu, o którym mowa w art. 27 ustawy o prawach konsumenta. Przepis ten nie wskazuje jednak od kiedy uprawnienie to przysługuje, a jedynie moment, względem którego wyznaczany jest termin jego realizacji. Z pomocą przychodzi treść Dyrektywy Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów. Polskie przepisy dotyczące ochrony praw konsumenta powstały na skutek implementacji tej dyrektywy, zatem zarówno ich treść, jak i wykładnia nie mogą zapewniać konsumentowi ochrony gorszej, niż określają to przepisy unijne. Zgodnie z pkt 40 preambuły do dyrektywy konsument powinien mieć możliwość skorzystania z prawa do odstąpienia od umowy przed wejściem w fizyczne posiadanie towarów. Z powyższego można wywnioskować, że art. 27 ustawy o prawach konsumenta należy traktować jako określenie terminu dotyczącego wygaśnięcia uprawnienia do zwrotu konsumenckiego, a nie okres, w którym uprawnienie istnieje i może zostać wykonane.

> Twierdzenie, że konsument nie może odstąpić od umowy przed otrzymaniem zakupionej rzeczy, jest nieprawdziwe i przekazywanie takiej informacji przez przedsiębiorcę może być uznane za nieuczciwą praktykę rynkową. [art. 5 ust. 3 pkt 4 u.p.n.p.r.]

Należy z całą stanowczością stwierdzić, że konsumentka nie uchybiła terminowi do złożenia oświadczenia o odstąpieniu od umowy zawartej na odległość. Przedsiębiorca zatem wprowadził ją w błąd w tym zakresie. Jednakże oświadczenie takie nie powinno być składane ustnie. Najlepiej jest złożyć je na piśmie bądź na innym trwałym nośniku. W przeciwnym razie ciężko będzie ten fakt udowodnić. Wzywanie do spełnienia roszczenia, którego wymagalność opieramy na okoliczności, której nie możemy udowodnić, nie spełni swojej funkcji.

Warto wspomnieć, że przedsiębiorca nie dochował obowiązku informacyjnego w zakresie, który obejmuje również udzielenie informacji na temat możliwości odstąpienia od umowy zawartej na odległość. Skutkuje to wydłużeniem okresu, w którym konsument może złożyć takie oświadczenie o 12 miesięcy. Gdyby przedsiębiorca nie ustosunkował

się do oświadczenia konsumentki, rzecznik zasugerowałby ponowne złożenie oświadczenia na piśmie. Wtedy termin zostałby dochowany. [art. 29 u.p.k.]

Przedsiębiorca odpowiedział jednak na oświadczenie konsumentki. Powołując się na art. 38 pkt 5 ustawy o prawach konsumenta, odmówił zwrotu kwoty zapłaconej za towar. Sprzedawca internetowy ma prawo odmówić zwrotu pieniędzy w kilku przypadkach, m.in. powołując się na względy higieniczne. Ten wyjątek dotyczy towarów dostarczanych w zapieczętowanym opakowaniu ze względów higienicznych. Odnosi się on jednak do produktów, których ponowne użycie po otwarciu jest absolutnie niemożliwe ze względów medycznych lub sanitarnych. Takimi towarami są np. szczoteczki do zębów, kosmetyki, hermetycznie zapakowana bielizna. Konsumentka zamówiła dwie sukienki, spodnie, bluzkę i koszulę. Każda z rzeczy zapakowana była w foliowy worek zabezpieczony klejem. Z tego faktu nie można wywodzić, że opakowanie to spełniało szczególną funkcję ze względu na ochronę zdrowia. [art. 38 u.p.k.]

Uprawnienie do odstąpienia od umowy zawartej na odległość nazywamy również prawem do zapoznania się z rzeczą. Realizacją tego prawa jest sytuacja, w której konsument może korzystać z rzeczy w zakresie analogicznym do tego, w jakim mógłby to zrobić, zapoznając się z towarem wystawionym na sprzedaż w sklepie stacjonarnym.

Rzeczy takie jak te zakupione przez konsumentkę można swobodnie przymierzać w każdym sklepie stacjonarnym, więc kwestia sposobu ich zapakowania nie odgrywa roli w przypadku odstąpienia od umowy. W tym zakresie należy uznać, że sprzedawca ponownie wprowadził konsumentkę w błąd. [art. 5 ust. 3 pkt 4 u.p.n.p.r.]

Po dokonaniu analizy wszystkich okoliczności sprawy rzecznik uznał, że roszczenia konsumentki są zasadne, a przedsiębiorca dopuścił się szeregu uchybień. W związku z tym zaproponował konsumentce pomoc w dochodzeniu jej roszczeń.

Wystąpienie do przedsiębiorcy

Na podstawie art. 42 ust. 1 pkt 3 ustawy o ochronie konkurencji i konsumentów, w związku z wnioskiem o pomoc złożonym przez konsumentkę, rzecznik wystosował pismo do sprzedawcy. W piśmie tym wskazał wszystkie okoliczności, które miały wpływ na kształtowanie sytuacji prawnej stron omawianego sporu, oraz podał podstawę prawną każdego z wywodzonych skutków. Wskazał również przedsiębiorcy, w jaki sposób powinien doprowadzić do stanu prawnie pożądanego.

Ponadto, na podstawie art. 12 ust. 2 pkt 4 ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym, rzecznik wezwał do zaniechania stosowania nieuczciwych praktyk

rynkowych w postaci wprowadzania konsumentów w błąd w zakresie korzystania z prawa do odstąpienia od umowy oraz do niezwłocznego zamieszczenia na profilu w serwisie Twarzokajet.pl pełnej treści regulaminu zawierającego wszystkie informacje wskazane w art. 12 ustawy o prawach konsumenta.

Rzecznik poinformował przedsiębiorcę o możliwych konsekwencjach na gruncie cywilnoprawnym, karnoprawnym i administracyjnym w przypadku niezastosowania się do zamieszczonych sugestii oraz wyraził nadzieję, że spór z konsumentką zakończy się na etapie przedsądowym.

Postępowanie przed sądem

W przypadku braku możliwości polubownego zakończenia sporu rzecznik, na podstawie art. 42 ust. 2 ustawy o ochronie konkurencji i konsumentów, może wytaczać powództwa na rzecz konsumentów oraz wstępować, za ich zgodą, do toczącego się postępowania w sprawach o ochronę ich interesów konsumentów.

Ponadto, na podstawie art. 42 ust. 3 ustawy o ochronie konkurencji i konsumentów, w sprawach o wykroczenia na szkodę konsumentów rzecznik jest oskarżycielem publicznym.

Na podstawie art. 12 ust. 2 pkt 4 ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym, w przypadku stwierdzenia niedozwolonego postępowania wobec konsumenta rzecznik może żądać:

1. zaniechania tej praktyki;

2. usunięcia skutków tej praktyki;

3. złożenia jednokrotnego lub wielokrotnego oświadczenia odpowiedniej treści i w odpowiedniej formie;

3a. obniżenia ceny;

4. naprawienia wyrządzonej szkody na zasadach ogólnych, w szczególności żądania unieważnienia umowy z obowiązkiem wzajemnego zwrotu świadczeń oraz zwrotu przez przedsiębiorcę kosztów związanych z nabyciem produktu;

5. zasądzenia odpowiedniej sumy pieniężnej na określony cel społeczny związany ze wspieraniem kultury polskiej, ochroną dziedzictwa narodowego lub ochroną konsumentów.

W przypadku zignorowania wystąpienia rzecznika i barku odpowiedzi ze strony przedsiębiorcy rzecznik, działając na podstawie art. 114 ust. 1 ustawy o ochronie konkurencji i konsumentów, może wystąpić do sądu o ukaranie przedsiębiorcy karą grzywny nie mniejszą niż 2000 zł.

Podsumowanie

Do podstawowych zadań powiatowych i miejskich rzeczników konsumentów należą: udzielanie poradnictwa prawnego, pomoc w dochodzeniu zasadnych roszczeń konsumentów, a także przeciwdziałanie negatywnym skutkom nieuczciwych praktyk rynkowych na gruncie sporu o charakterze indywidualnym. Praktyki naruszające zbiorowe interesy konsumentów to domena Urzędu Ochrony Konkurencji i Konsumentów. Rzecznicy konsumentów nie posiadają uprawnień kontrolnych i nie nakładają kar na przedsiębiorców. Pomoc rzecznika jest nieodpłatna na każdym etapie prowadzonego postępowania.

WAŻNE!

Na co trzeba uważać przy zawieraniu umów na odległość:

Regulamin

Na przedsiębiorcę zawierającego umowy na odległość prawo nakłada obszerny obowiązek informacyjny, który zazwyczaj jest realizowany poprzez wskazanie wymaganych informacji w regulaminie sklepu.

Dane przedsiębiorcy

Należy sprawdzić, czy mamy do czynienia z przedsiębiorcą zarejestrowanym na terenie Polski lub innego państwa UE. Jeśli stroną umowy jest podmiot zarejestrowany poza granicami Unii, dochodzenie roszczeń wobec niego może być problematyczne.

Opinie

Dobrym pomysłem jest sprawdzenie w internecie opinii o sprzedawcy przed zawarciem umowy.

Wykaz skrótów

u.o.k.i.k.	Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2007 r. Nr 50, poz. 331 z późn. zm.)
u.p.k.	Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2014 r., poz. 827 z późn. zm.)
k.c.	Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 1964 r. Nr 16, poz. 93 z późn. zm.)
k.k.	Ustawa z dnia 6.06.1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.)
k.k.s	Ustawa z dnia 10.09.1999 r. Kodeks karny skarbowy (Dz. U. z 1999 r. Nr 83, poz. 930 z późn. zm.)
u.p.n.p.r.	Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (Dz. U. z 2007 r. Nr 171, poz. 1206 z późn. zm.)

Europejskie Centrum Konsumenckie

Wojciech Szczerba,
Koordynator Projektu ECK Polska

Case study 1

Sprawa dotycząca opóźnienia i ostatecznego braku realizacji zamówienia

Sprawa rozwiązana

W kwietniu 2026 roku konsument zakupił klubową bluzę hokejową od sprzedawcy z siedzibą na Słowacji. Zamówienie zostało niezwłocznie opłacone za pomocą systemu BLIK. Po miesiącu oczekiwania na dostawę zamówienia i braku jakiejkolwiek informacji ze strony przedsiębiorcy, mimo wielokrotnych zapytań o status przesyłki, konsument zgłosił się do ECK Polska z prośbą o pomoc w rozwiązaniu problemu.

Jeśli zamówiony produkt nie dotarł na czas, nie zawsze oznacza to, że sprzedawca narusza swoje obowiązki. Co do zasady, gdy kupujemy przez internet, sprzedawca ma do 30 dni na realizację zamówienia, chyba że przed zakupem został wyraźnie ustalony inny termin dostawy.

Jeżeli minęło już 30 dni (lub uzgodniony termin dostawy), a zamówienie nadal nie zostało zrealizowane, warto skontaktować się ze sprzedawcą i poprosić o dostarczenie towaru w dodatkowym terminie. Jeśli to nie przyniesie efektu, możemy odstąpić od umowy i domagać się zwrotu pieniędzy.

W swoim zgłoszeniu konsument dodatkowo wskazał na szereg negatywnych opinii dotyczących sprzedawcy, na jakie natrafił w internecie już po złożeniu zamówienia i wystąpieniu problemów z jego realizacją. Chciał odstąpić od umowy i odzyskać pieniądze za niezrealizowane zamówienie. Zanim zwrócił się o pomoc do ECK Polska, próbowała wyjaśnić sprawę ze swoim bankiem. Okazało się jednak, że przy uiszczeniu należności za pomocą systemu BLIK nie jest możliwe skorzystanie z procedury chargeback, czyli mechanizmu reklamacyjnego zapewnianego przez organizacje obsługujące płatności kartą, który pozwala odzyskać pieniądze z takich transakcji.

Po potwierdzeniu, że sprzedawca nie odpowiedział na zgłoszenie i problem nadal nie został rozwiązany, sprawa została przekazana przez ECK Polska do jego słowackiego odpowiednika, który skontaktował się ze sprzedającym. Po dwóch ponagleniach przedsiębiorca zadeklarował ostatecznie zwrot pieniędzy na konto kupującego. Informacja została przekazana z powrotem ECK Polska, które z kolei potwierdziło otrzymanie zwrotu pieniędzy przez konsumenta.

Pamiętaj!

Jeżeli deklarowany czas realizacji jest podawany jedynie jako wartość szacowana, należy dać przedsiębiorcy możliwość realizacji zamówienia w terminie 30 dni.

Case study 2

Sprawa dotycząca niezgodności otrzymanego towaru z opisem zawartym w ofercie prezentowanej na stronie przedsiębiorcy

Sprawa nierozwiązana

Konsumentka zakupiła ubrania, za które zapłaciła za pomocą kodu BLIK. Po otrzymaniu przesyłki stwierdziła, że cechy towaru są niezgodne z opisem towarzyszącym ofercie na stronie. Świadoma swoich praw, zwróciła się do przedsiębiorcy o umożliwienie jej odstąpienia od umowy. W udzielonych odpowiedziach przedsiębiorca próbował przekonać ją, aby zatrzymała produkty w zamian za częściowy zwrot pieniędzy (obniżenie ceny). Ze względu na rażąco niską jakość otrzymanych produktów konsumentka nie zgodziła się na zaproponowane rozwiązanie. W toku negocjacji przedsiębiorca początkowo zaproponował 20% zwrotu, a ostatecznie zaoferował upust w wysokości aż 50% zapłaconej kwoty.

Warto pamiętać, że w przypadku zakupów online można odstąpić od umowy i zwrócić towar bez podawania przyczyny, o ile działanie zostanie podjęte w terminie określonym przez przepisy. Kupujący może zostać zobowiązany do pokrycia kosztów odesłania produktu do sprzedawcy. Co ważne, **przedsiębiorca nie ma jasno określonego w przepisach obowiązku zapewnienia adresu, pod którym przyjmuje zwroty, na terenie UE, lecz powinien w jasny i zrozumiały sposób poinformować konsumenta o sposobie skorzystania z prawa do odstąpienia od umowy**. Jeśli zakupiony produkt lub usługa nie są zgodne z umową, sprzedawca powinien naprawić lub wymienić produkt, obniżyć cenę albo zwrócić pieniądze. Wszystko powinno odbyć się w rozsądnym czasie, bez nadmiernych niedogodności i bez dodatkowych kosztów dla kupującego.

Konsumentka zwróciła się do ECK Polska o pomoc w polubownym rozwiązaniu problemu. Jako że instytucja już na wstępie otrzymało odpowiednią dokumentację, sprawa została skierowana do niderlandzkiego ECK, gdzie według deklaracji przedsiębiorcy znajdowała się jego siedziba. Mimo prób nawiązania kontaktu ze sprzedającym i przedstawienia mu argumentów opartych na obowiązujących przepisach, nie uzyskano odpowiedzi.

Ta sprawa pokazuje coraz częściej spotykany problem procederu tworzenia stron internetowych firm, które sprawiają wrażenie, że są prowadzone przez polskich przedsiębiorców (udają np. butiki albo projektantów mody). Wykorzystują nazwy złożone z polskich imion, nazwisk lub nazw miast, aby wzbudzić większe zaufanie. Z informacji podanych na ich stronach można wywnioskować, że prowadzą je podmioty zarejestrowane w różnych krajach UE. ECK Polska zwraca jednak uwagę, że wiele takich firm jedynie formalnie ma siedzibę na terenie Unii. W rzeczywistości ich centrale znajdują się poza terytorium wspólnoty i tylko realizują one zamówienia z magazynów logistycznych na jej terenie (tzw. *fulfilment*).

ECK Polska zachęca konsumentów do zapoznawania się z opiniami dotyczącymi sklepów internetowych przed złożeniem zamówienia. Nagromadzenie złych ocen lub brak jakichkolwiek opinii może być sygnałem ostrzegawczym, by zrezygnować z zakupu. Z obserwacji ECK Polska wynika, że złe opinie zaczynają się zwykle pojawiać dopiero po około 1–2 miesiącach od pojawienia się strony w sieci.

ECK Polska uczula, że warto sprawdzać nie tylko opinie dotyczące nazwy handlowej i marki sklepu czy firmy, ale weryfikować także nazwę przedsiębiorcy wskazaną w regulaminie. Ten sam podmiot często prowadzi kilka podobnych sklepów internetowych działających pod różnymi nazwami handlowymi.

Czym zajmuje się ECK Polska?

ECK Polska jest częścią sieci European Consumer Centre Network (ECC-Net), która obejmuje terytorium Unii Europejskiej, Norwegii i Islandii. ECC-Net dodatkowo współpracuje ze swoim byłym oddziałem w Wielkiej Brytanii (obecnie International Consumer Centre UK – ICC UK).

Zadaniem oddziałów krajowych ECK jest udzielanie porad konsumenckich w sprawach transgranicznych, gdzie strony umowy znajdują się w dwóch różnych krajach objętych zasięgiem sieci ECC-Net + ICC UK. Dodatkowo istnieje możliwość zaangażowania ECK w prowadzenie działań mających na celu polubowne rozwiązanie sporu między stronami.

ECK Polska zajmuje się szerokim spektrum tematów, m.in. zakupami konsumenckimi, prawami pasażerów, usługami turystycznymi, wynajmem samochodów. ECK nie może udzielić pomocy w przypadku sporu z usługodawcą działającym na polu usług finansowych (bankowość, ubezpieczenia, itp.), sporu pomiędzy dwiema osobami fizycznymi czy dwoma podmiotami gospodarczymi.

Należy pamiętać, że ECK nie posiada uprawnień do przeprowadzania dochodzeń, nie może też wprost nakazać przedsiębiorcy przyjęcia określonego stanowiska. Niemniej jednak skuteczność ECK w prowadzonych postępowaniach przekracza 50% przypadków, w których udaje się doprowadzić do rozwiązania akceptowalnego dla obu stron sporu.

W niektórych sytuacjach ECK może również wskazać konsumentowi inną ścieżkę rozwiązania zgłaszanego problemu, co zwykle jest podyktowane względami praktycznymi, takimi jak brak woli współpracy ze strony konkretnego przedsiębiorcy, czy też wiąże się z deklarowanym celem zgłoszenia konsumenta wykraczającym poza zakres kompetencji ECK.

Urząd Ochrony Konkurencji i Konsumentów

Andrzej Janyszko,
Departament Komunikacji UOKiK

Nie każda okazja jest prawdziwa. Co robi UOKiK, by chronić konsumentów podczas zakupów online?

My Polacy, coraz częściej i więcej kupujemy przez internet. Korzystamy z promocji, porównujemy ceny i szukamy najlepszych ofert. Nie zawsze jednak możemy polegać na informacjach, które mają nas przekonać do zakupu. Jako konsumenci, niestety coraz częściej, możemy zetknąć się z różnymi zagrożeniami – od fałszywych sklepów internetowych, przez przedsiębiorców podszywających się pod polskie marki i nieuczciwych pośredników ukrywających rzeczywiste warunki transakcji, po interfejsy zaprojektowane tak, aby wpłynąć na nasze decyzje zakupowe. Choć mechanizmy ich działania są różne, łączy je jedno: konsument może podjąć decyzję zakupową na podstawie nieprawdziwych lub niepełnych informacji.

Do UOKiK docierają sygnały dotyczące różnych nieprawidłowości związanych z zakupami w internecie. Konsumenci zgłaszają m.in. problemy z niedostarczonymi zamówieniami, otrzymywaniem produktów niezgodnych z opisem, utrudnionym kontaktem ze sprzedawcą czy odmową zwrotu pieniędzy. Zdarza się, że dopiero po dokonaniu zakupu odkrywają, że sklep, który przedstawiał się jako polska marka, w rzeczywistości prowadzony jest przez przedsiębiorcę spoza Unii Europejskiej. Niektóre strony wykorzystują nazwy sugerujące lokalne pochodzenie firmy, historie o wieloletniej tradycji rodzinnego biznesu czy komunikaty o likwidacji sklepu i wyjątkowych wyprzedażach. Takie działania mogą wprowadzać konsumentów w błąd co do tożsamości sprzedawcy i rzeczywistych warunków transakcji.

Wśród problemów, na które zwracamy uwagę, jest również ukryty dropshipping. Sam dropshipping jest legalnym modelem biznesowym, jednak konsumenci nie zawsze wiedzą, że strona, na której składają zamówienie, jedynie pośredniczy w zakupie, a umowę sprzedaży zawierają z innym przedsiębiorcą, często mającym siedzibę poza Unią Europejską. O rzeczywistej roli pośrednika dowiadują się niekiedy dopiero wtedy, gdy chcą zareklamować produkt lub odstąpić od umowy. Wówczas może się okazać, że odesłanie towaru za granicę wiąże się ze znacznymi kosztami, a dochodzenie roszczeń jest utrudnione. Dlatego tak istotne jest, aby przedsiębiorcy jasno informowali, z kim konsument zawiera umowę, kto odpowiada za jej wykonanie oraz jakie są warunki reklamacji i zwrotu towaru.

Sygnały napływające od konsumentów są dla UOKiK ważnym źródłem informacji o nieprawidłowościach na rynku. Analizujemy je przede wszystkim pod kątem możliwego naruszenia zbiorowych interesów konsumentów. Jeśli istnieją ku temu podstawy, Prezes UOKiK może wszcząć postępowanie, a w przypadku stwierdzenia naruszenia – nakazać zaniechanie zakwestionowanych praktyk i nałożyć karę finansową. Nie pozostawiamy jednak bez reakcji również tych zgłoszeń, które dotyczą spraw wykraczających poza nasze kompetencje. Informacje o podejrzanych stronach internetowych przekazujemy do CERT Polska, a gdy zachodzi podejrzenie popełnienia przestępstwa, składamy zawiadomienia do prokuratury. Współpracujemy także z innymi właściwymi instytucjami, przekazując im sygnały wymagające podjęcia działań w ramach ich kompetencji.

Istotnym wyzwaniem pozostaje również sposób, w jaki przedsiębiorcy docierają do konsumentów i wpływają na ich decyzje zakupowe. Dużą rolę odgrywają tu reklamy internetowe, szczególnie te publikowane w mediach społecznościowych. Sponsorowane posty i reklamy dopasowane do zainteresowań użytkowników mogą kierować ich na strony nieuczciwych sprzedawców. Sam fakt, że reklama pojawia się na znanej platformie, nie oznacza jednak, że reklamowany sklep jest wiarygodny. Dlatego UOKiK przygląda się również mechanizmom rozpowszechniania takich reklam i roli platform internetowych w docieraniu potencjalnie nieuczciwych ofert do konsumentów.

Poważnym problemem związanym z zakupami w internecie są również tzw. *dark patterns*, czyli rozwiązania stosowane na stronach internetowych i w aplikacjach, które wykorzystują mechanizmy psychologiczne, aby wpływać na zachowania i decyzje konsumentów. Mogą to być fałszywe liczniki odliczające czas do końca promocji, komunikaty sugerujące, że produkt zaraz się wyprzeda, automatyczne dodawanie produktów lub usług do koszyka czy ukrywanie dodatkowych kosztów do ostatniego etapu zamówienia. Manipulacja może polegać także na takim zaprojektowaniu strony, aby zakup lub uruchomienie subskrypcji były bardzo proste, ale rezygnacja z nich wymagała znacznie większego wysiłku. Wszystkie te rozwiązania mogą wykorzystywać pośpiech, obawę przed utratą okazji, nieuwagę czy przyzwyczajenia konsumentów, skłaniając ich do działań, których nie podjęliby w innych okolicznościach. To właśnie tutaj przebiega granica między zwykłym zachęcaniem do zakupów a manipulowaniem decyzjami konsumentów.

W UOKiK przyglądamy się takim praktykom i analizujemy, czy nie naruszają one zbiorowych interesów konsumentów. Ponieważ manipulacyjne mechanizmy mogą przybierać różne formy i występować na wielu stronach internetowych, w ich wykrywaniu wykorzystujemy również nowoczesne technologie, m.in. sztuczną inteligencję. Dzięki temu możemy sprawniej wychwytywać podejrzane rozwiązania i kierować je do dalszej weryfikacji przez ekspertów UOKiK. Jeśli analiza wykaże podstawy do podjęcia działań, Prezes UOKiK może wszcząć postępowanie wobec przedsiębiorcy.

Choć w UOKiK mamy doświadczonych ekspertów i korzystamy z nowoczesnych narzędzi, w tym sztucznej inteligencji, skala handlu internetowego i różnorodność stosowanych przez przedsiębiorców rozwiązań sprawiają, że nie jesteśmy w stanie samodzielnie wychwycić wszystkich nieuczciwych praktyk. Dlatego tak ważne jest, aby sami konsumenci potrafili rozpoznawać zwodnicze interfejsy i nie ulegali manipulacjom, z którymi mogą zetknąć się podczas zakupów w internecie. Chcemy, aby wiedzieli, na co zwracać uwagę, jak odróżniać rzeczywiste okazje od sztucznie wywoływanej presji i jak podejmować decyzje zakupowe bez ulegania takim mechanizmom.

Ważne jest również, aby konsumenci informowali nas o zauważonych nieprawidłowościach za pośrednictwem formularza na stronie uokik.gov.pl lub listownie. W zgłoszeniu warto opisać problem, wskazać przedsiębiorcę i dołączyć materiały dokumentujące praktykę, np. zrzuty ekranu, regulamin, korespondencję czy potwierdzenie zamówienia.

Trzeba przy tym odróżnić działania podejmowane w interesie zbiorowym, którymi zajmuje się UOKiK od pomocy w indywidualnym sporze ze sprzedawcą. Jeśli sklep nie uznaje reklamacji, odmawia zwrotu pieniędzy lub nie realizuje zamówienia, konsument może skorzystać z bezpłatnej pomocy miejskiego lub powiatowego rzecznika konsumentów, Inspekcji Handlowej albo porad udzielanych pod numerami 801 440 220 i 222 66 76 76 oraz przez formularz na stronie dlakonsumentow.pl. W sporach z przedsiębiorcami z innych państw Unii Europejskiej, Norwegii lub Islandii pomocą służy Europejskie Centrum Konsumenckie.

Najważniejsza pozostaje jednak ostrożność przed dokonaniem zakupu. Jeżeli oferta wydaje się wyjątkowo korzystna, a komunikaty na stronie nakłaniają do natychmiastowego zakupu, warto poświęcić chwilę na sprawdzenie adresu siedziby przedsiębiorcy i regulamin sklepu – w szczególności zasady dostawy, reklamacji i zwrotów. Niepokój powinny wzbudzać niepełne informacje kontaktowe, błędy językowe, nietypowe adresy internetowe czy wyjątkowo duże obniżki cen. Warto też pamiętać, że polska nazwa sklepu, atrakcyjna strona internetowa czy reklama w popularnym serwisie społecznościowym nie są gwarancją wiarygodności sprzedawcy.



- bezpiecznymiesiac.pl
- wiedza.cert.pl
- cert.pl
- nask.pl
- cbzc.policja.gov.pl
- rf.gov.pl
- konsument.gov.pl
- uokik.gov.pl



- „Okazja czy pułapka? Poradnik o bezpiecznych zakupach online”
- „Nie klikaj w ciemno! Od perswazji do dark patterns”
- Publikacje NASK kierowane do dorosłych użytkowników internetu
- Publikacje Rzecznika Finansowego
- Publikacje Europejskiego Centrum Konsumenckiego
- Publikacje Urzędu Ochrony Konkurencji i Konsumentów

Przypisy

[1] Raport „E-commerce w Polsce 2026”, Gemius, PBI, IAB Polska, Akademia Leona Koźmińskiego, Centrum Badań Mediów i Społeczeństwa ALK. https://gemius.com/documents/95/Raport_e-commerce_w_Polsce_2026.pdf

[2] Badanie „Zaufanie w polskim e – commerce” 2025, CE Research na zlecenie TrustMate, https://strategiczni.pl/ zaufanie-w-polskim-e-commerce-2025-mlodzi-konsumenci-odrzucaja-anonimowe-opinie-wyniki-badania-trustmate

[3] Raport „Nawyki e-zakupowe Polaków 2024”, SamoSEO, https://samoseo.pl/nawyki-e-zakupowe-polakow-raport-2024/

[4] Raport „E-commerce w Polsce 2025”, Gemius, PBI, IAB Polska, Akademia Leona Koźmińskiego, Centrum Badań Mediów i Społeczeństwa ALK., https://gemius.com/pl/news/raport-e-commerce-w-polsce-2025-jest-juz-dostepny/

[5] „Raport o stanie rynku pocztowego w 2025 r.”, Urząd Komunikacji Elektronicznej, https://bip.uke.gov.pl/ raporty/raport-o-stanie-rynku-pocztowego-w-2025-r-,112.html



NASK

CBZC

Rzecznik Finansowy

Europejskie Centrum Konsumenckie Polska

ECC Net

UOKiK

Urząd Ochrony Konkurencji i Konsumentów