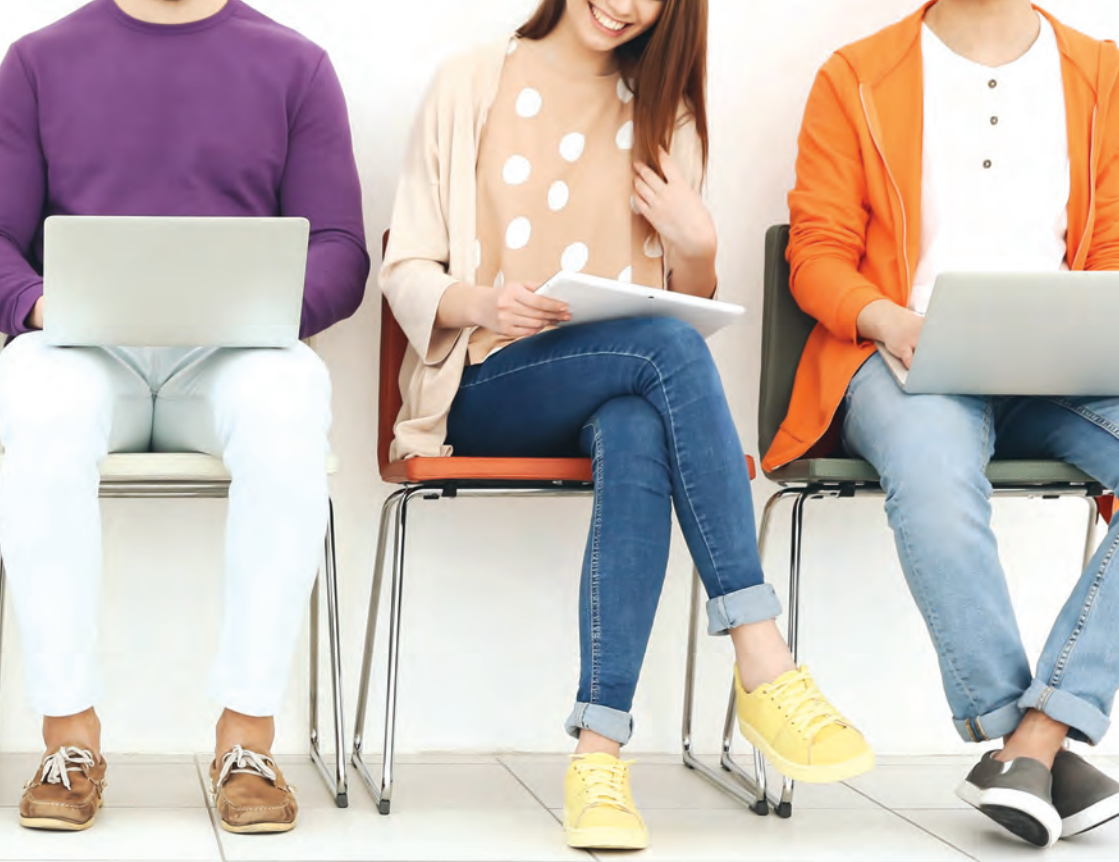
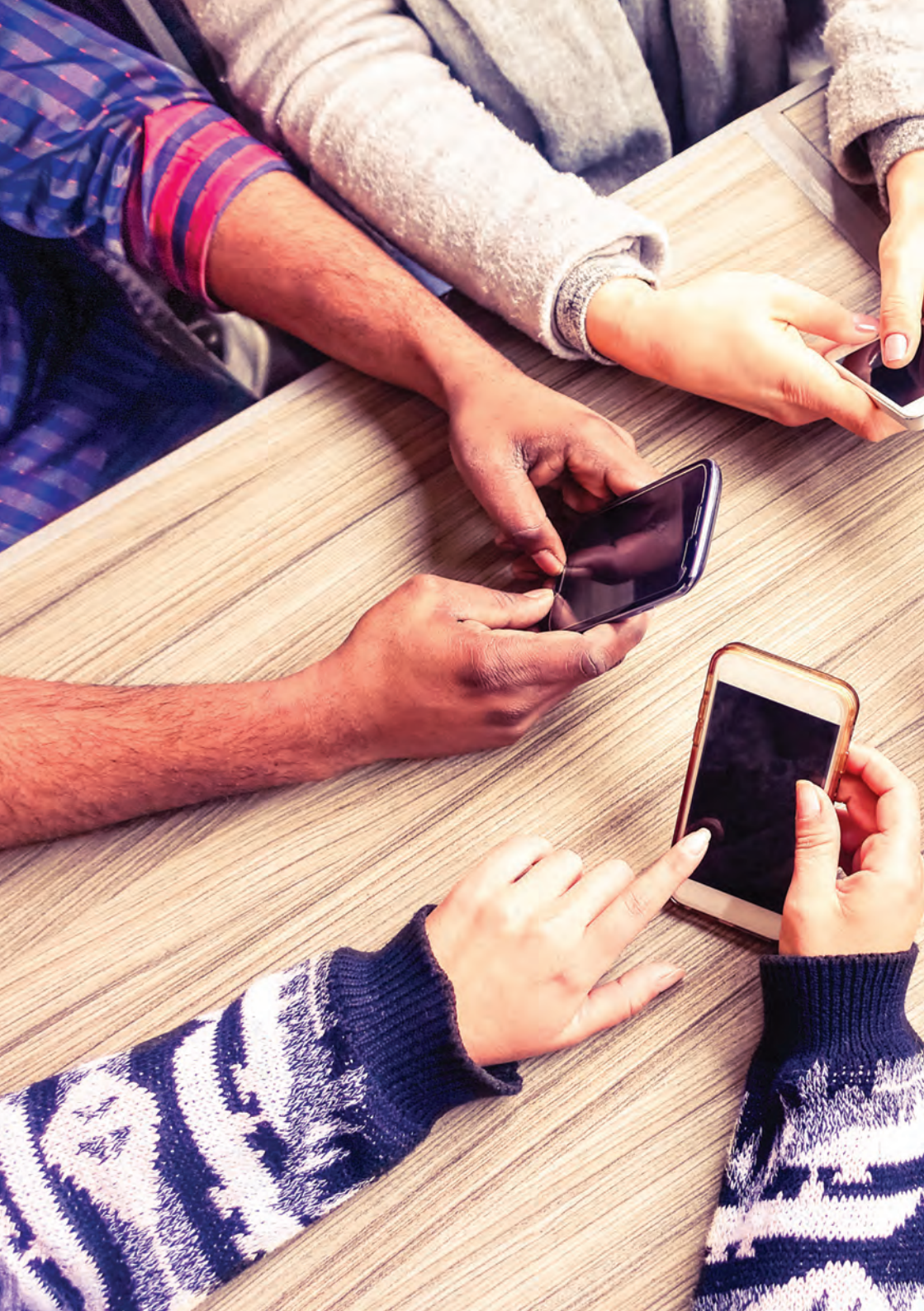


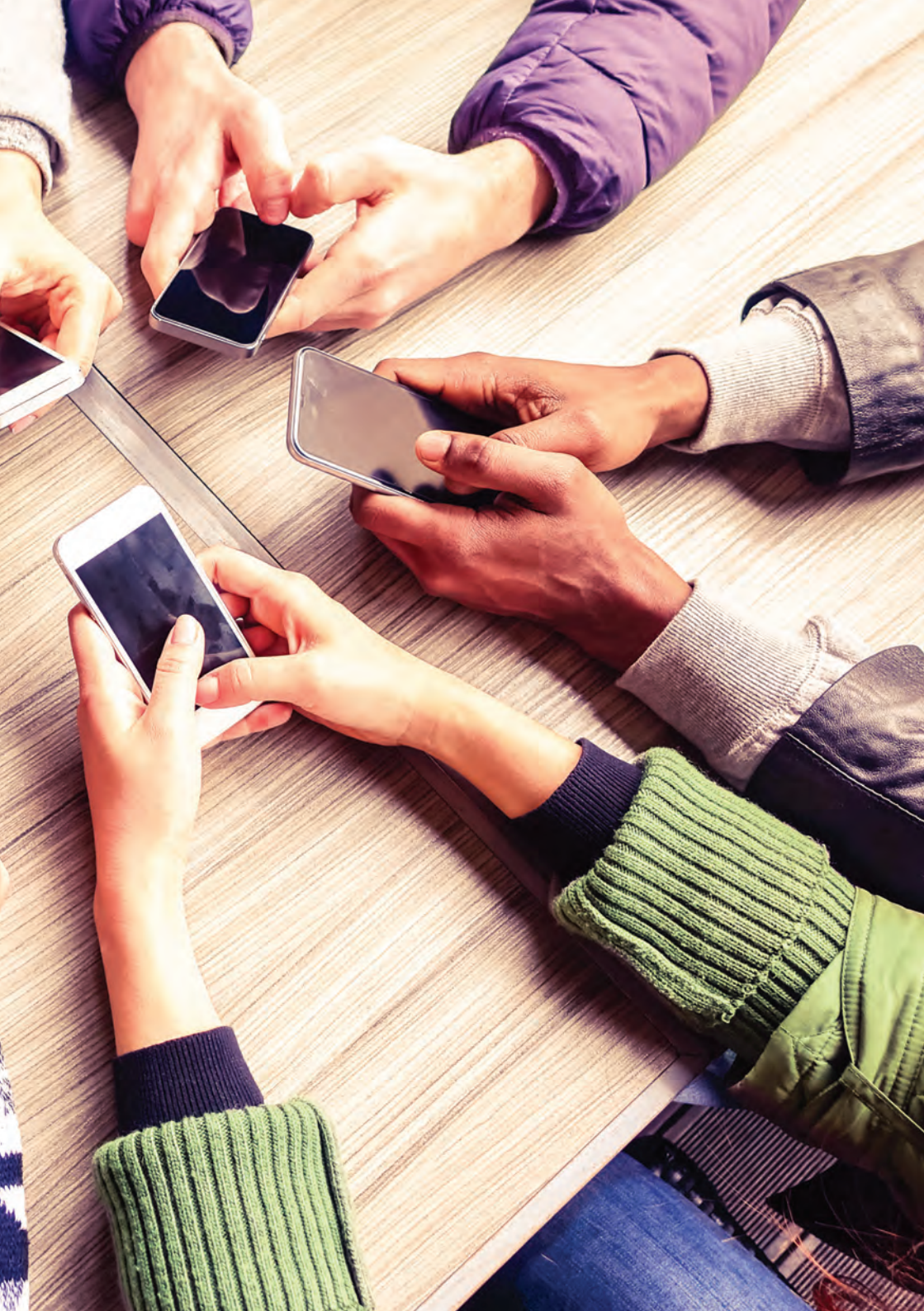
5 TIPS
FOR STAYING SAFER ONLINE
#toptip

BANCO DE PORTUGAL
EUROSYSTEM

The way in which we consume financial products and services has changed considerably over the last few years. Today we use these products and services, at any time and anywhere, via computer, smartphone or tablet, quickly and easily. But there are inherent risks and we have to bear these in mind, not only when we make payments or use homebanking, but also when we share personal information on social networks, by email or telephone, when we click on an apparently inoffensive link, or when we download an app or a file. I invite students and teachers to get to know certain rules for the safe use of financial products and services. Digital financial literacy is key to creating a generation of informed consumers, capable of benefiting from the best that innovation has to offer. **Check out our top tips!**

Carlos da Silva Costa
Governor of Banco de Portugal





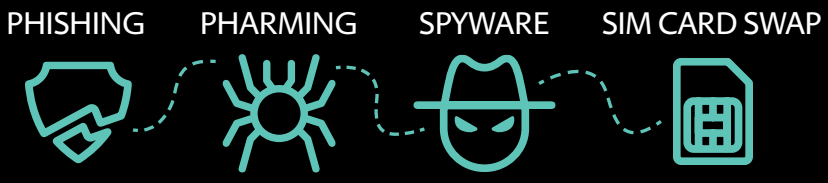
DON’T MAKE THE INTERNET A HIGH-RISK GAMBLE

#toptip

When you use the internet do you have any idea of the risks?

We hear more and more about hackers and cyber attackers accessing other people's personal data through security flaws in computers, phones, tablets and internet accounts.

Phishing? Spyware? What is this?



This is when people pretend to be other people in order to obtain your data.

A simple download installs a virus that opens pages asking you for personal data.

This is when apparently inoffensive apps and software spy on what you do.

In these attacks, all calls and SMSs you receive are directed to another phone.

Phishing

This is when a hacker pretends to be an institution or company and, through emails, social networks, calls or SMSs, tries to get you to divulge personal information.

It happens when you receive dubious emails with links that send you to false pages, for example, pages resembling the bank's website, and asking you to fill out a set of data.

Pharming

This is when a virus on your computer, tablet or phone (smartphone) redirects a link input by you to a false internet page (called a 'mirror website'). Sometimes this page looks like the bank's website, allowing third parties to obtain all the personal information that you type in.

This virus can be installed when you download an apparently inoffensive file.

Spyware

This is when malicious software installs itself on your computer, tablet or phone (smartphone), without you noticing, and spies on your equipment and on your data.

This software can be installed when you download an apparently inoffensive file.

Once installed, it detects whether you are accessing protected sites, like homebanking pages, and records the data inserted, which then may be used unduly by other people.

SIM Card Swap

This is when, for example, someone collects information about you, directly or through social media, and manages to pose as you in a phone store, to request the reissue of a SIM card.

This allows all calls and SMSs received, including one-time passwords ('disposable' passwords, valid only for one homebanking access or transaction, which are sent by SMS), to be directed to the SIM in the possession of that other person.

What can you do to protect yourself?

Protect your computer, tablet or phone

- Set passwords and create lock screen sequences so that your equipment can't be used by third parties;
- Do not give permission for sites or apps with confidential information to start sessions automatically, without requiring a log-in;
- Keep your operating system and anti-virus and anti-spyware software updated on all your equipment. Keep the firewall active;
- Avoid public equipment (shared computers for example), mainly when you want to conduct bank transactions or payments.

Protect your internet connections

- Don't connect to public or unknown wi-fi networks;
- Don't open suspect emails. Does the email have mistakes? Is it in another language? Is it abnormal that they contact you with that kind of email? Don't

trust it and report it directly to the person or through the official channels of any entity allegedly trying to contact you (for example the bank, the online store, the delivery services company...);

- Don't click on unknown links or download from unknown sources;
- Don't open email attachments from senders you do not recognise;
- Always type the URL you want instead of using a link or accessing the web history;
- Check that the address you wish to access starts with https:// and that there is a padlock in the navigation bar or at the bottom of the window. This means that the link is secure;
- You can test if the site is safe by using the 'wrong password trick'. Instead of your usual login, put the wrong password in. If it is accepted, this means that the entity in question is not checking your login (in other words, it may simply be collecting the password you put in for illicit use);
- Only install trustworthy apps from official app stores. Not all apps are secure and may contain malicious software.

Protect your data

- Do not give out your passwords to third parties;
- Don't write passwords or other confidential information on paper, or keep it in emails or on your phone;
- Choose passwords that are hard to guess and use different passwords for different accounts;
- Do not put your data (name, phone number, email address, ID card no., bank account numbers) into sites that you do not know or whose authenticity you cannot trust. In case of doubt, close the window and talk to your parents and the entities you usually contact (for example the bank or online store).

YOUR PHONE SAYS A LOT ABOUT YOU

#toptip

Do you use your phone (smartphone) to access social networks or email? And homebanking? Do you also make payments with your phone?

Your phone can store a large amount of confidential information about you and the transactions you make.

Do you use your phone for everything?

Do you use wi-fi everywhere you go?

Are you a sucker for a good app?

What can you do to protect yourself?

Make accessing your phone difficult

- Use safe passwords, which are not too obvious (for example never use passwords like 123456 or your date of birth);
- Use a lock screen sequence for your phone and change it regularly.

Protect your internet connections

- Do not give permission for sites or apps to start automatically, without requiring a log-in;
- Regularly update the software that protects your phone, like anti-virus software;
- Don't connect your phone to public or unknown wi-fi networks;
- Don't click on links or download stuff from unknown sources.

Use safe apps securely

- Only install trustworthy apps, through official app stores;
- If a deal seems too good to be true, do not trust it. If you know that an app or service normally costs something and you find a free version, remember that that version may contain a virus;
- Check the data access permissions required by the apps. Does it ask for access to your phone's camera at any time? And the microphone? Do not download apps that require apparently excessive permissions.

THINK BEFORE
YOU POST
#toptip

Is social media your second home?

Social media lets you talk to friends around the world and share stuff with them, and keeps you up-to-date on initiatives that might interest you, videos you might like, and charitable projects you might want to contribute to.

But, like everything, it comes with risks.

Do you post all the time?

Do you tell everyone everything about yourself?

What can you do to protect yourself?

Manage your privacy settings

- You must change your profile's privacy settings on social networks so that only 'Friends' or 'Followers' can see what you share;
- You can block specific people or groups of people, preventing them from seeing your profile.

Think before you share

- Don't disclose personal or confidential information. For instance, don't disclose your passwords or photos of your bank cards;
- Think if you need to share information like your date of birth, your phone number, the name of your school. If it is not necessary, don't do it;
- What you share on social networks may be seen and shared by others and may be misinterpreted or used fraudulently;
- Even if you delete information, it may be seen, recorded or shared before being deleted;
- Don't share images or videos without the authorisation of the people involved.

Read the data management policies

- Creating a profile on a social network is generally free. However, often companies that manage the social platforms collect your data and store everything you like, comment on or share, so that they can target you for specific advertising;
- Find out how your data are used in the social network's data policy.

DON'T
BE TRICKED
#toptip

Do you buy online safely?

Online purchases are a useful and often cheaper way to acquire goods and services. But you have to take care...

Do you buy online blindly?

Do you buy safely?

Do you go straight to what you want?

Do you give all the information they ask?

Do you buy and that's it?

What can you do to protect yourself?

Before making a purchase online or through apps, get informed

Find out about the seller

- Search the internet for the company name;
- Be suspicious if you do not find an address or phone number you can ring and the terms and conditions of the sale;
- Read about the experiences of other customers for a given product or online store, for example in discussion forums.

Check the site or app's security

- Check whether the address you wish to access starts with https:// and whether there is a padlock in the navigation bar or at the bottom of the window. This means that the link is secure;
- Only install trustworthy apps from official app stores.

Adopt habitual security procedures to protect your computer, tablet or phone

- Keep your anti-virus and anti-spyware software up-to-date and the firewall active;
- Don't connect to public or unknown wi-fi networks;
- Don't use public equipment to make payments.

Read the terms and conditions

- Check the payment methods;
- Learn about any added costs, such as postage or customs costs, if the store is based outside the EU;
- Check the conditions and costs applying to returns or exchanges. Normally in the EU you have 14 days to return any product bought over the internet.

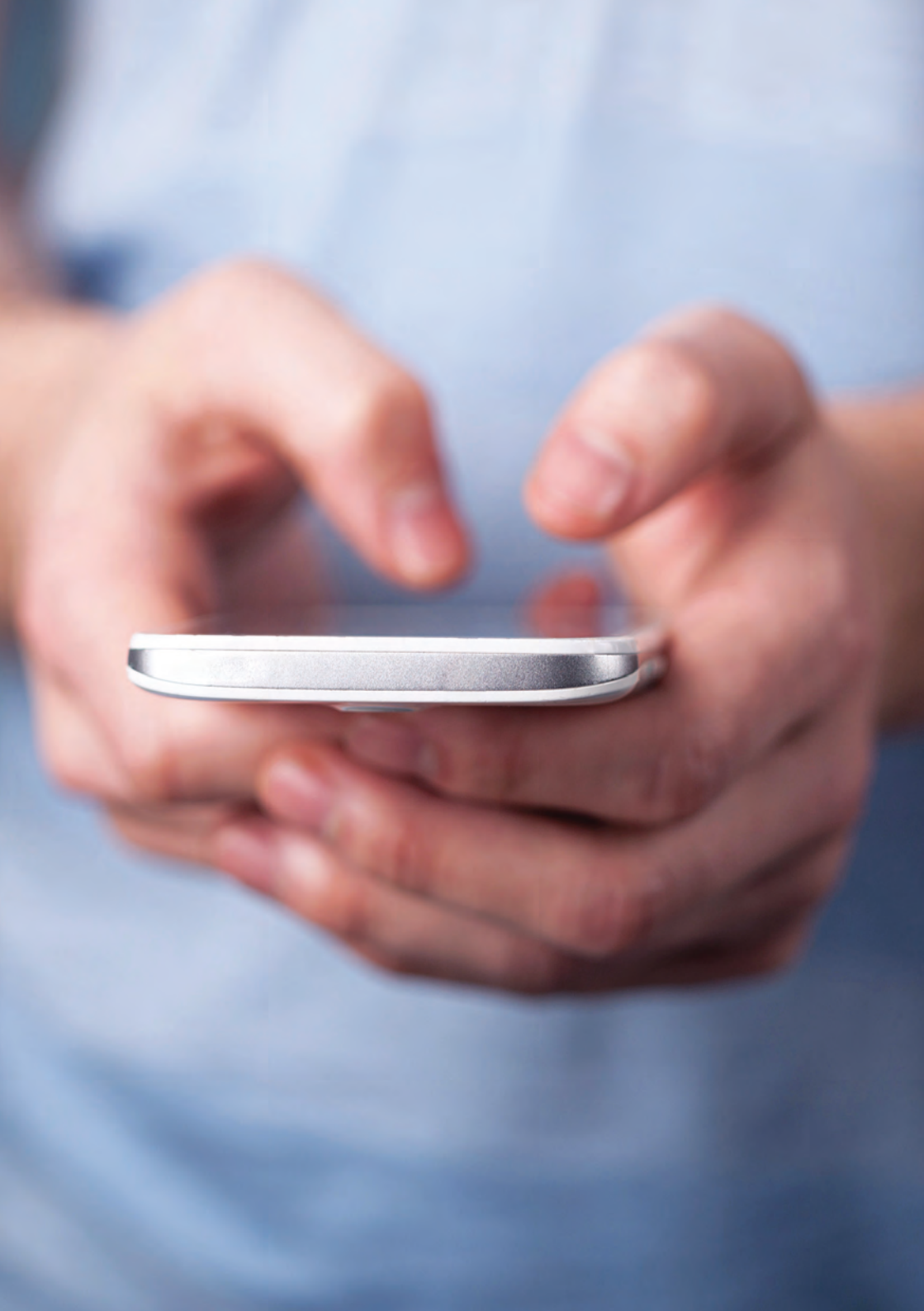
When you buy something

Make sure you only provide the information needed to complete the purchase and preferably opt for one of the following payment methods:

- Multibanco reference. In this case, the store sends you a message or email with the data you need to make your payment, within a given time period, at an ATM or through homebanking;
- Virtual cards. The MB WAY app, for example, allows you to create virtual MB NET cards. So when you pay, you put in the data for the virtual card and not the real card;
- Payment instruments with added security, like cards with a low credit limit, a short validity period or additional authentication procedures. Using the "strong customer authentication" method, you can shop online with your card's real data because during the act of payment, additional security procedures are used. In a payment using strong customer authentication, and as well as the card details, you will be asked, for example, to type in a unique code sent by text message to your mobile and then validate the purchase on the app, via a password or fingerprint.

After making your purchase

- Keep the records of the purchase made, including the information on the seller;
- Regularly check your bank account to see if the debits correspond to the purchases you made.



DON’T GIVE
IN TO FRAUD
#toptip

What if you are a victim of online fraud?

When you make bank transactions and payments over the internet or by phone (smartphone), beware of possible fraud situations.

In case of doubt, close the window and share your doubts with your parents and your bank.

Do you suspect a fraudulent situation?

Lost track of your bank card?

Have people taken money from your account without authorisation?

What can you do to protect yourself?

If you suspect fraud, move fast

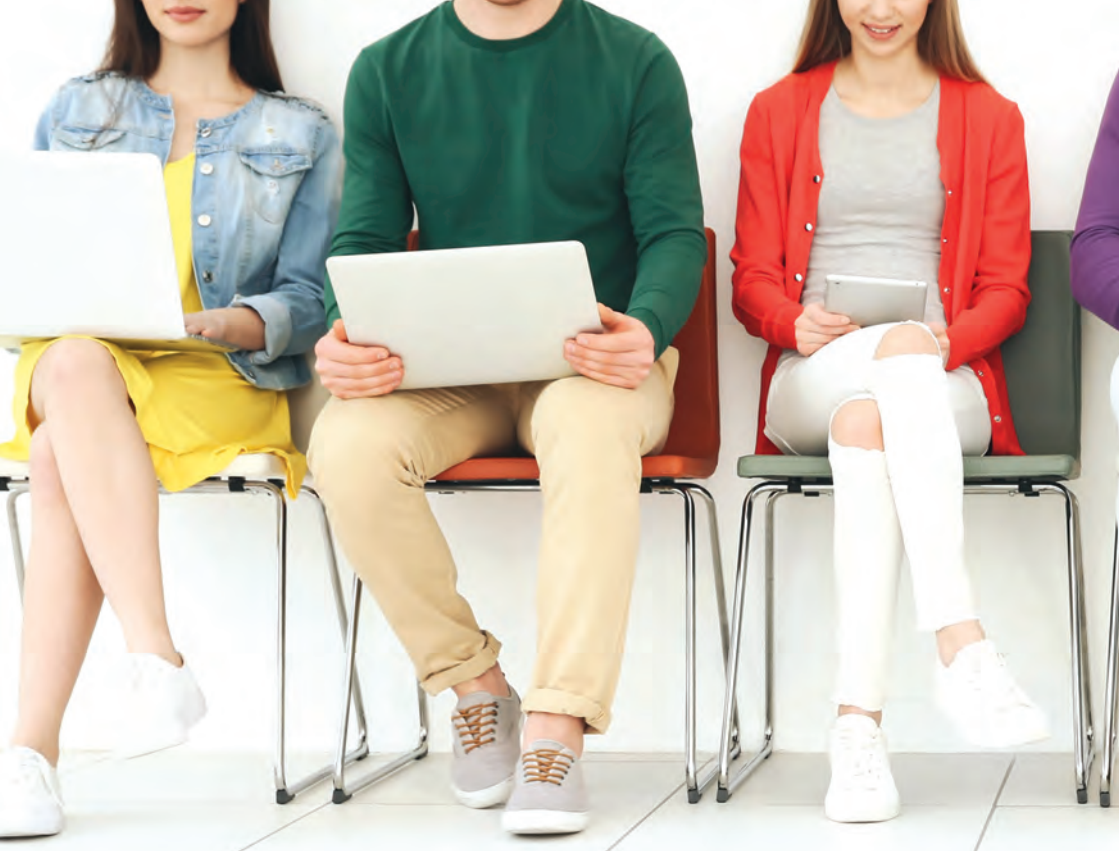
- Contact your bank immediately through the contact details it supplied you or through the contact information on the list of payment card issuers, available on the Banco de Portugal website and the Bank Customer Website;
- Ask for cancellation of the homebanking access credentials immediately or, where relevant, cancellation of the card;
- Inform the nearest police entity (PSP, GNR or PJ) or the Public Prosecutor's Office of the fraudulent situation.

If you lose your bank card, report the disappearance

- Immediately contact the entity that issued the card if you have lost it, if it was stolen or misappropriated, or if you believe that the card was cloned or counterfeited;
- You can check the contact details for card-issuing entities on the Banco de Portugal website and the Bank Customer Website.

Understand your rights and obligations

- If payments were made that you did not authorise, you may have to pay up to €50 at most;
- If you lie or if you have not complied with the security rules, you may have to pay an amount higher than €50;
- If you suffered loss, theft or misappropriation of access credentials for homebanking or for your card and if you alerted your bank to this, you cannot be asked to pay the sums that were moved without authorisation after this alert.



This brochure sets out Banco de Portugal's materials for the digital financial education campaign **#toptip**, which raises awareness among school-age children of precautions to take when using digital channels to access banking products and services.

This brochure is designed for secondary schools across the country and is also available on the **Bank Customer Website**, **https://clientebancario.bportugal.pt**, in the "Financial education" area, along with other support materials, and on **Instagram** at **@bancodeportugaloficial**.