

+ 5 tips

for

staying

safer

online



#toptip



BANCO DE PORTUGAL
EUROSYSTEM



Technological developments, ongoing financial innovation and the proliferation of digital financial services and products with easy and swift access make our relationship with the financial sector increasingly virtual, where digital channels are becoming the preferred means of accessing banking products. As this is a positive reality and close to the profile of the younger generations, it is not free from risks to which we must be increasingly attentive. It is very important to become familiar with the characteristics of new products, the risks of new access channels and the security procedures to be adopted. Information, knowledge and the informed use of digital tools allow us to enjoy the benefits and comfort of innovation, with the necessary safety and protection. For our part, we commit to promoting the provision of transparent and accessible information and fostering digital financial education. The tips we give here are a step in our commitment and clues to ensure the secure use of digital channels. **#TopTip**

Francisca Guedes de Oliveira

Member of the Board of Directors of the Banco de Portugal





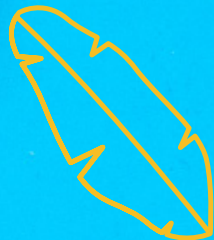
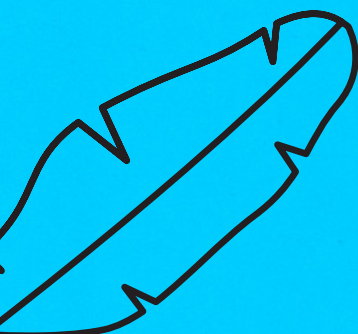
Digital

**financial
fraud**

**Would
you fall
for it too?**



#toptip





You receive an email or message from your bank, or other payment service provider or from an entity you have contracted a service with. They tell you that your account may be compromised or blocked and ask you to log in to regain access. Do you click on the link and enter your credentials or provide them over the phone without giving it a second thought?

This is likely to be a common form of phishing, i.e. an attack designed

to steal your personal details. And there are other fraudulent techniques, seemingly harmless but just as effective, that are used by people all over the world to get hold of your data. Hackers often use information they find on social media and use psychological manipulation to gain the trust of the victim and thus obtain confidential information.

Know the risks



A hacker contacts you by e-mail, by phone or by posting on social media, pretending to be, for example, a bank or other payment service provider, a public entity or a service provider. Sometimes, hackers use spoofing, by copying the phone numbers or emails and masquerading as an official entity to be more convincing. In these contacts, apparently for a legitimate reason, they try to convince you to provide your personal data (either directly or by providing you with a link to a fake page, even if seemingly legitimate). This type of attack is called **phishing** (also known as vishing or smishing, if the contact is made via a call or SMS respectively).



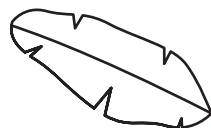
By downloading an apparently harmless file, you could be installing

a computer virus on your device. When you access a correct address, this virus redirects you to a false internet page, through which your personal data is wrongfully obtained. This type of attack is called **pharming**.



Other people can get hold of your data by installing malicious programs that collect your information. This type of attack is called **spyware**.

Another way third parties can get hold of your data is by directly observing information you are typing on your mobile phone, tablet or computer in crowded places, such as public transport or shopping centres. This type of attack is called **shoulder surfing**.



What can you do to protect your data

#1 Carefully assess the requests for information you receive.

- Never disclose personal information or access credentials to your digital channels or transaction authentication codes to third parties. A bank or other payment service provider would never ask you for this kind of information by email, SMS or phone.
- Don't disclose personal or confidential information via a phone call that you have not requested. Be suspicious of messages that indicate that a certain service has been blocked and needs to be activated or that request payment for an order you have not placed. Contacts with fraudulent intentions are usually made in an urgent tone, so that you quickly disclose personal data, without having time to think about the best way to act.
- If you receive a call, don't automatically assume that it is genuine just because the caller has your basic personal details. This information can be found online (for example, through social media).
- Don't open and immediately delete suspicious emails. Check the sender's address (not just the name), the language, the type and tone of the language used and the graphic presentation of the message received. Fraudulent messages often adopt less formal language, with spelling mistakes or semantic errors and are written to convey a sense of urgency to the reader.
- Don't click on links, don't perform the actions requested (don't run suggested programs) and don't open attachments from unknown sources.
- Don't enter confidential data and other personal information on sites whose authenticity is not guaranteed.

#2 Contact the entity concerned through the official contacts.

- Even if you think it is a legitimate contact, don't immediately disclose information and contact the entity concerned through the official

contacts (and never using the contact details provided in the emails, SMS or phone calls received).

- If you suspect fraud, report it immediately to your bank or other

payment service provider, through the usual channels, and to law enforcement agencies.

#3 Avoid sharing personal data when it is not essential to the service being provided.

- Many platforms and apps ask for access to personal information, such as your geographical location, contacts, microphone, camera and photo album, which is not relevant

for the provision of the services concerned. This information can then be shared with others without your knowledge.

#4 Check your privacy and security settings.

- Before you start using a new app or when you create a new internet user account, check your privacy and security settings and set them to a level of information sharing you are comfortable with.
- Every device, app or browser you use has different features to limit how and with whom you share information: explore the options and, if in doubt, find out more.

#5 Don't put off updates and always delete accounts and apps you no longer use.

- Updates to programs and apps allow you to correct security problems detected in the meantime. An app on your phone

that you don't use and don't update may be a "doorway" to possible cyber-attacks.

#6 Remain vigilant.

- Check your account movements regularly and contact your bank or other payment service

provider immediately if you notice movements that you have not authorised.



Digital

banking

Follow

these steps

to stay

safe



#toptip

When you access your account via the internet (home banking) or a mobile application (app), you should be aware of the associated risks.

Learn how you can protect yourself and pay attention to the security

procedures advised by your bank or other payment service provider.

If in doubt, don't proceed with the transaction without first clarifying the situation with your bank or other payment service provider.

When you use the internet



#1 Protect your computer, tablet or phone.

- Set passwords and create screen lock sequences so that your device cannot be used by third parties.
- Don't allow websites or applications with confidential information to launch automatically, without you needing to log in.
- Keep the operating system, antivirus and antispyware programs up to date on all your devices.
- Always keep your browser up to date.
- Don't click on links or download content from unknown sources.
- Don't use public or unknown wi-fi networks.
- Never leave your devices unattended.

#2 Protect your data.

- Don't share your passwords with third parties.
- Choose passwords that aren't too obvious (for example, never use 123456, ABCDEF, QWERTY) or that are not associated with easy-to-obtain personal information (such as birthdays, children's or spouse's names, mobile phone numbers).
- Don't use the same password to access the home banking service or apps of your bank or other payment service provider that you use to unlock your device or for social media connections, for example.
- Don't write passwords and other confidential information on paper, or send or save that information in email messages or on your phone.
- Use an offline password manager, such as Keepass.



When you access your home banking service or app

#3 Access your bank account securely via the internet (home banking).

- Always enter your home banking service's URL, rather than using a link, addresses saved in your "Favourites" or "History" or search results from search engines.
- Check that the address you've entered is the bank's official website address.
- Check that the website address begins with "https://" and that a padlock appears at the end of the address or in the bottom bar of the window. If this is not the case, the site is not secure.
- You can test whether the site is secure by using the "wrong password trick". On the first attempt to access the site, instead of your usual login, enter an incorrect password. If it's accepted, this means that the entity in question is not checking your login (i.e., it may just want to collect the password you type in order to misuse it).
- Ensure that you enter your home banking password and other authentication elements in a private place and that you're not being watched.
- After using your home banking service, log out and exit the internet page of your bank or other payment service provider by clicking on the icons provided for that purpose. Confirm that you need to log in again to access the page.

#4 Use your bank's app safely.

- Only install apps from official app stores. Not all apps are safe and may contain malicious software.
- Read the reviews of apps carefully before downloading them. Some apps have names and images that are very similar to the apps of banks or other payment service providers, purposely created to mislead users.
- Check the website of your bank or other payment service provider for information on the app you're



downloading and follow the configuration instructions.

- Confirm which authentication elements you are asked for each time you access the app of your bank or other payment service provider and be wary if you're asked for additional information.
- Ensure that you enter your password and other authentication elements to access the app of your bank or other payment service provider in a private place and that you're not being watched.

When possible on your device, use biometric authentication elements (e.g. fingerprint or facial recognition), which are elements that cannot be appropriated by third parties.

- After using the app of your bank or other payment service provider, make sure that you've logged out correctly and that you need to log in again.
- If in doubt, contact your bank or other payment service provider immediately via the usual channels; they will be able to help you.

#5 Use payment applications (payment apps) operated by third parties (for example, MB WAY, Apple Pay, Google Pay, Garmin Pay, Fitbit Pay, Swatch Pay) safely.

Find out which third-party payment apps your bank or other payment service provider offer. You can use these apps at the same time as the app of your bank or other payment service provider.

Read up on the features of the payment app you want to use, including the operations it allows and any fees you may be charged.

- Only install apps from official app stores.
- When signing up for the app, only add your phone number, if applicable. Never associate a

third-party phone number with your payment app, as doing so may allow an offender access to your information and/or funds.

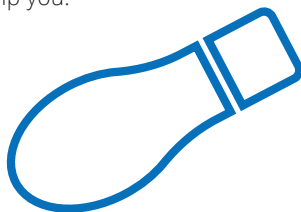
- Ensure that you enter your password to access the payment app in a private place and that you're not being watched.
- When carrying out transactions with the payment app, make sure you're using the correct feature and carefully read the notifications you receive on the app before accepting them. If your payment app allows transfers, be especially



careful if you receive a “money request” notification; by accepting, you are authorising a transfer of money from your account to someone else;

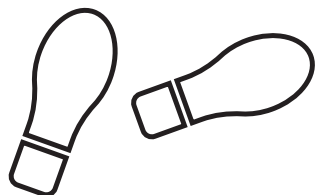
- Never share your payment app access information or transaction authentication codes with third parties.
- If you receive a notification for a transaction you haven't made, contact your bank or other payment service provider immediately via the usual channels; they will be able to help you.

After accessing your home banking service or app



#6 Remain vigilant.

- Check your account movements regularly.
- Check the date and time of your last access to the home banking service or app.
- Activate transfer and debit alerts or other security mechanisms provided by your bank or other payment service provider.
- If you receive a suspicious email or SMS supposedly from your bank, use the official contact details of the bank or other payment service provider to check its authenticity (and never the contact details provided in the suspicious email or SMS).
- Save the direct contact provided by your bank or other payment service provider to the contact list of your mobile phone. By doing so, if you detect any irregularities, you will be able to contact them more quickly.
- Remember that your bank or other payment service provider will never ask you for your access information to their home banking service or app by phone, email or SMS.



#7 If you suspect fraud, take appropriate action.

- Contact your bank or other payment service provider immediately if you notice movements you haven't authorised or don't recognise by using the contact details provided by your bank or other payment service provider, or the contact details on the [list of payment card issuers published on the Banco de Portugal's website](#).
- Request immediate cancellation of your access credentials to the home banking service or app of your bank or other payment service provider and, if applicable, of your payment card.
- Report the situation to the nearest police authority (PSP, GNR or PJ) or the Public Prosecutor's Office.

#8 If you lose your payment card or any security element, report it immediately to your bank.

- Immediately report the theft, robbery or misappropriation of your payment card, home banking or app access credentials or any security element used to carry out financial transactions through these channels to your bank or other payment service provider.
- If unauthorised payment transactions are carried out before you inform the bank or other payment service provider, you may have to pay up to €50 at most.
- In fraudulent or grossly negligent situations, you may have to pay an amount of more than €50.
- If your home banking service or app access credentials or those of your payment card are lost, stolen or misappropriated, and you have alerted your bank or other payment service provider to this, you are not obliged to pay any unauthorised amount removed after this alert.

**Opening
an account
remotely**

 **#toptip**

Did you know that you can now open a current account using remote communication?

Find out if the bank you want to open an account with allows you to do so remotely and what conditions are required.

Whatever channel you use to open an account, whether in person or remotely, the bank must provide you

with clear and complete information and answer all your questions.

A current account allows you to withdraw the funds deposited at any time. You can make deposits, payments and withdraw cash. It's usually possible to link a number of payment services, such as cards, transfers and direct debits to a current account.



Before opening an account

#1 Make sure that the bank you want to open an account with is registered with the Banco de Portugal.

- Make sure the bank is **registered with the Banco de Portugal** and that it is authorised to receive

deposits. Never make deposits with unauthorised entities.

#2 Find out from the bank you want to open an account with if it's possible to open an account through digital channels.

- Not all banks allow you to open an account through digital channels. In some cases, the process can be initiated via the bank's website or

app, by filling in personal data, but you may have to go in person to the institution to provide proof of some identification detail.

#3 Check the security of the bank's website or app.

- Check that the address you want to access begins with "https://" and that a padlock appears at the end of the

address or in the bottom bar of the window. If this is not the case, the page is not secure.

- Only install apps from official app stores.
- Adopt the usual security procedures to protect your computer, tablet or mobile phone:
 - Keep antivirus and anti-spyware programs up to date;
 - Don't click on links or download content from unknown sources;
 - Don't use public or unknown wi-fi networks;
 - Don't use public devices to make payments or other banking transactions.

Don't enter your data (name, mobile phone number, email, citizen card number, bank account numbers or credit card numbers) on sites that you're not familiar with or whose authenticity you don't trust.

#4 Analyse the information provided before opening the account.

After you have accessed the bank's website or app and filled in your details, the bank should provide you with detailed information on the account you want to open:

- Standardised information sheet — document with the characteristics of the account;
- Fee information document — document with information on the fees associated with the most representative payment services;
- Depositor information template — document with information on the deposit guarantee scheme;

- General terms and conditions of the account.

Carefully analyse all the information provided and compare it with alternatives, taking into account:

- Charges associated with the account, for example, maintenance fees;
- Charges associated with making payment transactions from that account, for example card or transfer fees.

When opening an account

#5 Check the procedures required to open the account through digital channels.

The steps to be followed to open an account remotely should be explained on

the platform used to open the account, namely the bank's website or app.

As a rule, you will have to:

- Read the documents with the characteristics of the account;
- Fill in your personal data;

- Provide proof of your identification details.



#6 Provide the bank with proof of your identification details.

To open an account, you will be asked to provide the following information:

- Full name, date of birth and type, number, expiry date and issuing entity of your identification document;
- Tax identification number;
- Profession and employer, if any;
- Full address of permanent residence.

Proof of the customer's identification details can be provided using the Mobile Digital Key, electronic use of the citizen card or via videoconference.

When using videoconferencing, please note that:

- The videoconference must be recorded by the bank and held in real time and without pauses, with

an indication of the date and time, and with sound and image quality;

- During the video conference, you will be asked to show the front and back of your identification document so that the bank can capture the image of the identification elements, including the photograph and signature;
- During the video conference, you will be asked to enter a "one-time password" (OTP) into the platform used to open the account. The code will be sent by your bank to the contact you indicated (mobile phone or email);
- You may also be asked for other supporting documents, such as proof of address (e.g. a water or electricity bill) and proof of your employment status (e.g. a pay slip).

#7 Keep a copy of the account opening agreement.

- Keep a copy of the account opening agreement. The bank is obliged

to provide you with this copy on a durable medium.

After opening the account

#8 Always keep your details with the bank up to date.

- You should inform the bank of any changes to the identification elements and contact details provided when opening the account, such as your address, telephone number or email address.

#9 Use your account responsibly.

- Keep sufficient funds in your account to cover your transactions. balance but be aware that this is a loan and you'll have to pay it back, plus charges.
- The bank may allow you to use funds beyond your account

#10 Know that you have the right to close the account free of charge.

- Closing your account is free of charge, but you may be required to give one month's notice. This means that once you notify the bank that you want to close the account, it has a maximum of one month to do so.
- You can confirm the closure of your account by consulting your Bank Account Database, available online through the Banco de Portugal's website, the Bank Customer Website or in person at the respective branches.



**Shop
safely
online**



#toptip

Online shopping is a convenient and sometimes cheaper way to purchase goods and services. But some care should be taken.

Look for information about the seller and, if you go ahead with the purchase, always use a payment method with added security.

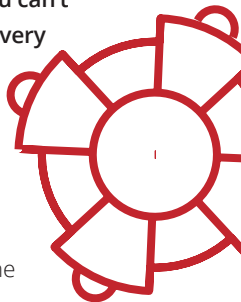
Before making a purchase online or via apps



#1 Look for information about the seller.

- Make sure the seller is credible: search the internet for the company name or ask friends or acquaintances for references.
- Be suspicious if you don't find an address or telephone contact details or the terms and conditions of the sale.
- Research and read about what other customers have experienced in relation to a particular product or online store, for example in discussion forums.

Be cautious about offers you can't refuse or bargains because very often they are fraudulent.



#2 Check the security of the website or app.

- Check that the address you want to access begins with "https://" and that a padlock appears at the end of the address or in the bottom bar of the window. If this is not the case, the page is not secure.
- Only install apps from official app stores.
- Follow the usual security procedures to protect your computer, tablet or mobile phone:
 - Keep antivirus and anti-spyware programs up to date and ensure the firewall is active;
 - Don't click on links or download content from unknown sources;
 - Don't use public or unknown wi-fi networks;
 - Don't use public devices to make online payments.



Don't enter your data (name, mobile phone number, email, citizen card, bank account numbers or credit

card numbers) on sites that you don't know or whose authenticity you don't trust.

#3 Read the terms and conditions.

- Check the available payment methods.
- Find out about any additional costs – for example, shipping costs or customs duties if the shop is based outside the European Union.
- Check the conditions and costs for returns and exchanges. Within the EU, you have 14 days to return any item bought over the internet.

When you make the purchase

#4 Make sure that you only provide the data required to complete the purchase.

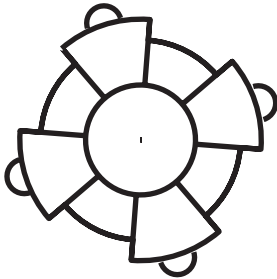
- Be suspicious of requests for data (e.g. passwords, personal identification document data or payment card details) that seem excessive or strange to you, even if they come from an apparently reliable entity. If in doubt, ask your bank or other payment service provider for clarification via the official channels.

#5 Opt for a payment method with added security.

- **Cards with limited credit and a short validity period**, such as prepaid cards. These cards limit the possibility of misusing the card and the sum of possible losses.
- **Single-use virtual cards or with a limited amount and validity period**. A virtual card is a card that is generated and used in an electronic context. At the time

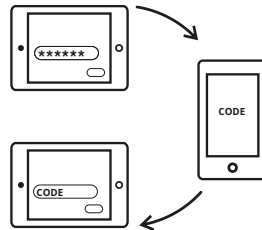
of the purchase, the real card data is not disclosed, making the transaction more secure. This feature may be offered by your bank or other payment service provider and by certain payment apps.

- **Payment instruments with added security.** Choose cards with added security procedures such as the latest version of the 3D Secure service. As a rule, this service will already be active on credit or debit cards that allow you to make online purchases. If not, ask your bank or other payment service provider to subscribe/activate it. In this case, when making



a purchase, you will usually be asked to perform strong customer authentication, that is, to enter two valid authentication elements, in addition to the card data. The most common solution for strong authentication of online card transactions is to validate the transaction in the app of your bank or other payment service provider.

Strong customer authentication



Strong customer authentication requires at least two different authentication elements (e.g. password plus code sent to the phone)

After making the purchase

#6 Keep records.

- Keep records of your purchase, including information about the seller and its email address.

Whenever possible, print screenshots of the transaction data.

#7 Check your account regularly.

- Check your account on a regular basis and make sure that the movements correspond to the

purchases you have made.

#8 Report suspected fraud.

- If you suspect misuse or unauthorised use of your payment card, or if you suspect that your identification or validation details (such as access credentials to the home banking service) have been wrongfully used, report the situation immediately to your bank or other payment service provider, through the contacts provided or through the contacts disclosed

on the **Banco de Portugal's website and on the Bank Customer Website.**

- Report the situation to the nearest police authority (PSP, GNR or PJ) or the Public Prosecutor's Office.
- If necessary, ask your bank or other payment service provider to cancel the card or the home banking service access credentials.

A yellow ukulele is positioned diagonally across the frame, pointing towards the top right. The background is a solid bright blue. Scattered around the ukulele are several musical notes: a single eighth note at the top, a pair of beamed eighth notes to the left, a single eighth note to the right, a pair of beamed eighth notes at the bottom left, and a single eighth note at the very bottom. The text 'Online consumer credit' is overlaid on the image in three stacked rectangular boxes.

Online

consumer

credit



#toptip

Did you know that it's now possible to take out consumer credit products through digital channels, online or via your mobile phone?

Check with your bank if the credit product you want to take out is available through digital channels and find out the conditions required for this.

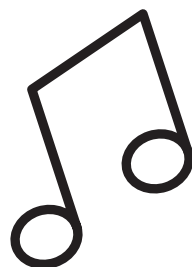
Regardless of the channel used, institutions must provide you with clear and complete information at the various stages of the application as

well as the means for you to clear up any questions you may have.

Check if your income is sufficient to pay off the debt you want to take on and any other you already have. Bear in mind that credit instalments are a fixed monthly expense in the household budget, with an impact until the loan is fully repaid, so you should take into account your income and the expenses you anticipate having in the future.



Before taking out consumer credit through digital channels



#1 Make sure that the institution is authorised to grant credit.

- Confirm that the institution is **registered with the Banco de Portugal** and that it is authorised to grant credit. Never take out a loan with an entity that is not authorised to do so.

#2 Check the security of the credit institution's website or app.

- Check that the address you want to access begins with "https:///" and that a miniature padlock appears at the end of the address or in the bottom bar of the window. If this is not the case, the page is not secure.
- Only install apps from official app stores.
- Follow the usual security procedures to protect your computer, tablet or mobile phone:



- Keep antivirus and anti-spyware programs up to date;
- Don't click on links or download content from unknown sources;
- Don't use public or unknown wi-fi networks;
- Don't use public devices to make payments or other banking transactions.

Don't enter your data (name, mobile phone number, email, citizen card number, bank account numbers or credit card numbers) on sites that you're not familiar with or whose authenticity you don't trust.

#3 Compare different options before taking out a loan.

- Provide the credit institution with truthful and complete information and clearly state the purpose of the loan you want to take out. Different **types of consumer credit** have different purposes, terms and associated costs.
- Before you decide on a loan, compare different options.
- Institutions should prominently display information on the key characteristics of the loan, fees and any charges on the screen or homepage of the marketing platform. This information should be presented in larger characters, information boxes, simulations, summaries or other similar means.
- Download and carefully read the **standardised information sheet**, which describes the loan's main characteristics.
- Carefully analyse all the information provided and:
 - Consider all the costs of the loan, checking the APR — the annual percentage rate of charge — and the total amount to be reimbursed of the credit options;
 - Check whether the credit options include the purchase of other products. The interest rate may be lower if you agree to buy certain proposed products; however, these products usually have costs;
 - Pay attention to the loan term. Loans with longer terms generally have lower instalments, but you will have to pay interest for longer.



#4 Answer all your questions before taking out the loan.

- Find out about the applicable procedures. Institutions are obliged to present the stages of the process and the elements required to take out the loan on the screen or on the homepage of the marketing platform so that the following are clearly obvious at the outset:
 - The various stages of the loan process;
 - Whether it's necessary to use other channels, devices or means of communication during the loan process;
- The documents that are necessary to take out the loan.
- Institutions should provide you with assistance regarding the loan, the stages of the process and the documentation required, for example by providing a support line or live chat, a chatbot, answers to frequently asked questions, an infographic or an explanatory video.

When concluding a consumer credit agreement through digital channels

#5 Read all documents carefully.

- Check the options associated with the loan, such as optional cross-selling of other products (e.g. insurance or credit cards) or the financing of charges, and select them only if they are beneficial to you. Please note that these other products should not be pre-selected and are always optional, i.e. you are not obliged to choose any of them to have access to the loan. Be aware of the possible impact on the total cost of the financial product by checking the effect on the APR and the total amount to be reimbursed.
- In order to proceed with the contracting process, you will have

to consult all the pages of the mandatory information documents, such as the standardised information sheet and the draft

agreement, and confirm they have been duly read at the end of the documents.

#6 Confirm your wish to take out the loan.

- The institution should inform you in advance of the methods available to confirm your wish to take out the loan, which may include a

qualified electronic signature, Digital Mobile Key or strong customer authentication.



During the term of the agreement

#7 You can exercise your right of free revocation and early repayment.

- On the marketing platform, on the website or the app, the credit institution provides you with a dedicated space to communicate your interest in exercising the right of free revocation. This means that you have 14 calendar days from the date of signing the agreement to withdraw from the agreement without having to justify the decision to the institution. Once the right of revocation has been exercised, you

have a period of 30 days to pay the institution the capital and interest accrued from the date the credit was used until the date the capital is repaid.

- To repay all or part of the credit before the term laid down in the agreement, you must notify the institution by the means indicated to this effect. To exercise this right of early repayment, you may have to pay a fee.





#8 Analyse the information sent to you by the institution during the term of the agreement.

- 
- Pay attention to the notifications the institution sends you by email, SMS or push notifications, informing you that relevant information is available in the private area of the institution's marketing platform, website or app (namely, changes in contractual conditions regarding fees and expenses that may be applicable).
 - Check the detailed statement that the institution should provide on a regular basis with information on the evolution of the loan.
 - Find out what means are available to you to file a complaint or resort to alternative dispute resolution.

#9 Pay the agreed instalments on time and keep your data updated with the institution.

- Pay your loan instalments on time.
- If you have or anticipate having difficulties in paying your instalments, notify the institution so that it can promote measures to avoid default (**Pre-arrears action plan**).
- Always inform the institution of changes to your address, contact details or other relevant data.

The #TopTip campaign is a digital financial education campaign launched by the Banco de Portugal to promote the safe use of banking products and services on digital channels.

This publication compiles the tips aimed at the general population, which are also available on the **Bank Customer Website** — <https://cliente bancario.bportugal.pt/en> —, in the “Financial education” area, along with other support materials, on **Instagram** — [@bancodeportugaloficial](https://www.instagram.com/bancodeportugaloficial) — and on **YouTube** — <https://www.youtube.com/@BancodePortugalOficial>.