

UKE HOLIDAY GUIDE NOV





When planning a holiday, it is worth to remember the basic safety rules that will allow you to enjoy your holiday without unnecessary worries.

In this guide you will find practical tips on how to protect yourself, your loved ones and your assets when using telecoms services while travelling.

You will find information about:

- When are you charged for roaming services?
- Is it safe to call back unknown number?
- Can a holiday storm damage devices at home?
- Is using a hotel Wi-Fi safe?
- Is it safe to post your photos from holidays online?

We wish you a happy, safe holiday
and enjoy the read:)

Table of contents:

1. [Roaming and RLAH rule](#)
2. [Limits on data roaming charges](#)
3. [The difference between roaming and International call](#)
4. [Beware of border roaming](#)
5. [Does the RLAH rule apply on a ferry or ship?](#)
6. [Be cautious about returning missed calls!](#)
7. [Block premium rate services](#)
8. [Protect your equipment against storms](#)
9. [Take care of your devices while travelling](#)
10. [Public WIFI networks](#)
11. [Beware of phishing!](#)
12. [Beware of false apartment reservations](#)
13. [Summer deals hunters](#)
14. [Beware of BLIk fraud!](#)
15. [Share memories, not data](#)
16. [Phone numbers worth knowing](#)





1. Roaming and RLAH rule

Roaming is a mechanism that allows mobile telecommunications services to be used while a subscriber is within range of another service provider. We use roaming most frequently when travelling abroad.

Your service provider must inform you of costs of roaming services, regardless of the country you are visiting. You should receive an SMS with information on the price of services every time you cross a country's border – even if the price is 0 zloty.

Within the European Union or European Economic Area (EU/EEA) charges are billed according to the Roam like at Home (RLAH) rules. According to the RLAH rule, roaming charges should be the same as the charges for using the same services at home and in case of internet access, your service provider may give you a certain data transmission limit, after which it will start to charge you. When you travel from Poland to another EU/EEA country, your service provider may not charge you additional fees, except under the Fair Use Policy or if your service provider has obtained approval from the President of UKE to apply additional fees.

2. Limits on roaming data charges

Service providers are obliged to protect their subscriber from high data costs within the EU/EEA. Outside the EU/EEA, such an obligation also exists as long as the foreign network operator allows monitoring of data consumption.

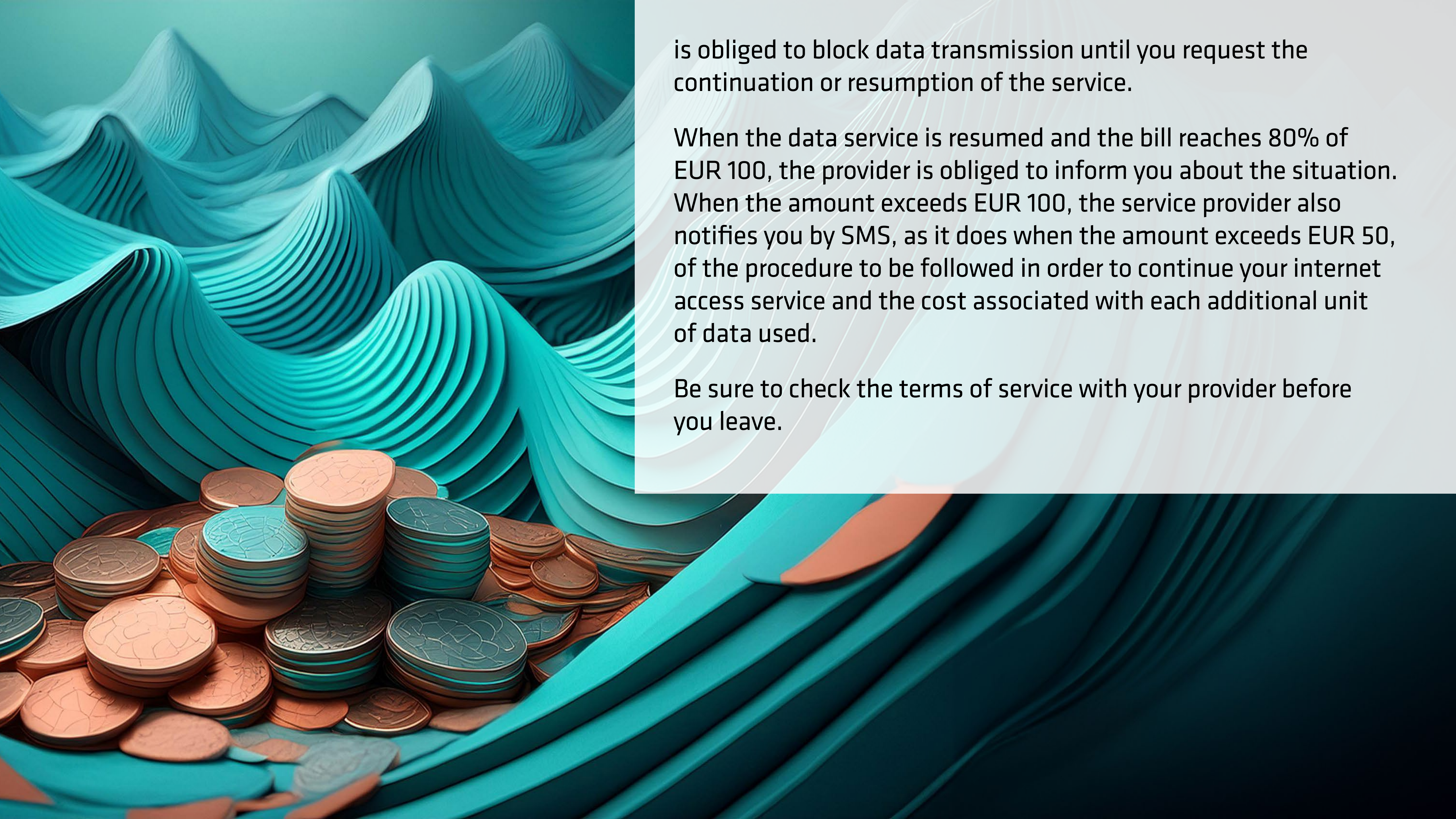
As a standard subscriber protection mechanism, operators must set a default limit of the equivalent of 50 EUR per month and the equivalent of 100 EUR per month for data roaming.

When your data roaming bill reaches 80% of EUR 50, your service provider must inform you about that. Once the amount of EUR 50 is exceeded, the service provider notifies you by SMS:

- the procedure to be taken to continue your internet access service,
- the cost associated with each additional unit of data used.

If you do not respond to the notification, the provider





is obliged to block data transmission until you request the continuation or resumption of the service.

When the data service is resumed and the bill reaches 80% of EUR 100, the provider is obliged to inform you about the situation. When the amount exceeds EUR 100, the service provider also notifies you by SMS, as it does when the amount exceeds EUR 50, of the procedure to be followed in order to continue your internet access service and the cost associated with each additional unit of data used.

Be sure to check the terms of service with your provider before you leave.

3. The difference between roaming and International call

A call in roaming is when you make a call from Polish phone number while abroad. It does not matter where you call – to a Polish or foreign number. The important thing is that your phone is logged into the foreign network.

If you are sitting on a beach in Greece or eating a pizza in Naples and you call your family in Poland or a friend in Germany, you are making a roaming call.

However, when you call from Poland to the USA or Germany, you are making an international call. You will pay for this call as an international call, according to your provider's price list. The RLAH rule does not apply to international calls.





4. Beware of border roaming

In a border area, if your phone has automatic network selection set, it may log on to the network of a foreign service provider having a stronger signal in the area. Remember that when you are close to a border, you can automatically connect to a foreign network. Your service provider will then charge you according to the applicable roaming price list. If you connect to the network of a non-EU/EEA operator, the charges will be much higher.

When going to border areas, set your phone to manually select the network. You will be assured that calls will be made on your service provider's network.

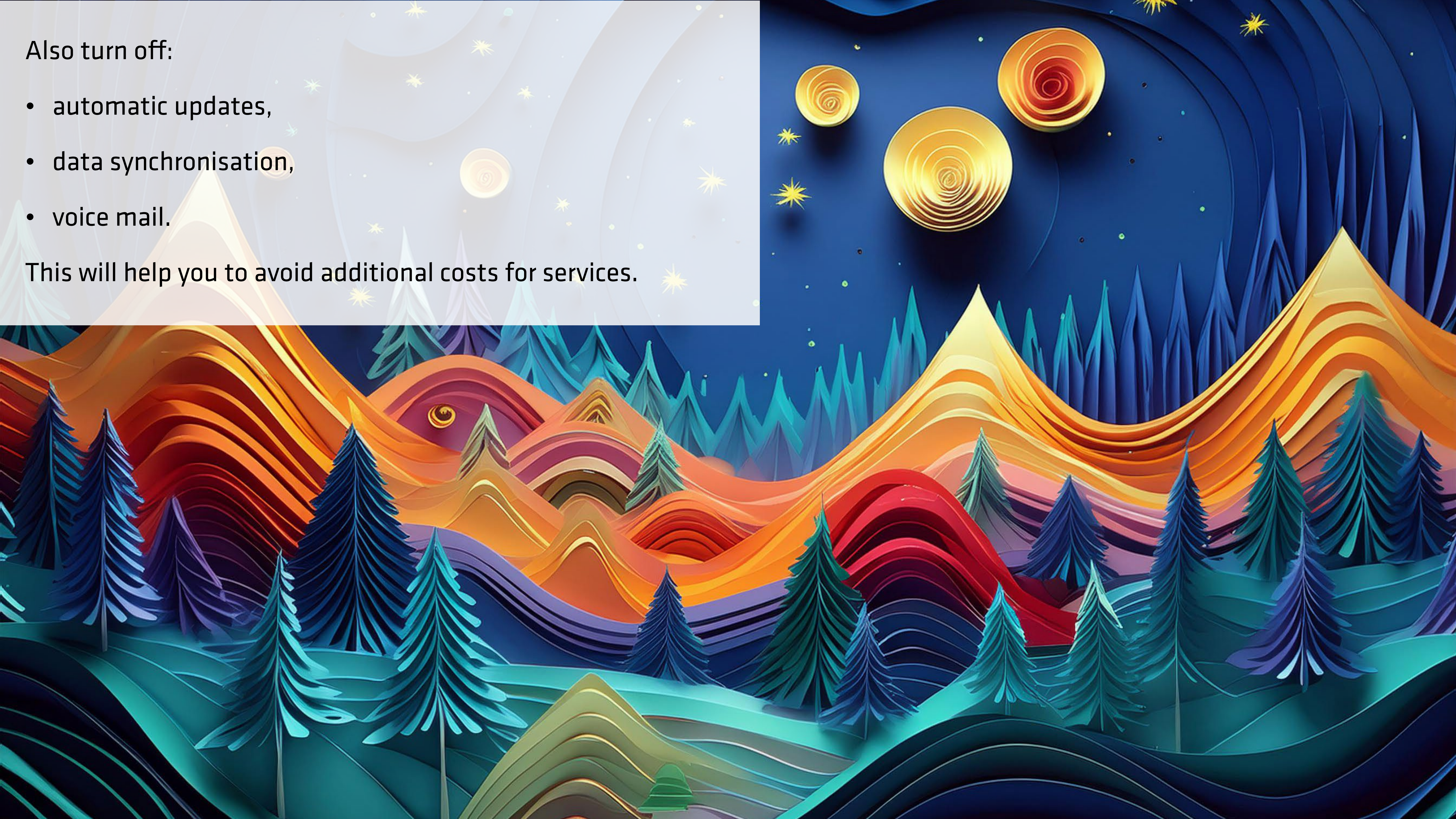
You can also:

- disable foreign roaming completely - then your phone will not connect to foreign networks;
- disable data roaming abroad itself - then your phone will not connect to the internet.

Also turn off:

- automatic updates,
- data synchronisation,
- voice mail.

This will help you to avoid additional costs for services.





5. Does RLAH rule apply on a ferry or ship?

If your mobile phone is connected to a terrestrial mobile network (e.g. when travelling on a river, lake or along the coast) in one of the EU/EEA countries, you will be able to roam according to the RLAH regulation.

The problem of lack of coverage in open waters is solved by satellite networks. EU roaming regulations only apply to terrestrial mobile networks. If, during your cruise, mobile services are provided over other types of radio networks, such as a ship's satellite systems, your calls, SMS and data transmission will not be covered by the RLAH rule.

You will find the costs for voice calls, SMS messages and data transfer in the price list of your provider or the respective satellite network operator.

6. Be cautious about returning missed calls!

During vacation time there may be an increasing activity of scammers taking advantage of our tendency to return missed calls

If you are not expecting a call from abroad and the phone number displayed on your screen is remarkably long – be careful! Polish numbers, both mobile or landline, have 9 digits. By keeping this rule in mind you may avoid an unwanted, expensive call.

Some of the African prefixes deceptively resembles those assigned to Polish cities. For example, +225 is Ivory Coast, and 22 in this case may be confused with the area code of Warsaw.

Remember! Polish area code prefix is +48 or 0048.





7. Block the premium rate services

Your service provider will block possibility to use premium rate services by default when you spend 35 PLN on them in a month/ settlement period.

You may choose to block such services completely. You may block:

- outgoing or incoming messages,
- selected or all premium rate numbers.

If you consciously, often use these services, you do not need to block them. You may choose a different spending limit threshold, for example 100 zloty, beyond which your provider will block further use of the services.

You can also avoid additional costs by activating your payment block for extra services, electronic purchases, i.e. direct carrier billing, that is automatic payments added to your bill. Contact your service provider and have your blocking activated.

8. Protect your equipment against storms

Summer is a time of frequent lightning strikes. A short circuit may happen during a storm and, for example, a router or decoder may break down.

Remember that the service provider is not liable for damage resulting from so-called force majeure. We deal with it when an event comes from outside, is extraordinary and cannot be predicted. Force majeure may include, for example, lightning.

Make sure to protect your modem, router or computer against damage caused by surges. Before a storm, disconnect household appliances from electricity. There are also devices available on the market that protect the equipment against such situations.





9. Take care of your devices while travelling

A smartphone, laptop or tablet is a huge source of data. Devices contain a lot of information about us, our friends, habits, work and our sensitive data.

We have banking applications, e-mail, photos and documents installed on our smartphones. To protect this data, you must remember to protect your device.

- set a screen lock on each device,
- make backups regularly,
- remember about antivirus program and to update your software,
- delete confidential data from your phone,
- do not write down or share login passwords

10. Public WI-FI Networks

Are you in a hotel, gallery, restaurant or airport and want to use a public Wi-Fi network (Hotspot)? This will help you avoid high data transfer fees, especially when you are outside the EU/EEA. However, be careful because connecting to an unsecured network without a password may have negative consequences!

Cybercriminals can create fake Wi-Fi access points. Such hotspots make it possible to intercept part of the data sent by users to websites (e.g. bank, store, etc.).

If you use Wi-Fi, remember the safety rules:

- when connecting to Wi-Fi, do not select the option to remember it on your smartphone,
- make sure that the access point belongs to the place to which it is assigned,
- regularly update your device's operating system,
- install an antivirus application on your smartphone
- if you must use a public network, avoid logging in to sensitive personal accounts (e.g. online banking, email).





II. Beware of phishing!

Phishing is a fraud through which we can unknowingly provide criminals with our personal data such as logins, passwords or payment card numbers. Moreover, we will be convinced that we are providing the information to an institution we know - e.g. a travel agency.

During the holiday season, many people look for travel offers, browse websites offering accommodation or cheaper tickets. Fraudsters can create fake websites and send e-mails and text messages in which they ask, for example, to provide personal data or transfer the amount that is allegedly missing in the payment for our trip.

To avoid this, carefully check the address of the link you received or contact the company from which you allegedly received the information.

How to avoid phishing?

- be vigilant, if an offer seems too good or cheap to be true, it is probably fake
- pay attention to the domain address and the appearance of the website,
- check if you know the sender who is sending the message with the link you should click,
- verify at the source (e.g. a travel agency) whether it sent a message requesting data update, additional payment, etc.,
- when making reservations and purchasing tickets, use trusted websites by entering the website address manually in the browser bar,
- update the browser you are using to the latest version offered by the manufacturer,
- remember about antivirus software,
- change your passwords regularly,
- use different passwords for different accounts and remember that your passwords should be strong and difficult to crack.





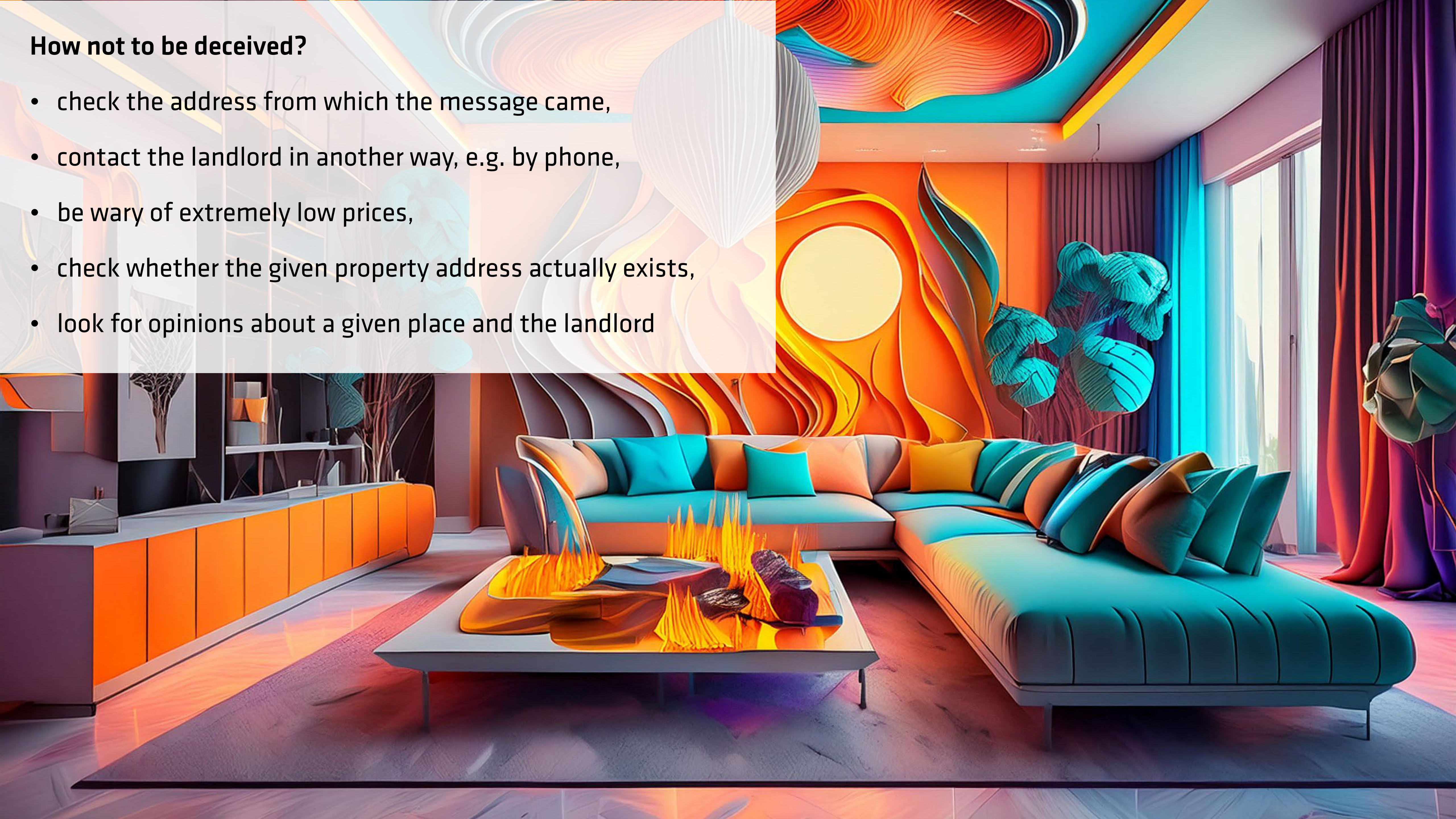
12. Beware of false apartment reservations

Holidays, festivals and concerts of famous artists are an excellent opportunity for fraudsters to rent non-existent apartments, flats or rooms. False offers can be found not only on websites dealing directly with real estate rentals, but also from brokers.

There were also cases of e-mails being sent to customers of a well-known portal with information about the need to provide additional data necessary to confirm the reservation or the need to pay an additional fee. The fraudsters relied on fear and haste, as the fake message contained information that if no action is taken, the reservation will be cancelled. In fact, the sent link was to a fake website where fraudsters extort personal data and payment card details.

How not to be deceived?

- check the address from which the message came,
- contact the landlord in another way, e.g. by phone,
- be wary of extremely low prices,
- check whether the given property address actually exists,
- look for opinions about a given place and the landlord





13. Summer deals hunters

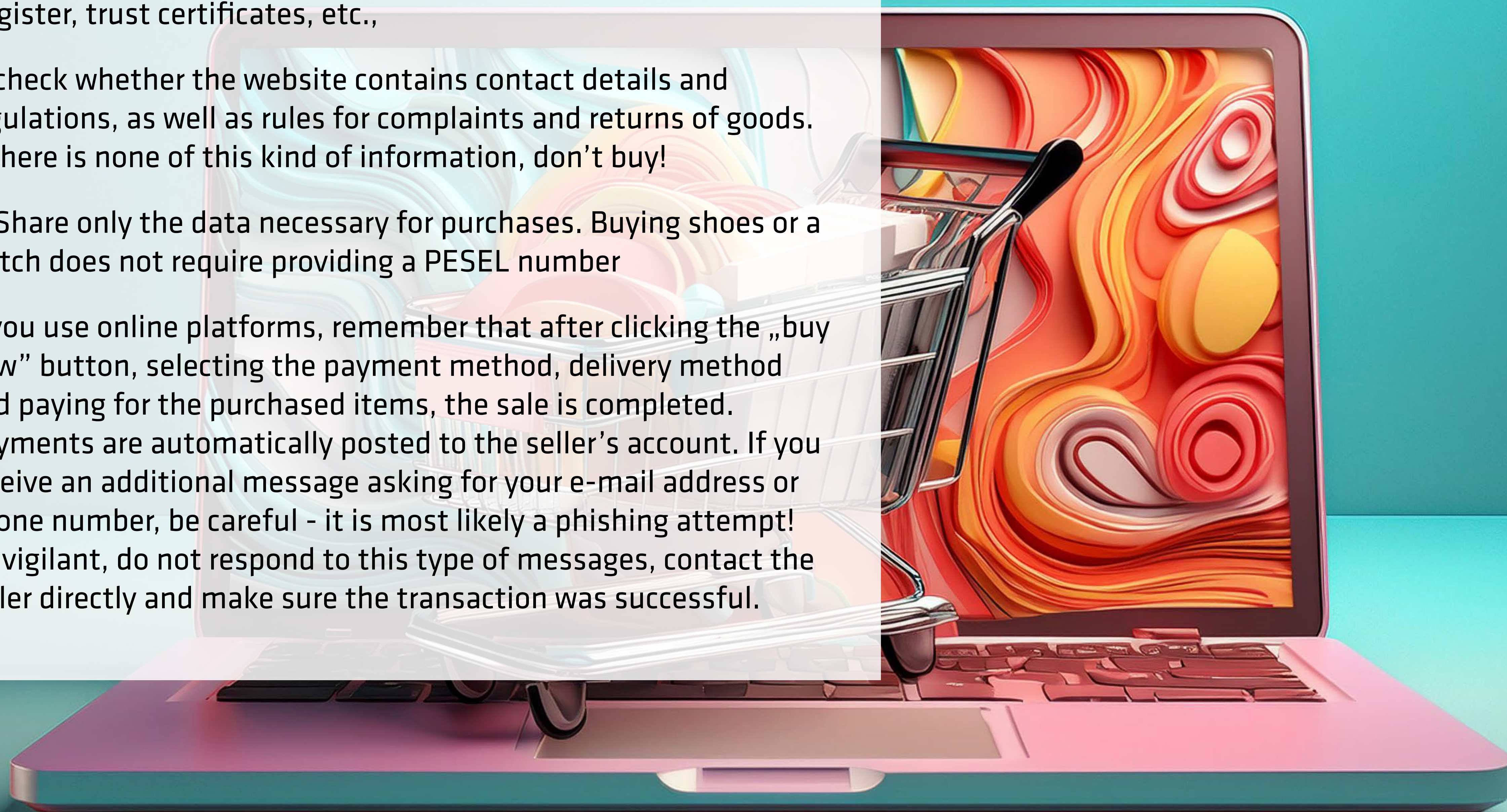
Holidays are a time when stores offer us promotions for online shopping, discount coupons, etc. This is used by online fraudsters who can impersonate well-known brands. A common scheme is to send mass text messages with a link to download an application that offers a supposed discount on purchases. By clicking on such a link, you expose yourself to the risk of downloading malware, losing data, or even stealing funds from payment cards and taking complete control over the device.

- do not open attachments and links from suspicious e-mails and text messages,
- check sources, e-mail addresses and message content,
- pay attention to typos and lack of Polish characters,
- do not share logins and passwords,
- do not share payment card details,
- before making purchases, check the credibility of the seller: look for information about him, the history of previous

transactions, check whether he has an entry in the National Court Register, trust certificates, etc.,

- check whether the website contains contact details and regulations, as well as rules for complaints and returns of goods. If there is none of this kind of information, don't buy!
- Share only the data necessary for purchases. Buying shoes or a watch does not require providing a PESEL number

If you use online platforms, remember that after clicking the „buy now” button, selecting the payment method, delivery method and paying for the purchased items, the sale is completed. Payments are automatically posted to the seller's account. If you receive an additional message asking for your e-mail address or phone number, be careful - it is most likely a phishing attempt! Be vigilant, do not respond to this type of messages, contact the seller directly and make sure the transaction was successful.





14. Beware of BLIK fraud!!

Hacking into social media accounts increases during the holidays. Thanks to this, fraudsters can trick our friends into loans using electronic payment methods. The criminal, impersonating us or a person we know, tries to obtain a BLIK code, which we will confirm during authorization.

If we receive a request for a loan or to make a BLIK payment for someone, let's call that person directly. Let's verify whether he really needs such a payment. Often, during a conversation, it turns out that our friend's profile has been taken over by fraudsters, and the person concerned does not have access to it.

Bank regulations usually include provisions that one-time passwords (such as the BLIK code) cannot be made available to third parties. If we ourselves provide the code to a fraudster, we must take into account that the bank will not accept our complaint.

Remember:

- do not make transfers in situations that raise your doubts,
- watch out for „fast” payments,
- never share your passwords and codes





15. Share memories, not data

While enjoying the charms of holidays and visiting new places, it's hard to resist the temptation to publish photos and videos on social media. However, it is worth to wait and pay attention to what we post online. By posting holiday photos, tagging the location or showing the plane ticket, we unknowingly expose ourselves to a number of dangers.

By tagging a photo from a resting place, we give a signal to criminals that we are not at home. And by inserting photos of tickets (e.g. airline tickets) or sharing documents, we provide our data, e.g. residential address, telephone number, and sometimes even PESEL number.

Before you share your holiday memories, remember:

- do not post photos containing personal data or other information that could be used for a crime or a stupid joke,
- publish photos and information after returning from vacation, do not inform potential criminals about the date of departure or return from vacation,
- take care of your privacy settings on social networking sites.

16. Phone numbers worth knowing

112 – European emergency number,

997 – police (Emergency Notification Center),

998 – fire brigade (Emergency Notification Center),

999 – emergency service (Emergency Notification Center),

987 – crisis management center,

991 – energy emergency,

995 – Police Headquarters – Child Alert system,

601100300 – mountain rescue number,

601100100 – water rescue number,

116000 – number for parents and guardians whose child is missing,

116111 – helpline for children and young people

116123 – crisis helpline (for adults).

Remember!

These numbers could save someone's life. Don't block them for no reason.



The image features a vibrant, layered paper art landscape. In the center, a circular frame contains a bright sun with orange and yellow rays, set against a backdrop of blue and teal mountains. The sun is partially obscured by the mountain peaks. The entire scene is surrounded by a dense forest of stylized evergreen trees in shades of brown, orange, and teal. The background consists of more layers of paper art, creating a sense of depth and texture.

Consumer Information Center

cik.uke.gov.pl

Text: Milena Górecka, Agnieszka Osełka
Translation: Jadwiga Mrozowska, Kinga Cielemecka
Design: Wojciech Gunia