



# Poradnik wakacyjny UKE 2023



Czas wakacji powinien być okresem relaksu i odpoczynku. Planując urlop warto pamiętać o podstawowych zasadach bezpieczeństwa i korzystania z usług telekomunikacyjnych.

## Korzystanie z usług telekomunikacyjnych

### Roaming i zasada RLAH

Aby skorzystać z roamingu włącz usługę roamingu u swojego dostawcy. **Włączenie/ wyłączenie roamingu jest bezpłatne** i odbywa się:

- za pomocą krótkich kodów USSD,
- poprzez kontakt z biurem obsługi klienta operatora.

Dostawcy usług **muszą informować Cię o kosztach realizacji usług w danym kraju**, niezależnie czy jest on częścią Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, czy też nie. Powinieneś otrzymać SMS z informacją za każdym razem, gdy przekraczasz granicę danego państwa.

Na terenie Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego (UE/EOG) opłaty są rozliczane według zasady RLAH (Roam Like At Home). 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. Zgodnie z zasadą RLAH **opłaty w roamingu powinny być takie same jak opłaty za korzystanie z usług w kraju**, a w przypadku dostępu do internetu operator przyznaje Ci







określony limit transmisji danych.

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, operator 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 dodatkową wykorzystaną jednostką danych.

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



## Jaka jest różnica pomiędzy roamingiem a połączeniem zagranicznym?

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.

Gdy dzwonisz **z Polski do USA (kierunkowy +1) czy do Niemiec (kierunkowy +49) wykonujesz połączenie międzynarodowe**.

Za to połączenie zapłacisz zgodnie z cennikiem dostawcy.







## 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 połączyć się z zagraniczną siecią.

Twój dostawca naliczy opłaty zgodnie z obowiązującym cennikiem. Jeśli połączysz się z siecią operatora spoza Unii Europejskiej, 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
- i pocztę głosową.

To pozwoli Ci uniknąć dodatkowych kosztów za usługi.





## Jak skorzystać z usług telekomunikacyjnych 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, będziesz mógł korzystać z usług roamingu UE.

Problem braku zasięgu na otwartych akwenach wodnych 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 pułapami cen obowiązującymi w UE.

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





## Oddzwaniaj z głową!

W wakacje nasila się aktywność oszustów wykorzystujących naszą skłonność do oddzwaniań 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.** Pamiętaj, że 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 numer kierunkowy to +48 lub 0048.





## Jeśli chcesz uniknąć kosztów, zablokuj usługi Premium Rate

Premium Rate to usługi o podwyższonej opłacie. Zanim skorzystasz z usługi specjalnej, przeczytaj jej regulamin. **Dostawca usług domyślnie zablokuje usługi Premium, kiedy wydasz na nie 35 zł w ciągu miesiąca/okresu rozliczeniowego.**

Możesz wybrać całkowitą blokadę usług o podwyższonej opłacie. Możesz zablokować:

- wychodzące lub przychodzące wiadomości
- wybrane lub wszystkie numery Premium

Jeśli świadomie, często korzystasz z usług Premium Rate, nie musisz blokować tych usług. **Możesz wybrać inny próg kwotowy** 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.



## 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.

Pamiętaj, że **dostawca usług nie odpowiada za szkody powstałe w skutek 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.



## Bezpieczeństwo w sieci

### Zadbaj o urządzenia w podróży

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
- zrób kopie zapasowe
- pamiętaj o aktualizacji oprogramowania i programie antywirusowym
- usuń poufne dane z telefonu
- nie zapisuj i nie udostępniaj haseł logowania





## Publiczne sieci Wi-Fi

Jesteś w hotelu, 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 za granicą. 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.) Urządzenia mobilne często automatycznie wyszukują niezabezpieczone hasłem lub znane im punkty dostępowe.

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 się do wrażliwych kont osobistych (np. bankowość online, poczta elektroniczna)





## 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 do naszego wyjazdu.

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

Jak ustrzec się phishingu?

- zachowaj czujność, jeśli jakaś oferta wydaje się zbyt piękna, 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



## 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 SMS-ów wraz z linkiem do pobrania aplikacji, która umożliwi 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 SMS-ów
- 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.





## Uważaj na oszustwo z BLIKiem!

W wakacje często nasila się zjawisko włamań na konta na portalach społecznościowych. Dzięki temu oszuści mogą naciągać naszych znajomych na pożyczki, wykorzystując do tego elektroniczne metody płatności. Przesiępca 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 takiej 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**





## 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 kierunku 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
- zadbaj o ustawienia prywatności na portalach społecznościowych



## 11 numerów, 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

Pamiętaj!

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



Szukasz porady? Skontaktuj się z **Centrum Informacji Konsumentckiej**

22 330 40 00 (tonowo 1)

pn. – pt. 8:15 – 16:15

**[cik.uke.gov.pl](http://cik.uke.gov.pl)**





Opracowanie merytoryczne: Wydział Kampanii Informacyjno-Edukacyjnych UKE

Opracowanie graficzne: Wydział Komunikacji UKE

Źródło zdjęć: stock.adobe.com