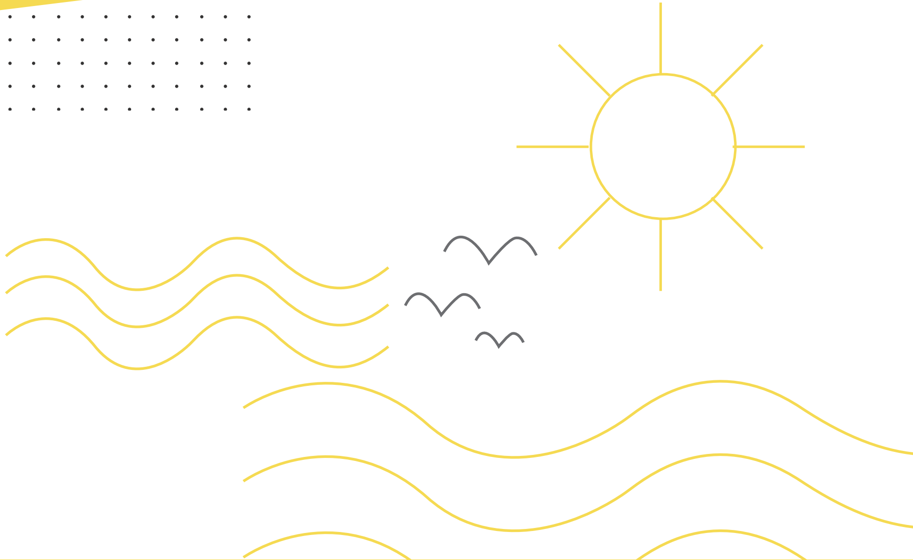
NaviRisk

www.wearenavirisk.com



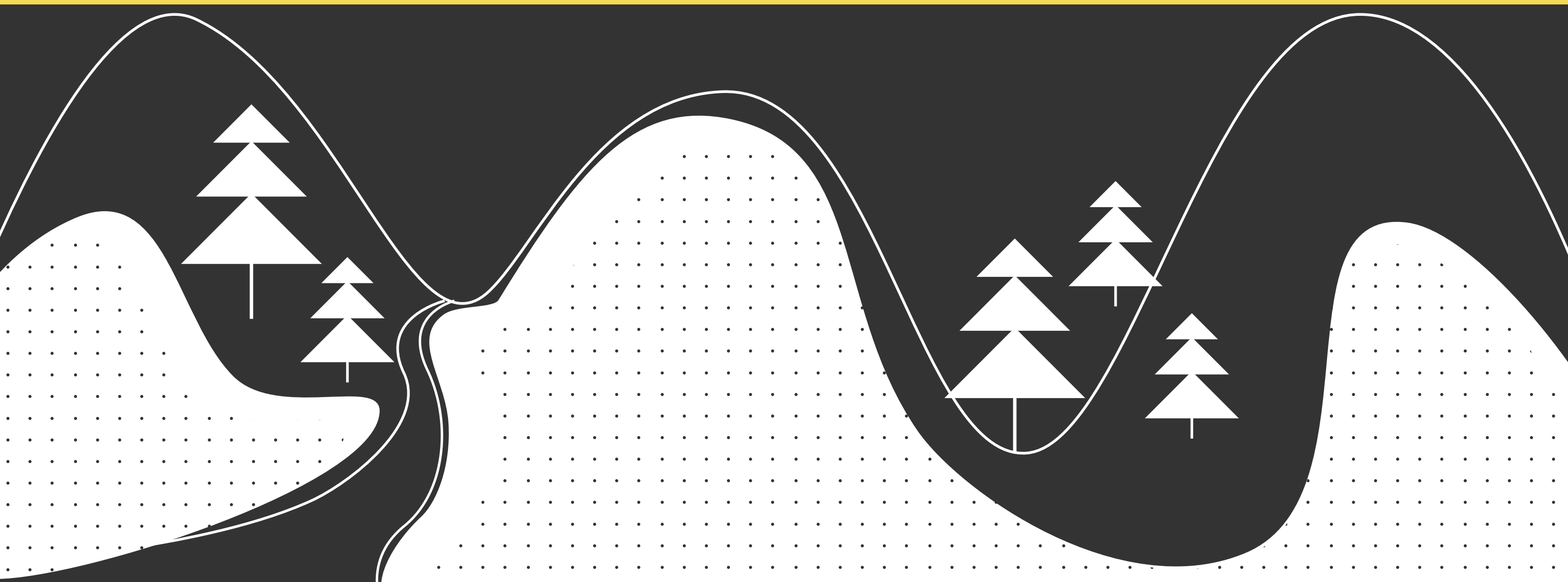
Holiday cybersecurity with NaviRisk

CYBER GUIDE

The holiday season is almost here. Is Everyone hungry for sun and rest? We are excited to search for the perfect vacation, trying to provide ourselves and our loved ones with a beautiful time and unforgettable impressions.

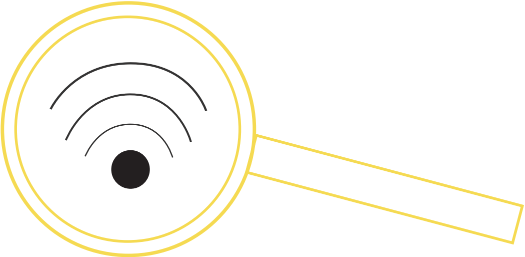
We usually take many precautions when going on vacation. We buy travel insurance, keep our wallets in our front pockets, and do not keep all cards, documents, and cash in one place.
We should also take similar precautions in cyberspace. Cybercriminals want our money just like any other thief. If they cannot reach for it directly, they will be happy to extract any valuable information from us that they can monetize.

Therefore, for an unforgettable experience to be only positive, make sure you are safe by following the tips below:



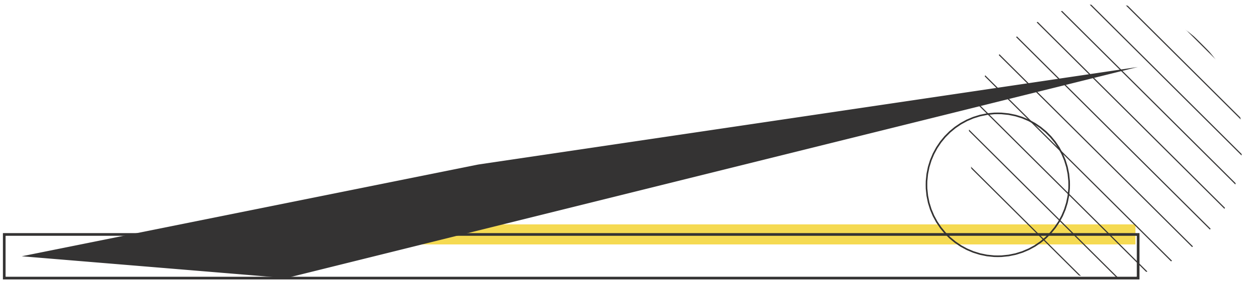
1 Avoid public Wi-Fi hot spots.

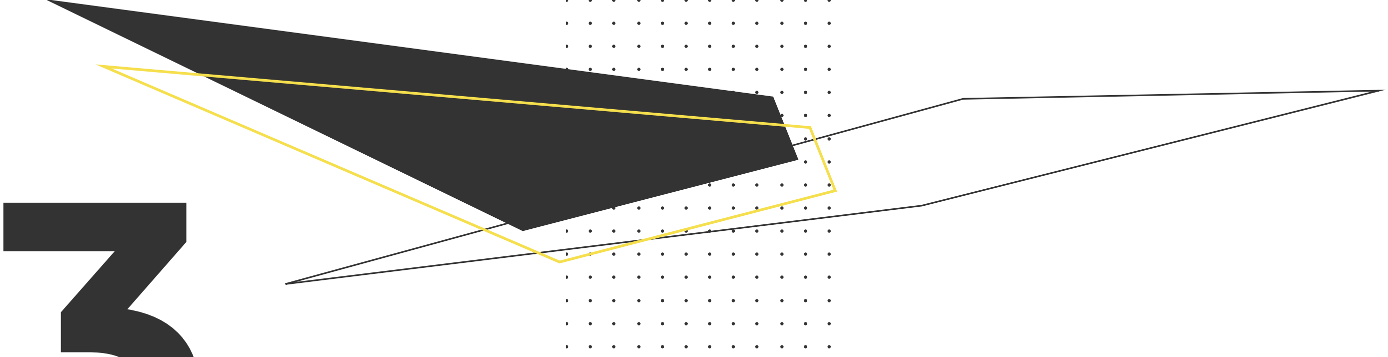
Be especially careful when using internet cafes and free Wi-Fi hot spots. In particular, free Wi-Fi access, although attractive, can seriously threaten your data's security. So if you have to use them, use VPN to encrypt the transmission or avoid logging into sensitive personal accounts (e.g. online banking) or browsing confidential data. To avoid using public networks, e.g., navigation, load all the most important locations in the form of offline maps beforehand. It is not uncommon for cybercriminals to connect to publicly available networks or hotel chains looking for weak, unsecured devices. Use reasonable AV solutions, anti-malware, and other protection elements on your computer and smartphone to minimize the risk of your device being hacked on an untrusted network.



2 Disable automatic connection to Wi-Fi.

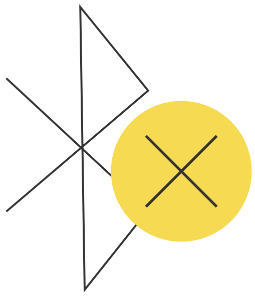
Many phones have a setting that allows them to connect to a Wi-Fi network when it is available automatically. While this feature can be very convenient at home or in the workplace, it is better to be careful with it when you are away. It won't let you decide which network you want to connect to and which not. In addition, according to recent studies, when searching for Wi-Fi available and connection attempts, some smartphone models often send unsecured information about remembered Wi-Fi networks that your device used to connect to in the past, and these are not only the names of these networks.





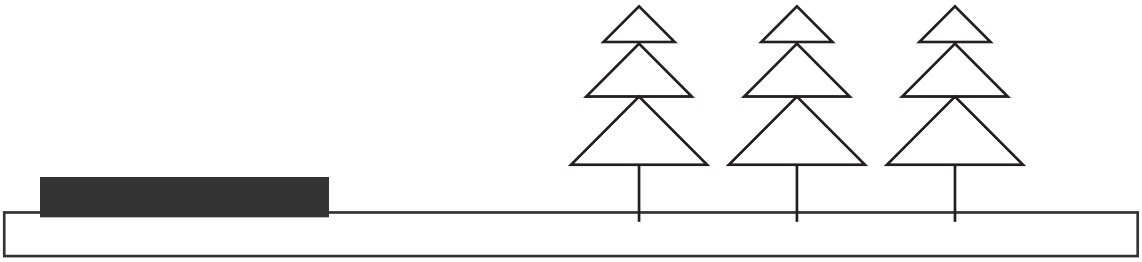
3 Turn off Bluetooth when not in use.

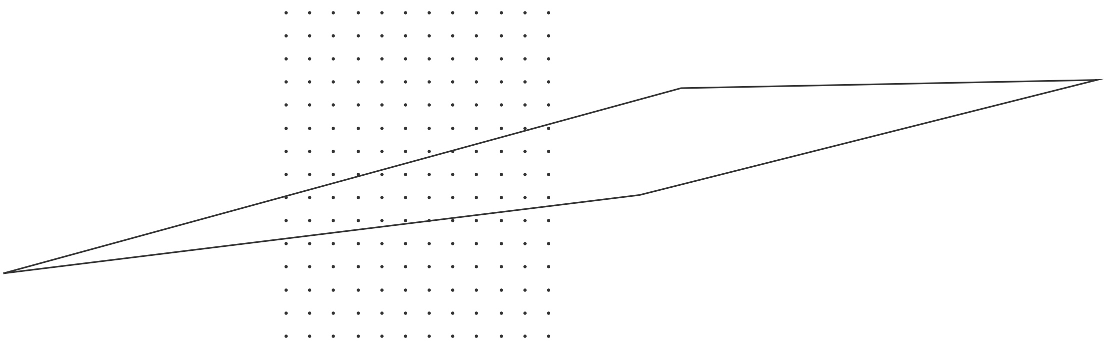
Like automatic Wi-Fi on your phone, Bluetooth connectivity, signals from anywhere can also be problematic. If your Bluetooth remains on, attackers in the vicinity may try to connect to your phone and potentially hack the device by exploiting some vulnerability of the Bluetooth protocol or its implementation on your device. So turn on Bluetooth only when you intend to use it. Remember that in the case of Apple devices, it is not enough to "un-click" the Bluetooth or Wi-Fi icon in the Control Center to disable the services permanently. In addition, with Bluetooth turned off, the device uses less energy. Go to Settings and switch it off from this level.



4 Beware of those looking over your shoulder.

The person sitting next to you can have excellent insight into all the data you enter. To avoid such situations, you can buy a screen protector to help hide your laptop or mobile phone from unauthorized eyesight. Check if there are no cameras behind you, above, or next to you, pointing at the monitor, phone screen, or keyboard. Be especially careful when performing operations where confidentiality is of particular importance to you.

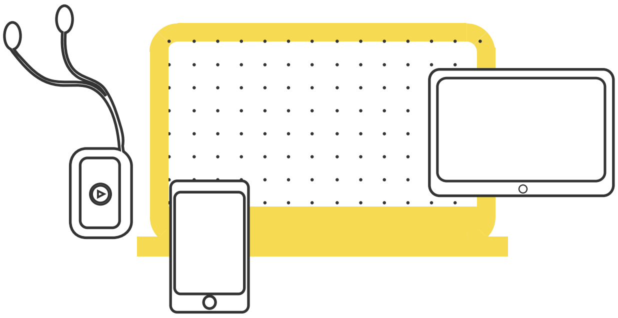




5

Secure your data.

Do not leave your computer, phone, or tablet unattended. Remember to block access to it whenever you move away from the equipment. Make sure your password is strong and preferably use two-factor authentication. You must encrypt your computer, phone, or portable drive if you do not want your data to fall into the wrong hands in the event of loss or theft of equipment. Also, remember to back up your valuable data before you leave.



6

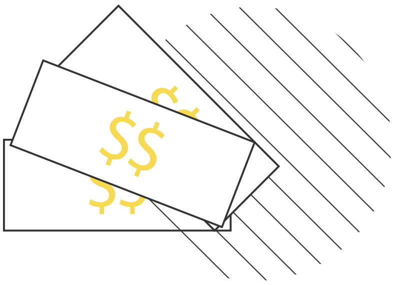
Do not share the equipment others.

Your devices (especially your smartphone) are a huge source of information. Be suspicious if someone asks you to use your phone. If a stranger needs help, it is better to make the call yourself than share the device.

7

Update your software and install a good antivirus.

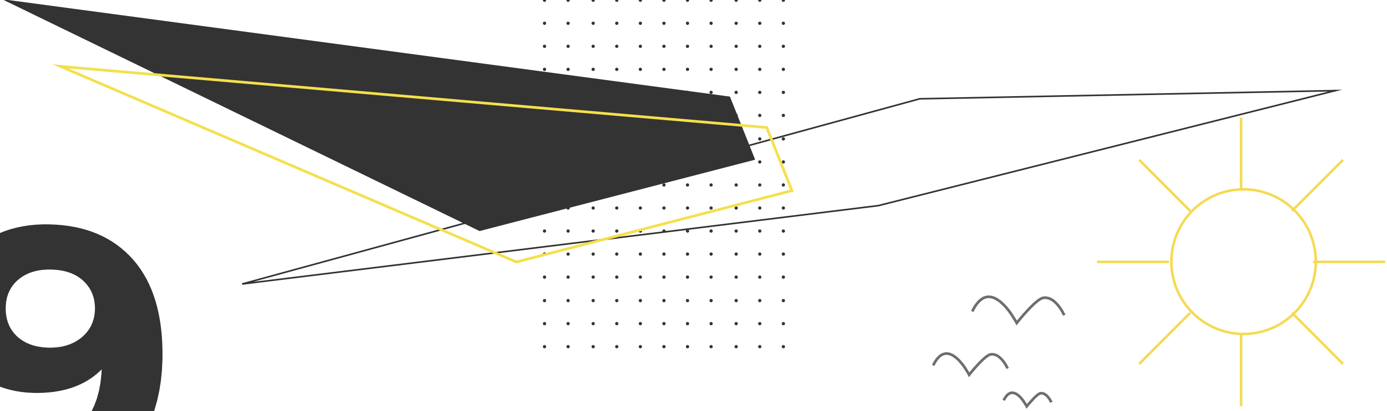
Installing an antivirus should be self-explanatory - after all, it's essential to protecting any hardware. Make sure that each device on vacation has an up-to-date and proven antivirus program so that no malware gets into your data and spoils your trip. Failure to update makes your devices vulnerable to cybercriminal attacks and increases the likelihood of installing malware (which is currently one of the most commonly used forms of attack).



8

Withdraw money only from proven ATMs.

Avoid withdrawing cash from unmonitored ATMs. Cybercriminals, especially tourist areas, often connect tools to ATMs that steal credit and payment card credentials. Use ATMs located in bank branches, preferably inside buildings, reducing the risk of robbery.

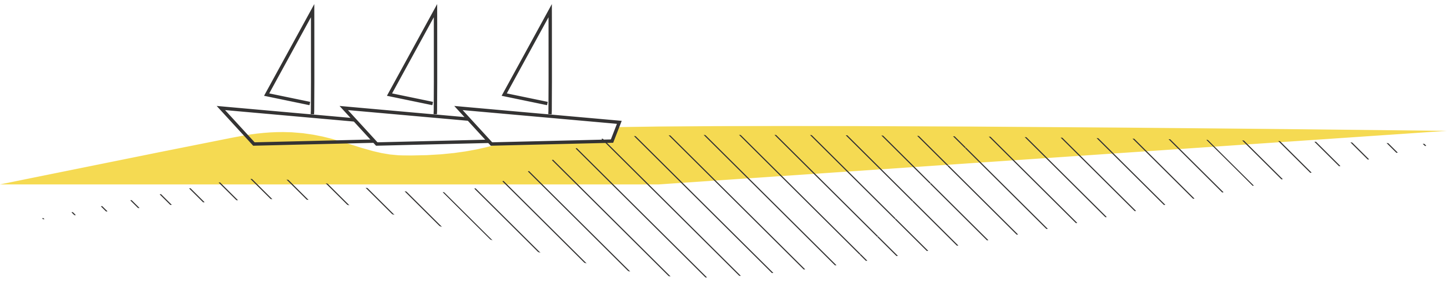


9 Do not leave documents "as collateral".

Do not leave documents "as collateral", e.g. at sports equipment rental points. The person who requests to leave an identity document in exchange for renting the equipment is acting against the law! The Polish Act on the Protection of Personal Data and the EU Regulation (GDPR) are violated. By succumbing to such practices, you risk losing control of your data, which may end up in illegal use. It is an excellent practice to have a "business card", preferably in the shape of an ID card, with data you can leave behind without too much risk. Before going to a foreign country, particularly outside the European Economic Area, it is worth getting acquainted with the local customs in this regard.

10 Be careful when copying your documents.

If someone needs to scan or photocopy your passport or other documents, the first thing to check is whether they have the right to do so according to the applicable regulations and if it is necessary for a specific purpose. If so, let the scan/photocopy be performed in your presence and make sure you get a sign of a declaration of such activity. Cover the document with data that are not required at the moment and remember that the scan/photocopy should contain information that it is a scan/photocopy of the document made on a specific date by a particular entity.



11

When using generally available equipment (e.g. a computer in a hotel or an internet cafe), follow the most important safety rules:

As a rule, we advise against using generally available equipment, but in an emergency, when you have no other option, follow the good practice:

Use portable software. A suitable method for safely using computers in public places is to use portable software that does not require installation in the operating system and can be run directly from a USB key.

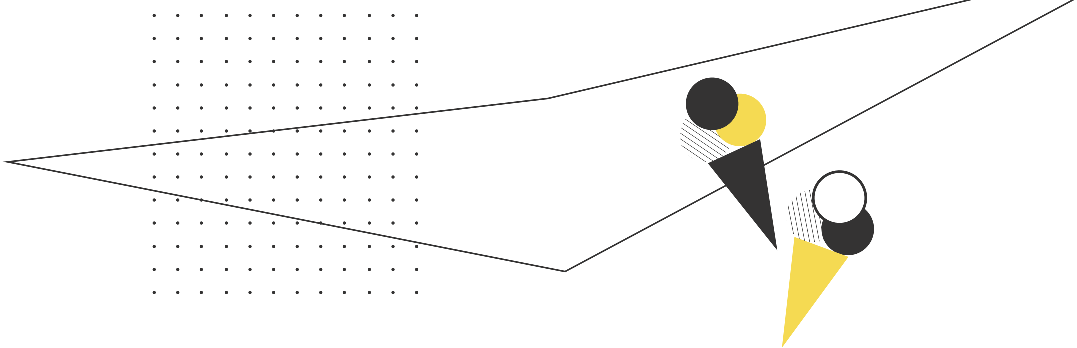
Use the computer in isolation. Always try to use your computer in the most secluded place possible.

Don't leave any files. Under no circumstances should you leave any downloaded files on the computer, especially your files. To ensure the files are deleted, use special applications for irreversible data deletion.

Remove traces of your activity. Remove any private data from your web browser. In particular: the history of pages viewed, cookies, and passwords. If possible, use a private (incognito) mode that does not save browsing data, sessions, or cookies.

Don't give out confidential information. When using a public computer, try not to make purchases and avoid websites that require you to enter confidential information such as credit card numbers, service passwords, or PINs. However, if necessary, it will be a good practice to change the passwords once you have access to a trusted device. Remember that in most cases, it will be safer if you call someone you trust (who will be able to do this on their computer) to do the steps above. While this violates the non-disclosure of credentials policy, it will often be less risky.

Remember to log out and restart. After finishing your work, do not forget to log off and restart your computer. Thanks to this, you can be sure that the RAM memory will be cleared of data and that another user of a public computer will not have access to data from your session.



12

Leave your equipment at home.

If possible, leave primary devices (computer, smartphone) on which you have a large amount of information you want to protect at home, and take spare devices - containing only the necessary data - on your trip.

13

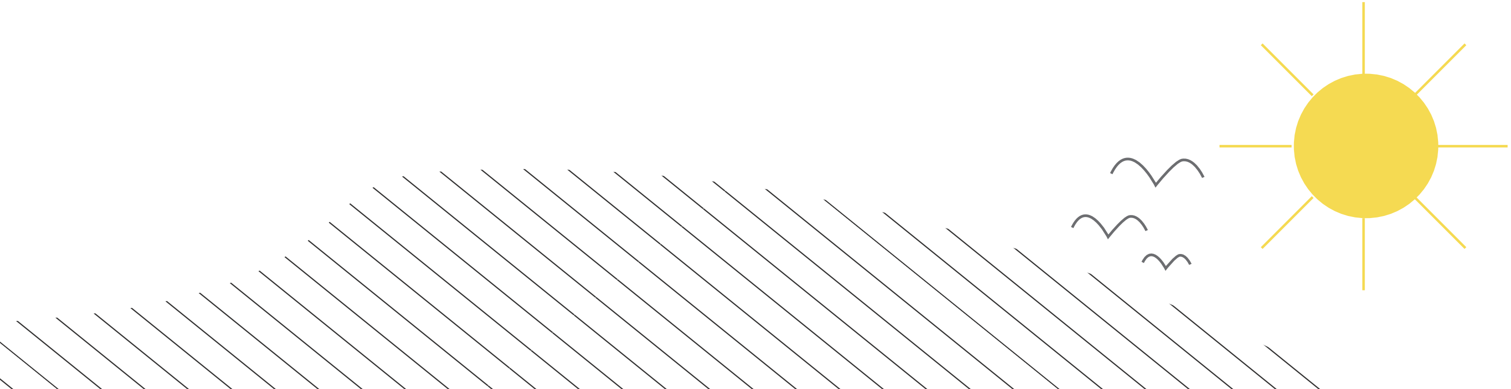
Get support.

Make sure that a trusted person who remains in place during your trip can safely access your data (e.g. bank account) or make a specific order with the service provider in case you need help.

14

Check their rules.

When travelling abroad, especially to high-risk countries, **check their rules**, e.g. regarding the possibility of emergency communication, using certain websites, tracking your location by trusted people who stay in the country, etc.



15

Have a procedure.

In high-risk countries, always have a procedure in place in the event of theft of documents, equipment, or money. Do not wonder how likely such an event is, but how you will act when it does happen.

16

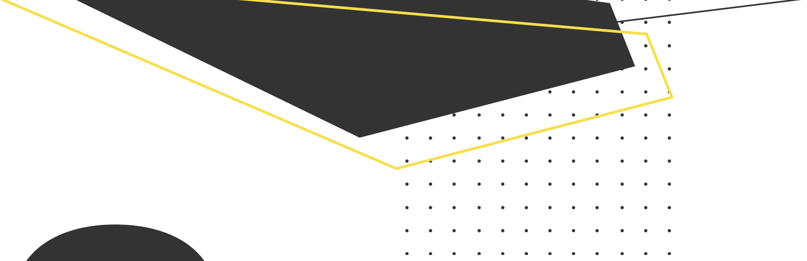
Make a scan of your documents.

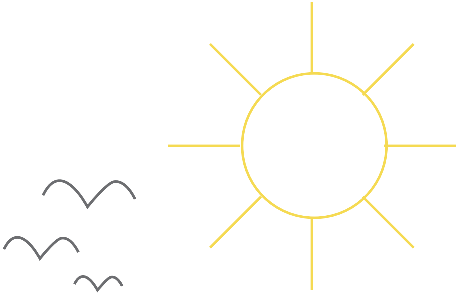
Make and keep a scan of your passport and/or other documents in a safe place, in case the original is stolen or lost. It will be easier for you to confirm your identity.

17

Use a separate bill and payment card than the main one.

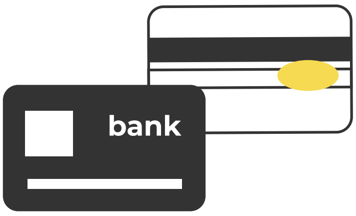
An account on which you will not have a large amount of money - in the event of theft or hacking of the bill, will protect you from losing all your savings.





18 Pay by card.

Where possible, pay by card. This will enable you to use the **chargeback procedure.** It consists in returning funds for a transaction made with a payment card carried out by the card issuer and initiated by the customer in a situation where he did not receive the products or services for which he paid (or, for example, turned out to be defective), there was a technical error in settlement of the transaction, or the transaction was fraudulent.



19 Cover the CVC2 code.

On your credit or payment card, cover the CVC2 code to prevent its reading when entering it in a store or during a contactless payment. There are known cases when cameras installed in shops read all data from both sides of payment cards.

20 Don't share your data.

Remember that you should never enter your payment or credit card details in an open analogue form, on an unsecured website, via e-mail, or during a phone call.

21 Check the room.

After checking into the hotel, check the room for the presence of hidden cameras.

22 Secure the room.

Remember that hotels have relatively easy-to-force doors and easy-to-open locks, so if you are concerned about unwanted visits, consider getting a portable door lock or a travel lock. Additionally, you can assume monitoring your hotel room while you are away.

23

Do not post.

Avoid posting reports from the trip on social media. The information you publish online can be used by criminals to rob your home, and it will facilitate the work of fraudsters who, taking advantage of your absence or unavailability, can obtain your data. It will be more difficult for you to notice and react.

24

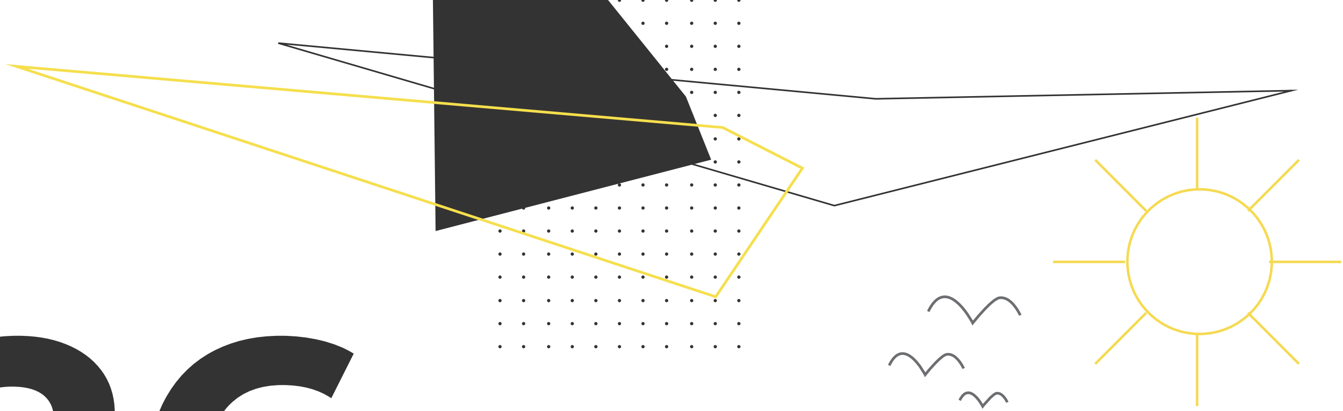
Do not take photos of your tickets public.

Do not take photos of electronic tickets in public. In some instances, you can make an unfavourable transaction for yourself based on the data contained in such a ticket.

25

Do not accept gifts or gratuities.

In particular, portable data carriers, USB cables, and chargers. They may be infected or contain surveillance elements (e.g. wiretaps), and by connecting them, we may be exposed to attacks by cybercriminals. Similarly, when it is not necessary, do not use publicly available charging stations. Instead, equip yourself with a portable power bank. Turn off the refreshing of unnecessary applications and currently unused communication interfaces (Bluetooth, Wi-Fi, GPS), thanks to which you will extend the working time of the device without having to charge it. When going abroad, check the standard of power sockets in a given place and equip yourself with the appropriate socket adapter.

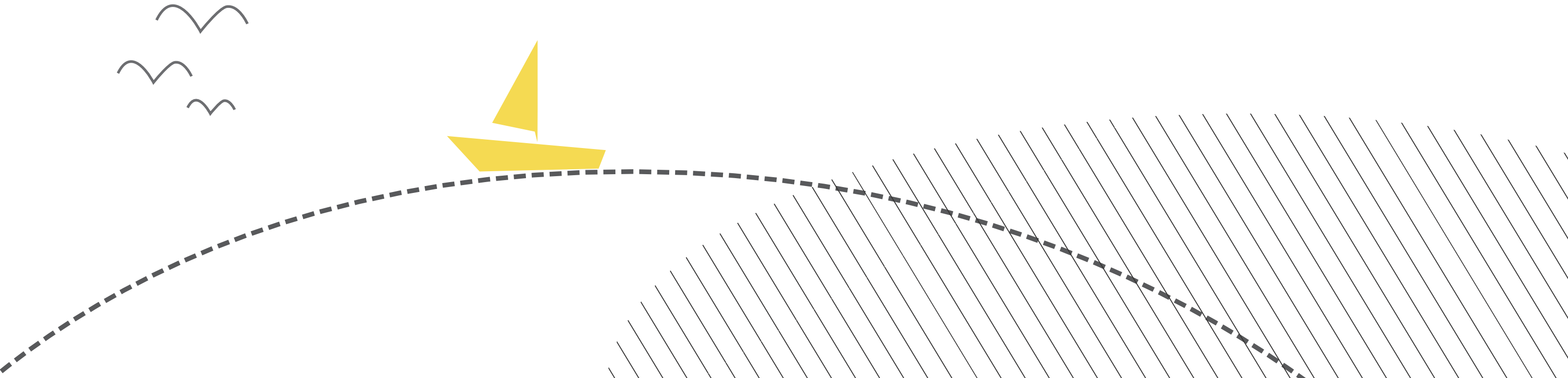


26 Be careful with online travel agencies.

And just as important - **be careful before going on vacation!** Especially when purchasing a trip or booking through online travel agencies. There are more and more cases of fraudsters impersonating the websites of travel agencies or booking portals and providing false bank account numbers or phishing data (e.g. cards or access to bank accounts). Don't fall for promotions or low prices. Be vigilant and always check the pages you are on.

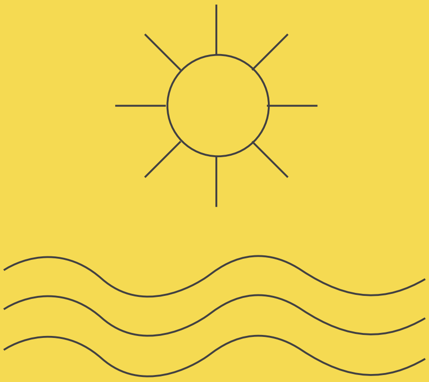
27 Take care of your connectivity.

Also, before leaving, before crossing the border, set up the **appropriate roaming tariff plans and limits for telephone calls**, text messages, and data transmission packages to make sure that in the country you are traveling to, you will have access to the services you need, but also not to expose yourself to large bills when you return home. Also, remember to turn off data roaming for applications you will not use abroad.



NaviRisk

Most of these tips apply during the holidays, business trips, and everyday life. Most importantly, many are pretty simple to use and require just a few steps. Remember, however, that the condition of reasonable security is always your vigilance and common sense.



CONTACT

Find us:
www.wearenavirisk.com
and find out more.

NaviRisk Sp. z o.o.
Huculska 5/6 Street
00-730 Warszawa

E-MAIL: **info@wearenavirisk.com**