
PORADNIK WAKACYJNY 2024

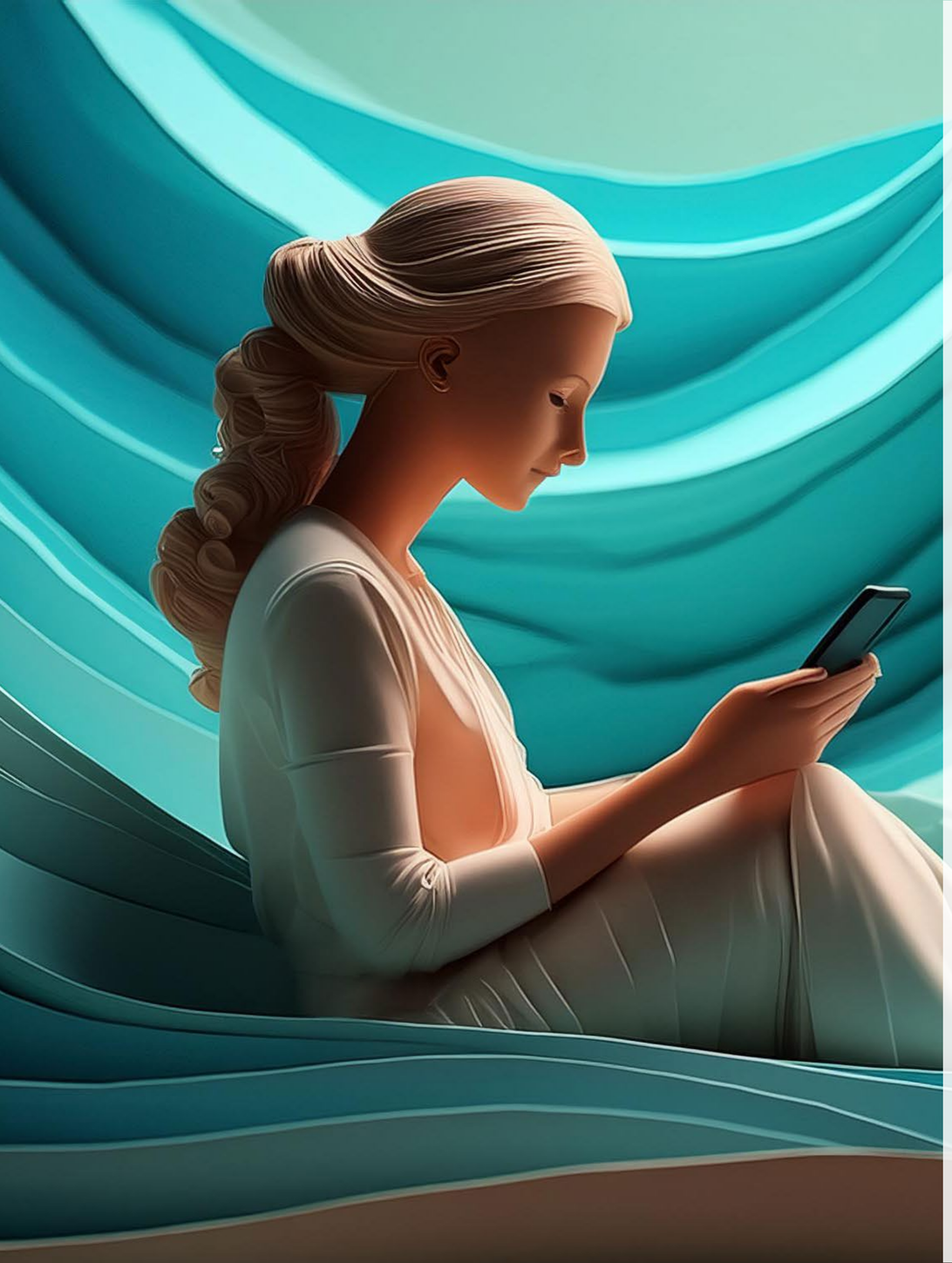
Planując wakacje, warto pamiętać o podstawowych zasadach bezpieczeństwa, które pozwolą cieszyć się urlopem bez zbędnych zmartwień.

W tym poradniku znajdziesz praktyczne wskazówki, jak chronić siebie, swoich bliskich i swój majątek, korzystając z usług telekomunikacyjnych w trakcie podróży i wypoczynku. Przeczytasz m.in. o:

- kiedy usługi w roamingu są płatne?
- czy oddzwanianie na nieznane numery jest bezpieczne?
- czy wakacyjna burza może uszkodzić urządzenia w domu?
- czy hotelowe Wi-Fi jest bezpieczne?
- czy fotorelacje z wakacji są bezpieczne?

Życzymy udanych, bezpiecznych wakacji i miłej lektury:)

Spis treści



1. Roaming i zasada RLAH

Roaming to mechanizm, który pozwala na korzystanie z mobilnych usług telekomunikacyjnych kiedy abonent przebywa w zasięgu innego dostawcy usług. Najczęściej z roamingu korzystamy podczas zagranicznych podróży.

Twój dostawca usług musi Cię informować o kosztach usług w roamingu, niezależnie od kraju, do którego przyjeżdżasz. Powinieneś otrzymać SMS z informacją o cenach usług, za każdym razem, gdy przekraczasz granicę danego państwa – nawet jeśli cena wynosi 0 zł.

Na terenie Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego (UE/EOG) opłaty są rozliczane według zasady RLAH (Roam Like At Home). Zgodnie z zasadą RLAH opłaty w roamingu powinny być takie same, jak opłaty za korzystanie z tożsamych usług w kraju, a w przypadku dostępu do internetu operator może przyznać Ci określony limit transmisji danych, po wykorzystaniu którego zacznie naliczać opłaty. Kiedy podróżujesz z Polski do innego kraju UE/EOG, dostawca usług nie może naliczać dodatkowych opłat, za wyjątkiem opłat wynikających z Polityki Uczciwego Korzystania lub jeżeli dostawca usług uzyskał zgodę Prezesa UKE na stosowanie dodatkowych opłat.

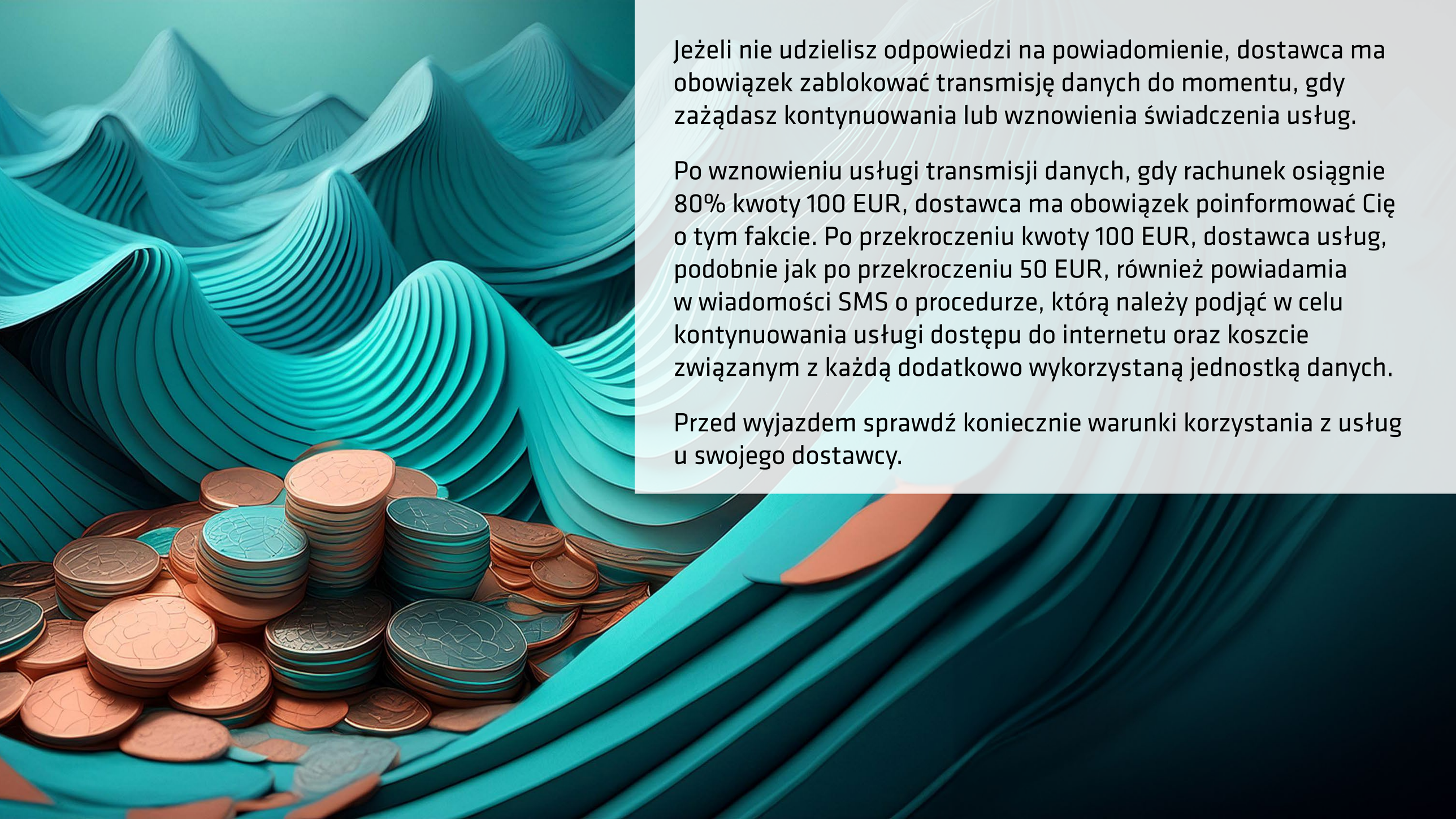
2. Limity na wydatki w roamingu

Dostawcy usług mają obowiązek ochrony abonenta przed wysokimi kosztami transmisji danych na terenie UE/EOG. Poza UE/EOG obowiązek taki również istnieje, o ile operator sieci zagranicznej umożliwia monitorowanie zużycia danych.

W ramach standardowego mechanizmu ochrony abonentów operatorzy muszą ustawić domyślny limit kwotowy w wysokości równowartości 50 EUR miesięcznie oraz równowartości 100 EUR miesięcznie na transmisję danych w roamingu.

Gdy rachunek za transmisję danych w roamingu osiągnie 80% kwoty 50 EUR, dostawca usług ma obowiązek poinformować Cię o tym fakcie. Po przekroczeniu kwoty 50 EUR, dostawca usług powiadamia w wiadomości SMS o:

- procedurze, którą należy podjąć w celu kontynuowania usługi dostępu do internetu,
- koszcie związanym z każdą dodatkowo wykorzystaną jednostką danych.



Jeżeli nie udzielisz odpowiedzi na powiadomienie, dostawca ma obowiązek zablokować transmisję danych do momentu, gdy zażądasz kontynuowania lub wznowienia świadczenia usług.

Po wznowieniu usługi transmisji danych, gdy rachunek osiągnie 80% kwoty 100 EUR, dostawca ma obowiązek poinformować Cię o tym fakcie. Po przekroczeniu kwoty 100 EUR, dostawca usług, podobnie jak po przekroczeniu 50 EUR, również powiadamia w wiadomości SMS o procedurze, którą należy podjąć w celu kontynuowania usługi dostępu do internetu oraz koszcie związanym z każdą dodatkowo wykorzystaną jednostką danych.

Przed wyjazdem sprawdź koniecznie warunki korzystania z usług u swojego dostawcy.

3. Różnica pomiędzy roamingiem a połączeniem międzynarodowym

Połączenie w roamingu wykonujesz, gdy dzwonisz z polskiego numeru będąc za granicą. Nie ma znaczenia dokąd dzwonisz – na polski czy na inny zagraniczny numer. Istotne, że Twój telefon zalogowany jest do sieci zagranicznej.

Gdy siedząc na plaży w Grecji lub jedząc pizzę w Neapolu, dzwonisz do rodziny w Polsce lub kolegi w Niemczech, wykonujesz połączenie w roamingu.

Natomiast, gdy dzwonisz z Polski do USA czy do Niemiec wykonujesz połączenie międzynarodowe. Za to połączenie zapłacisz jak za połączenie międzynarodowe, zgodnie z cennikiem dostawcy. Zasada RLAH nie odnosi się do połączeń międzynarodowych.

4. Uważaj na roaming przygraniczny

Na terenie przygranicznym, jeżeli telefon ma ustawiony automatyczny wybór sieci, może zalogować się do sieci zagranicznego dostawcy usług mającego silniejszy sygnał na danym terenie. Pamiętaj, że kiedy jesteś blisko granicy, możesz automatycznie połączyć się z zagraniczną siecią. Wówczas Twój dostawca naliczy opłaty zgodnie z obowiązującym cennikiem w roamingu. Jeśli połączysz się z siecią operatora spoza UE/EOG, opłaty będą znacznie wyższe.

Wyjeżdżając na tereny przygraniczne ustaw w telefonie ręczne wybieranie sieci. Będziesz mieć pewność, że połączenia będą realizowane w sieci Twojego dostawcy usług.

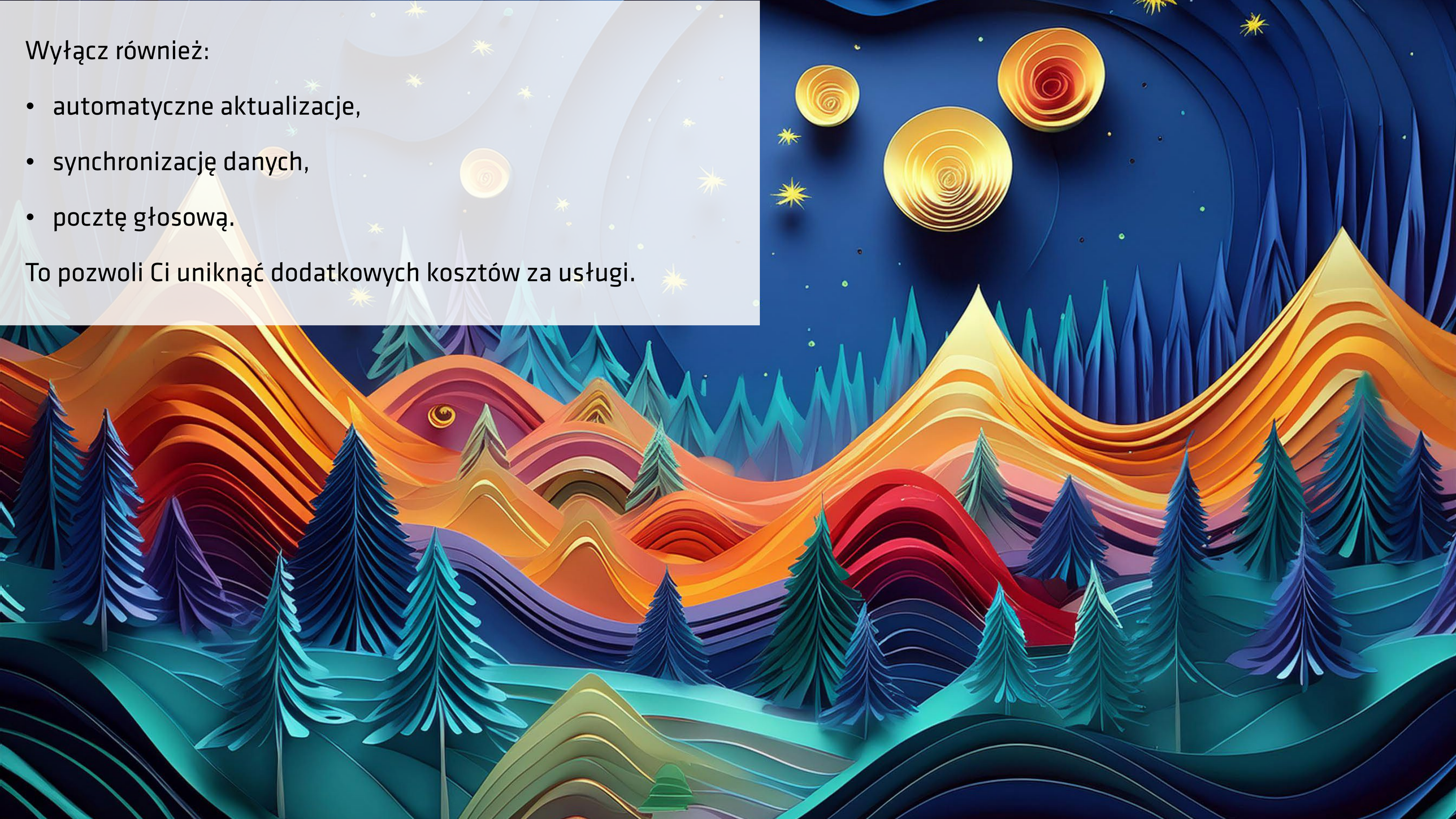
Możesz też:

- wyłączyć roaming zagraniczny całkowicie - wtedy Twój telefon nie będzie logował się do sieci zagranicznych;
- wyłączyć samą transmisję danych w roamingu zagranicznym - wtedy Twój telefon nie będzie łączył się z internetem.

Wyłącz również:

- automatyczne aktualizacje,
- synchronizację danych,
- pocztę głosową.

To pozwoli Ci uniknąć dodatkowych kosztów za usługi.



5. Czy RLAH obowiązuje na promie lub statku?

Jeśli Twój telefon komórkowy będzie podłączony do naziemnej sieci komórkowej (np. podczas podróży po rzece, jeziorze lub wzdłuż wybrzeża) w jednym z krajów UE/EOG, będziesz mógł korzystać z usług roamingu zgodnie z zasadą RLAH.

Problem braku zasięgu na otwartych akwenach rozwiązywany jest dzięki sieciom satelitarnym. Unijne przepisy dotyczące roamingu mają zastosowanie wyłącznie do naziemnych sieci komórkowych. Jeżeli podczas rejsu usługi telefonii komórkowej będą świadczone za pośrednictwem innych rodzajów sieci radiowych, takich jak np. systemy satelitarne statku, Twoje połączenia, SMS-y i transmisja danych nie będą objęte zasadą RLAH.

Koszty połączeń głosowych, wiadomości SMS i transferu danych znajdziesz w cenniku dostawcy lub danego operatora sieci satelitarnej.

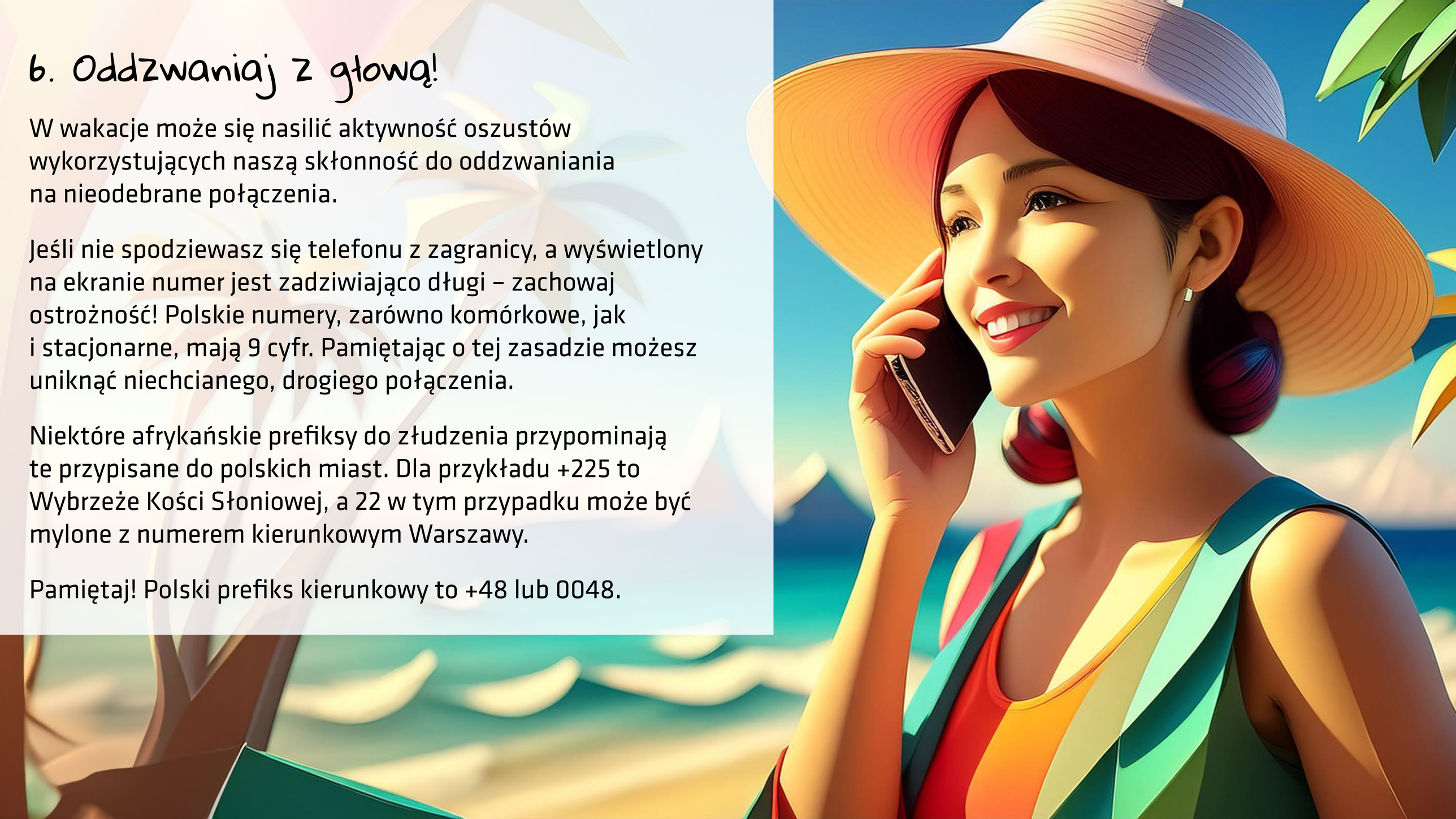
6. Oddzwaniaj z głową!

W wakacje może się nasilić aktywność oszustów wykorzystujących naszą skłonność do oddzwaniania na nieodebrane połączenia.

Jeśli nie spodziewasz się telefonu z zagranicy, a wyświetlony na ekranie numer jest zadziwiająco długi – zachowaj ostrożność! Polskie numery, zarówno komórkowe, jak i stacjonarne, mają 9 cyfr. Pamiętając o tej zasadzie możesz uniknąć niechcianego, drogiego połączenia.

Niektóre afrykańskie prefiksy do złudzenia przypominają te przypisane do polskich miast. Dla przykładu +225 to Wybrzeże Kości Słoniowej, a 22 w tym przypadku może być mylone z numerem kierunkowym Warszawy.

Pamiętaj! Polski prefiks kierunkowy to +48 lub 0048.



7. Zablokuj usługi o podwyższonej opłacie

Dostawca usług domyślnie zablokuje korzystanie z usług o podwyższonej opłacie, kiedy wydasz na nie 35 zł w ciągu miesiąca/okresu rozliczeniowego.

Możesz wybrać całkowitą blokadę takich usług. Możesz zablokować:

- wychodzące lub przychodzące wiadomości,
- wybrane lub wszystkie numery o podwyższonej opłacie.

Jeśli świadomie, często korzystasz z tych usług , nie musisz ich blokować. Możesz wybrać inny próg limitu wydatków, np. 100 zł, po przekroczeniu którego Twój dostawca zablokuje dalsze korzystanie z usług.

Możesz również uniknąć dodatkowych kosztów, zlecając aktywację blokady płatności usług dodatkowych, zakupów elektronicznych, tj. direct carrier billing, czyli automatycznych płatności doliczanych do rachunku. Skontaktuj się ze swoim dostawcą i zleć aktywację blokad.

8. Zabezpiecz sprzęt przed burzą

Lato to czas częstych wyładowań atmosferycznych. Zdarza się, że podczas burzy dochodzi do spięcia i może zepsuć się na przykład router czy dekoder.

Pamiętaj, że dostawca usług nie odpowiada za szkody powstałe wskutek tak zwanej siły wyższej. Mamy z nią do czynienia, gdy zdarzenie pochodzi z zewnątrz, ma charakter nadzwyczajny i nie da się go przewidzieć. Siłą wyższą mogą być na przykład wyładowania atmosferyczne.

Zadbaj o zabezpieczenie modemu, routera czy komputera przed uszkodzeniami spowodowanymi przepięciami. Przed burzą odłącz od prądu sprzęty domowe. Na rynku dostępne są też urządzenia, które zabezpieczają sprzęt przed tego typu sytuacjami.

9. W podróży zadbaj o urządzenia

Smartfon, laptop czy tablet to ogromne źródło danych. Urządzenia zawierają mnóstwo informacji o nas, naszych znajomych, nawykach, pracy i naszych danych wrażliwych.

Na smartfonach mamy zainstalowane aplikacje do banku, pocztę elektroniczną, zdjęcia, dokumenty. Aby chronić te dane, musisz pamiętać o ochronie urządzenia.

- ustaw blokadę ekranu na każdym urządzeniu,
- regularnie rób kopie zapasowe,
- pamiętaj o aktualizacji oprogramowania i programie antywirusowym,
- usuń poufne dane z telefonu,
- nie zapisuj i nie udostępniaj haseł logowania.

10. Publiczne sieci Wi-Fi

Jesteś w hotelu, galerii, restauracji czy na lotnisku i chcesz skorzystać z publicznej sieci Wi-Fi (tzw. Hotspot)? To pozwoli uniknąć wysokich opłat za transfer danych, szczególnie kiedy jesteś poza granicami UE/EOG. Zachowaj jednak ostrożność, bo podłączenie do niezabezpieczonej sieci bez hasła może mieć negatywne skutki!

Cyberprzestępcy mogą tworzyć fałszywe punkty dostępowe Wi-Fi. Takie hotspoty umożliwiają przechwycenie części danych przesyłanych przez użytkowników do stron internetowych (np. banku, sklepu itp.).

Jeśli korzystasz z Wi-Fi, pamiętaj o zasadach bezpieczeństwa:

- łącząc się z Wi-Fi, nie wybieraj w smartfonie opcji jej zapamiętania,
- upewnij się, czy punkt dostępu należy do miejsca, do którego jest przypisany,
- regularnie aktualizuj system operacyjny urządzenia,
- zainstaluj na smartfonie aplikację antywirusową,
- jeśli musisz skorzystać z publicznej sieci, unikaj logowania do wrażliwych kont osobistych (np. bankowość online, poczta elektroniczna).

II. Uwaga phishing!

Phishing to oszustwo, przez które nieświadomie możemy przekazać przestępcom swoje osobiste dane takie jak loginy, hasła czy numery kart płatniczych. Co więcej, będziemy przekonani, że informacje przekazujemy instytucji, którą znamy - np. do biura podróży.

W okresie wakacyjnym wiele osób szuka ofert podróży, przegląda strony z ofertami noclegów czy tańszych biletów. Oszuści potrafią tworzyć fałszywe strony, a także wysyłać maile i SMSy, w których np. proszą o podanie danych osobowych lub przelew kwoty, której rzekomo brakuje w płatności za nasz wyjazd.

Aby tego uniknąć sprawdź dokładnie adres linku, który dostałeś bądź skontaktuj się z firmą, z której rzekomo otrzymałeś dane informacje.

Jak ustrzec się phishingu?

- zachowaj czujność, jeśli jakaś oferta wydaje się zbyt piękna czy tania, aby była prawdziwa, najprawdopodobniej jest fałszywa.
- zwracaj uwagę na adres domeny i wygląd strony internetowej,
- sprawdź czy znasz nadawcę, który wysyła wiadomość z linkiem, w który masz kliknąć,
- zweryfikuj u źródła (np. w biurze podróży) czy wysłało wiadomość z prośbą o aktualizację danych, dopłatę itp.,
- robiąc rezerwacje i kupując bilety, korzystaj z zaufanych stron internetowych, wprowadzając adres strony ręcznie w pasku przeglądarki,
- aktualizuj przeglądarkę, z której korzystasz do najnowszej oferowanej przez producenta wersji,
- pamiętaj o oprogramowaniu antywirusowym,
- regularnie zmieniaj hasła,
- stosuj różne hasła do różnych kont i pamiętaj, żeby Twoje hasła były silne i trudne do złamania.

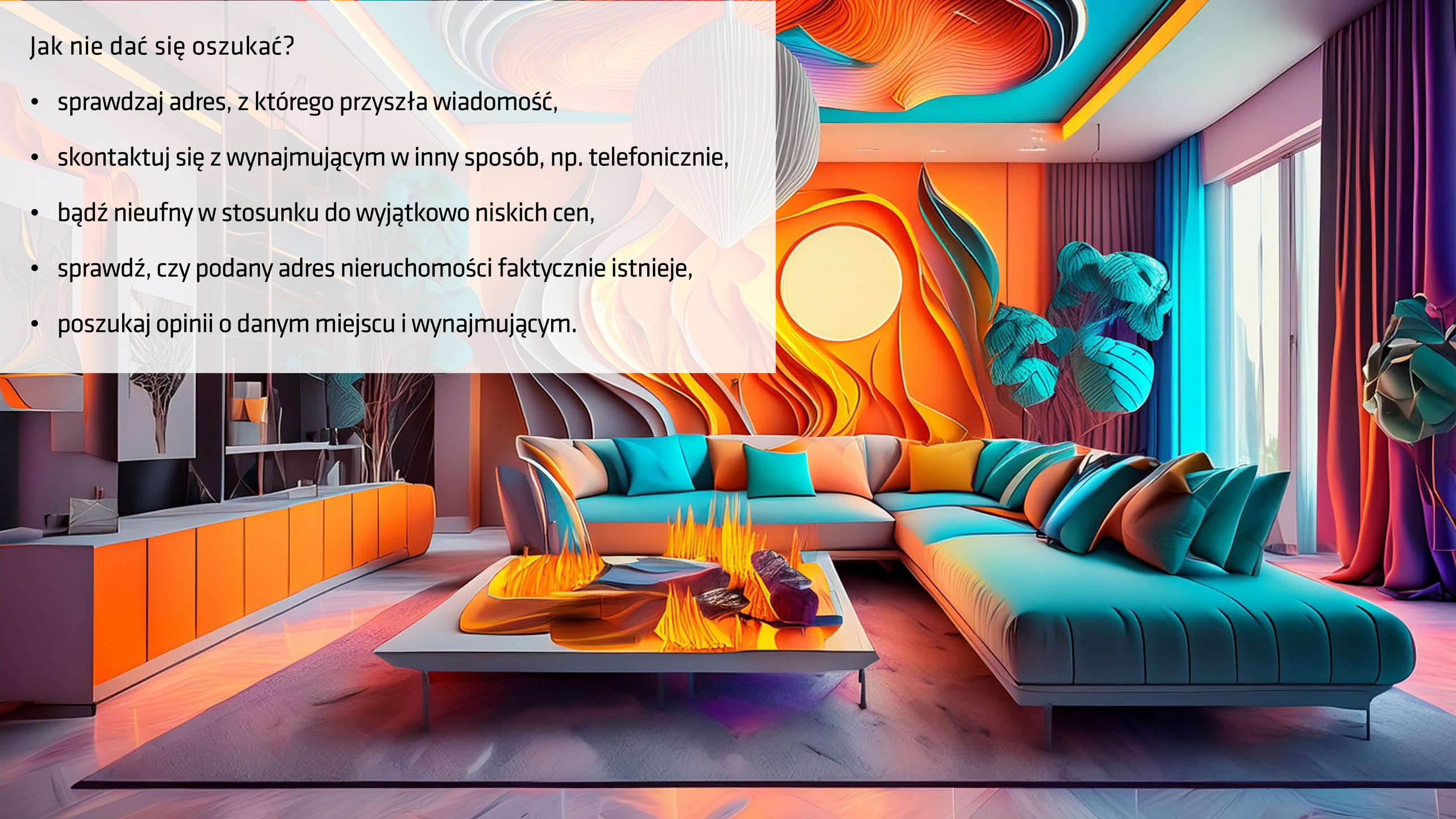
12. Uwaga na fałszywe rezerwacje mieszkań

Wakacje, festiwale czy koncerty znanych artystów do doskonała okazja dla oszustów na wynajem nieistniejących apartamentów, mieszkań lub pokoi. Fałszywe oferty można znaleźć nie tylko w serwisach zajmujących się bezpośrednio wynajmem nieruchomości, ale również u pośredników.

Zdarzały się również przypadki wysyłki maili do klientów znanego portalu z informacją o konieczności podania dodatkowych danych niezbędnych do potwierdzenia rezerwacji czy konieczności dopłaty. Oszuści bazowali na strachu i pośpiechu, gdyż w spreparowanej wiadomości pojawia się informacja, że w przypadku braku działania rezerwacja zostanie odwołana. W rzeczywistości podesłany link przenosił na fałszywą stronę internetową, na której oszuści wyłudzają dane osobowe oraz dane kart płatniczych.

Jak nie dać się oszukać?

- sprawdzaj adres, z którego przyszła wiadomość,
- skontaktuj się z wynajmującym w inny sposób, np. telefonicznie,
- bądź nieufny w stosunku do wyjątkowo niskich cen,
- sprawdź, czy podany adres nieruchomości faktycznie istnieje,
- poszukaj opinii o danym miejscu i wynajmującym.



13. Łowcy letnich promocji

Wakacje to czas, gdy sklepy oferują nam promocje na zakupy online, kupony rabatowe itp. Wykorzystują to oszuści internetowi, którzy mogą podszywać się pod znane marki. Częstym schematem działania jest masowa wysyłka SMSów wraz z linkiem do pobrania aplikacji, która umożliwia rzekomą zniżkę na zakupy. Klikając w taki link narażasz się na ściągnięcie złośliwego oprogramowania, utratę danych, a nawet kradzież środków z kart płatniczych i przejęcie całkowitej kontroli nad urządzeniem.

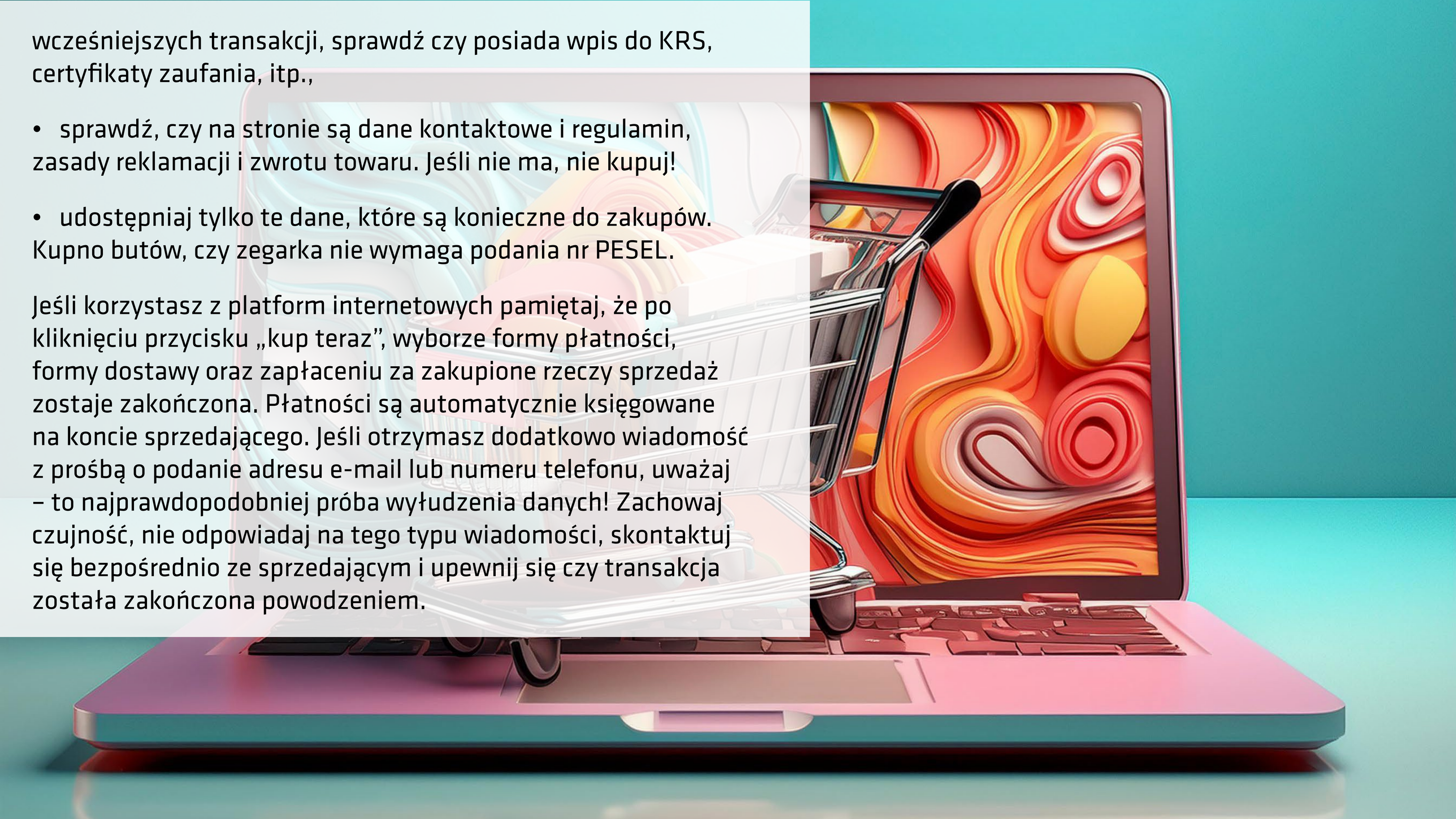
- nie otwieraj załączników i linków z podejrzanych e-maili i SMSów,
- sprawdzaj źródła, adresy e-mailowe i treść wiadomości,
- zwracaj uwagę na literówki i brak polskich znaków,
- nie udostępniaj loginów i haseł,
- nie udostępniaj danych z karty płatniczej,
- przed zrobieniem zakupów sprawdź wiarygodność sprzedającego: poszukaj informacji o nim, historii

wcześniejszych transakcji, sprawdź czy posiada wpis do KRS, certyfikaty zaufania, itp.,

- sprawdź, czy na stronie są dane kontaktowe i regulamin, zasady reklamacji i zwrotu towaru. Jeśli nie ma, nie kupuj!

- udostępniaj tylko te dane, które są konieczne do zakupów. Kupno butów, czy zegarka nie wymaga podania nr PESEL.

Jeśli korzystasz z platform internetowych pamiętaj, że po kliknięciu przycisku „kup teraz”, wyborze formy płatności, formy dostawy oraz zapłaceniu za zakupione rzeczy sprzedaż zostaje zakończona. Płatności są automatycznie księgowane na koncie sprzedającego. Jeśli otrzymasz dodatkowo wiadomość z prośbą o podanie adresu e-mail lub numeru telefonu, uważaj – to najprawdopodobniej próba wyłudzenia danych! Zachowaj czujność, nie odpowiadaj na tego typu wiadomości, skontaktuj się bezpośrednio ze sprzedającym i upewnij się czy transakcja została zakończona powodzeniem.



14. Uważaj na oszustwo BLIKiem!

W wakacje nasila się zjawisko włamań na konta na portalach społecznościowych. Dzięki temu oszuści mogą naciągać naszych znajomych na pożyczki, wykorzystując do tego elektroniczne metody płatności. Przestępca podszywając się pod nas lub pod znaną nam osobę próbuje pozyskać kod BLIK, który my potwierdzimy podczas autoryzacji.

Jeśli dostaniemy prośbę o pożyczkę lub zrobienie za kogoś płatności BLIKiem, zadzwońmy bezpośrednio do tej osoby. Zweryfikujmy, czy na pewno potrzebuje takiej płatności. Często podczas rozmowy wychodzi na jaw, że profil naszego znajomego został przejęty przez oszustów, a sam zainteresowany nie ma do niego dostępu.

W regulaminach banków zazwyczaj widnieją zapisy, że jednorazowe hasła (takie jak kod BLIK) nie mogą być udostępniane osobom trzecim. Jeśli sami udostępnimy kod oszustowi, musimy liczyć się z tym, że bank nie uzna naszej reklamacji.

Pamiętaj:

- nie rób przelewów w sytuacjach, które budzą Twoje wątpliwości,
- uważaj na „szybkie” płatności,
- nigdy nie udostępniaj swoich haseł i kodów.

15. Dziel się wspomnieniami, nie danymi

Korzystając z uroków wakacji i zwiedzając nowe miejsca ciężko oprzeć się pokusie publikacji zdjęć i filmów w mediach społecznościowych. Warto jednak odczekać i zwracać uwagę co wrzucamy do sieci. Wstawiając zdjęcia z wakacji, oznaczając lokalizację lub pokazując bilet lotniczy nieświadomie narażamy się na szereg niebezpieczeństw.

Oznaczając zdjęcie z miejsca wypoczynkowego dajemy sygnał przestępcom, że nie ma nas w domu. Zaś wstawiając zdjęcia biletów (np. lotniczych) lub udostępniając dokumenty, udostępniamy nasze dane, np. adres zamieszkania, numer telefonu, a czasem nawet numer PESEL.

Zanim podzielisz się wspomnieniami z wakacji, pamiętaj:

- nie wstawiaj zdjęć, na których widoczne są dane osobowe lub inne informacje, które mogą posłużyć do przestępstwa lub głupiego żartu,
- publikuj zdjęcia i informacje po powrocie z urlopu, nie informuj potencjalnych przestępców o terminie wyjazdu czy powrotu z wakacji,
- zadbaj o ustawienia prywatności na portalach społecznościowych.

16. Numery, które warto znać

112 – europejski numer alarmowy,
997 – policja (Centrum Powiadamiania Ratunkowego),
998 – straż pożarna (Centrum Powiadamiania Ratunkowego),
999 – pogotowie ratunkowe (Centrum Powiadamiania Ratunkowego),
987 – centrum zarządzania kryzysowego,
991 – pogotowie energetyczne,
995 – Komenda Główna Policji – system Child Alert,
601100300 – numer ratunkowy w górach,
601100100 – numer ratunkowy nad wodą,
116000 – numer dla rodziców i opiekunów, którym zaginęło dziecko,
116111 – telefon zaufania dla dzieci i młodzieży
116123 – kryzysowy telefon zaufania (dla dorosłych).

Pamiętaj!

Te numery mogą uratować komuś życie.
Nie blokuj ich bez powodu.

Opracowanie merytoryczne: Milena Górecka, Agnieszka Osełka
Opracowanie graficzne: Wojciech Gunia