febelfin

Phishing and other lurking dangers

Online fraud is everywhere. In 2023, cybercriminals continued to send phishing messages en masse, posing as a close relative or a trusted organisation, such as a bank or government agency. The banking sector blocked or recovered 75% of all fraudulent transfers as a result of phishing in 2023. Despite these efforts, criminals still managed to net €40 million[1] through phishing.

We also see that other forms of online fraud in which the customer is manipulated into making a fraudulent payment continue to rise sharply. Examples include investment fraud and bank help desk fraud[2]. Alarmingly, the general public is still not aware enough of these new forms of fraud.

Fortunately, there is also good news. Despite the many attempted and successful cases of online fraud, we see a positive trend in the actions people take when they suspect it is happening. In 2023, 91% of potential victims acted when they had such a suspicion. A decrease can also be observed in the number of people sharing PIN codes and sending their bank card to a specific address. The general public is also more aware of the phenomenon known as money mules.

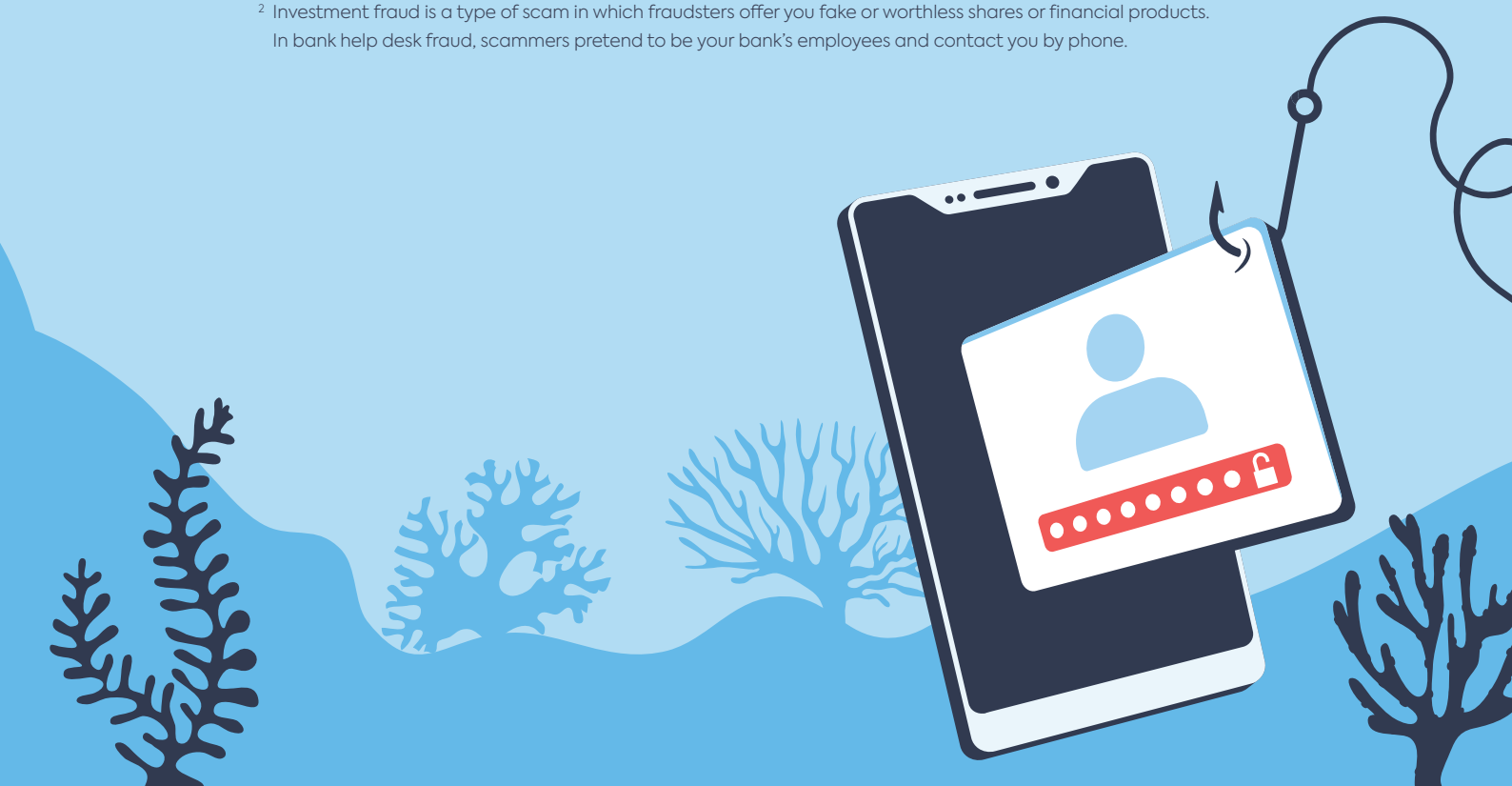
All these findings demonstrate that we must remain committed to raising awareness on a permanent basis. Anyone can become a target of online fraud. We see fraudsters targeting young people, in particular, as they tend to be more laid back about online safety.

As a sector, we therefore remain committed to new initiatives and partnerships to fight online fraud together.

What is the general public's awareness of online fraud? What forms of fraud are on the rise, how 'safely' do we behave when shopping online, and do we still share our codes as easily? What efforts has the sector made? And what are our priorities for the future? Read all about these questions and more in this storytelling brochure with the latest figures.

[1] Source: Febelfin figures based on a survey of Fraudsys committee members

[2] Investment fraud is a type of scam in which fraudsters offer you fake or worthless shares or financial products. In bank help desk fraud, scammers pretend to be your bank's employees and contact you by phone.



THE ‘PHISHING NET’ IS STILL LARGE

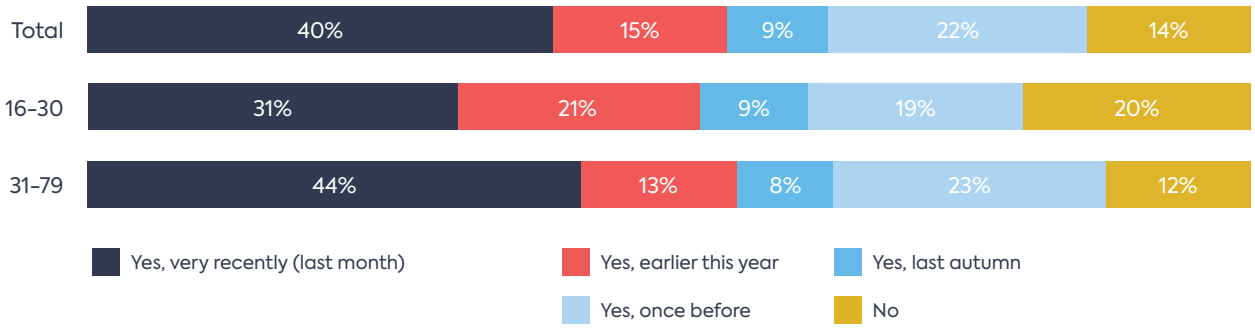
Stolen amount of **€40 million** in 2023

Despite all the initiatives to raise awareness, phishing continues to be a popular fraud technique for cybercriminals.

Although banks blocked or recovered 75% of fraudulent transfers as a result of phishing in 2023 (as in the previous year), cybercriminals were able to net around €40 million[3] through phishing.

A recent survey carried out by Febelfin in collaboration with the research agency Indiville[4] confirms just how widespread phishing attempts continue to be. In fact, 55% of the population have already received at least one phishing message this year, and in 40% of cases very recently. This is in line with last year’s figures.

Have you received a phishing message before? When was the last time this happened?



Source: Indiville

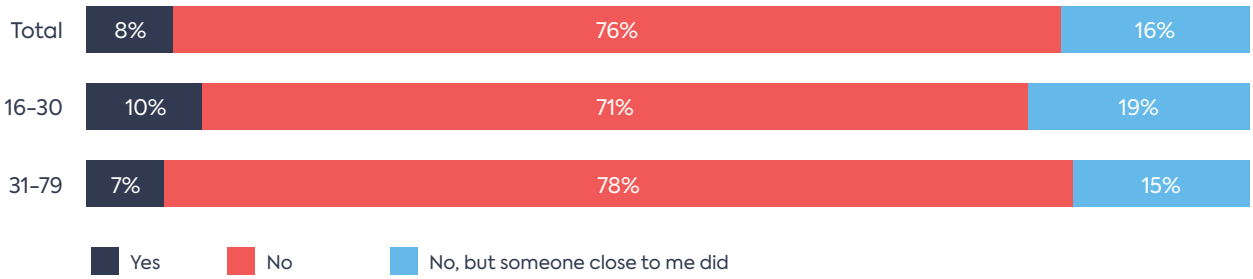
Cybercriminals thus continue to send phishing messages en masse. In 2023, private individuals forwarded nearly 10 million messages to the reporting centre verdacht@safeonweb.be. In 2022, that figure was 6 million. An average of 27,000 messages are forwarded each day.

The survey shows that 8% of people have been victims of phishing. Young people are more vulnerable (10%). They are also more likely to know someone who has already been a victim (19%, 2022: 15%).

[3] Source: Febelfin figures based on a survey of Fraudsys committee members

[4] Indiville survey, 1–18 March 2024, on a representative sample of the Belgian population n: 2109 NL/FR surveys, age 16–79. Maximum margin of error: 2.1%

Have you fallen victim to phishing before?

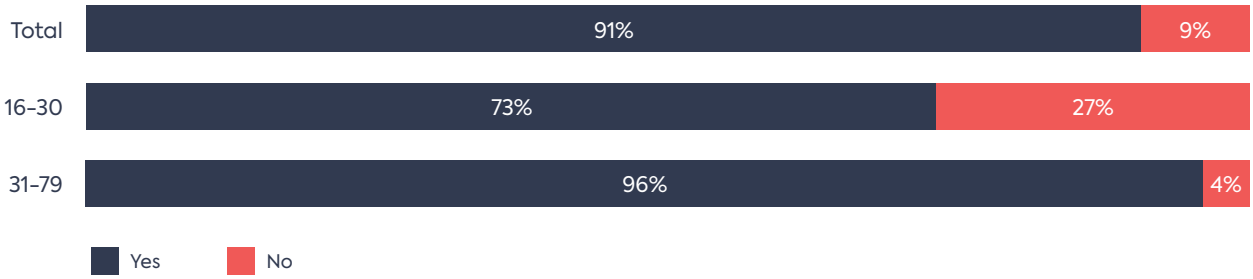


Source: Indiville

Knowledge of phishing needs to improve

Some 9% of the Belgian population have never heard of phishing. The older age group is slightly more aware of this type of fraud. Only 4% have never heard of it. Yet nearly a third of young people are not familiar with the term 'phishing'. This is a worse result than a year ago and is a particular cause for concern.

Have you ever heard of phishing?



Source: Indiville

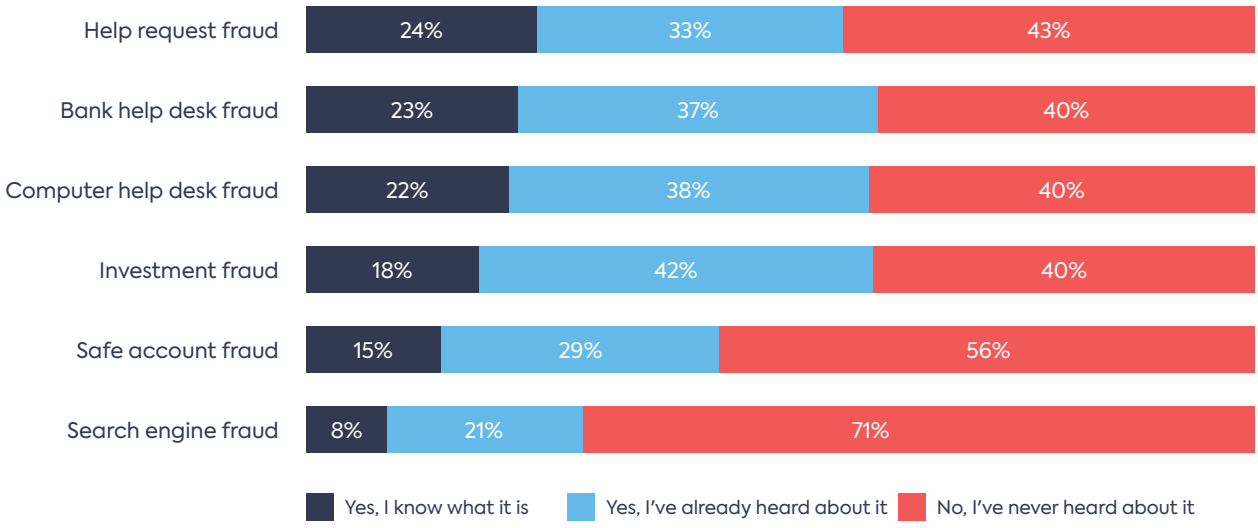
This figure shows how crucial it is to keep young people informed and vigilant about phishing, as they are still a prime target for cybercriminals. Febelfin therefore does its utmost to adapt its communication to this target group. For example, in November 2023, we launched the campaign 'Phishing: the devil's in the details!' in collaboration with Safeonweb and the Cyber Security Coalition. And we created a mobile escape game, The Hacker Hotline, which sees Febelfin criss-crossing the country every week to educate young people. It makes them aware of the dangers of online fraud in a fun way and teaches them how to protect themselves.

OTHER LURKING DANGERS

Other forms of online fraud are on the rise

Forms of online fraud where the victims make the transfer themselves at the cybercriminal's behest have continued to increase. Examples include invoice fraud, CEO fraud, friendship fraud, help request fraud, bank and computer help desk fraud, investment fraud, and safe account fraud. Belgians generally know little or nothing about them. On average, just under one in five Belgians know what the forms of fraud entail: 33% have heard of it, but almost half the population is completely in the dark. On average, young people seem to be slightly more aware of these forms of fraud than the other age group (17% versus 21%). But awareness remains low in both groups.

Do you know what these forms of fraud are?



Source: Indiville

TIP

If you still can't see the wood for the trees, take a look at the **online file** on the Febelfin website and find out about different types of online fraud.

More reports of bank and computer help desk fraud

More cases of bank and computer help desk fraud were reported over the past year.

WHAT IS COMPUTER HELPDESK FRAUD?

In computer helpdesk fraud, scammers call you pretending to be employees from the help desk of a computer company. They ask you to turn on your computer and follow their instructions, making as though there is a problem with your computer. Nothing could be further from the truth: in fact, they hack you and take over your computer to empty your accounts.

WHAT IS BANK HELPDESK FRAUD?

Bank helpdesk fraud is similar to computer help desk fraud but the scammers pretend to be from your bank. They call you to share your computer screen and provide personal codes because suspicious transactions have supposedly been detected in your bank account. This is how they are able to make transfers from your account and cheat you out of large sums of money.

Febelfin issues several press releases in this context, urging you to be cautious if you are contacted and asked to share your computer screen, divulge personal codes, and carry out online transactions.

A bank employee or a computer firm's help desk employee will never ask you for your personal codes or prompt you to install software that allows them to take over your computer remotely.

Beware of Card Stop fraud by phone

Another type of fraud we have warned about several times in 2023 and more recently is Card Stop fraud. How does it work? People receive a call from a mobile phone number. The voice on the other end claims to be from Card Stop, saying that suspicious transactions have been detected on a bank account. In fact, this is a fraudulent call not from Card Stop but from scammers. In partnership with Worldline, Febelfin has reminded consumers that they should never give out their bank details by text message, email, social media or telephone.

INTERESTING SNIPPET

In the sector, we often call this behaviour robotic phone scamming, i.e. a robotic voice calls numbers en masse and asks the person on the line to press a button if they want further assistance. A human operator then takes over, knowing that the potential victim has already been fooled by the robot manipulation and is thus more likely to fall into the trap after the human manipulation.

Banking help at home mostly results in scams

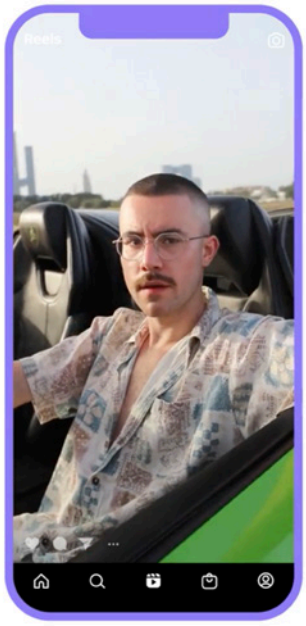
A new type of scam that we have seen in recent months involves 'a bank's fraud service employees', 'Card Stop employees' or 'the police' contacting elderly people by telephone to inform them that fraudulent activity has been detected in their accounts. These fraudsters then suggest visiting the victim's home to 'resolve' the situation. Unfortunately, they have only one goal in mind: to steal as much as possible (bank card, cash, jewellery, and so on).

Because senior citizens are obviously a vulnerable target and we want to avoid these cases as much as possible, we have communicated about this in partnership with the Federal Police and the FPS Home Affairs.

Investment fraud peaks

Investment fraud is on the rise. In 2023, fraudsters managed to pocket at least €15.48 million (source: FSMA) through investment fraud. Investors are slightly more aware of investment fraud. However, it generally remains a little-known form of fraud among Belgians.

For this reason, Febelfin launched a campaign on investment fraud in March 2024 in collaboration with the well-known influencer Jonatan Medart entitled 'Don't follow your hero with money!'. From a luxury yacht, he urged his followers to follow his financial advice and join his private Telegram group to, as he put it, 'get rich quick'. In the end, it turned out to be one big lie, and Jonatan reminded his followers to be on the lookout for investment scams from fake 'finfluencers' on social media. Febelfin reached a lot of young people with the essential message 'Don't follow your hero with money!' in this way.



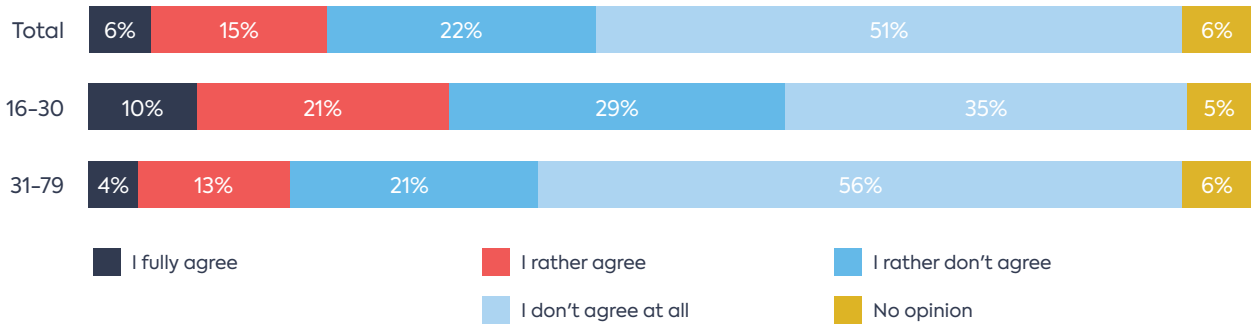
Tips to avoid investment fraud:

- **Always check the identity of the provider:** name, registered office, country of establishment, contact details, and so on.
- **Never trust a provider that you cannot clearly identify.** If the company is based outside the EU, be aware that difficulties could arise if you end up in a dispute and want to take legal action.
- **Be wary of 'cold calling':** If someone contacts you online or by telephone with an unsolicited financial offer, this is often a fraudulent practice.
- **Be wary if the person contacting you asks you to transfer money** to a bank account in a country other than where the provider is based.
- If the provider requests **an additional payment**, this is often a sign of fraud.
- Briefly put, if it sounds too good to be true, it usually is.

How do we perceive security in online shopping?

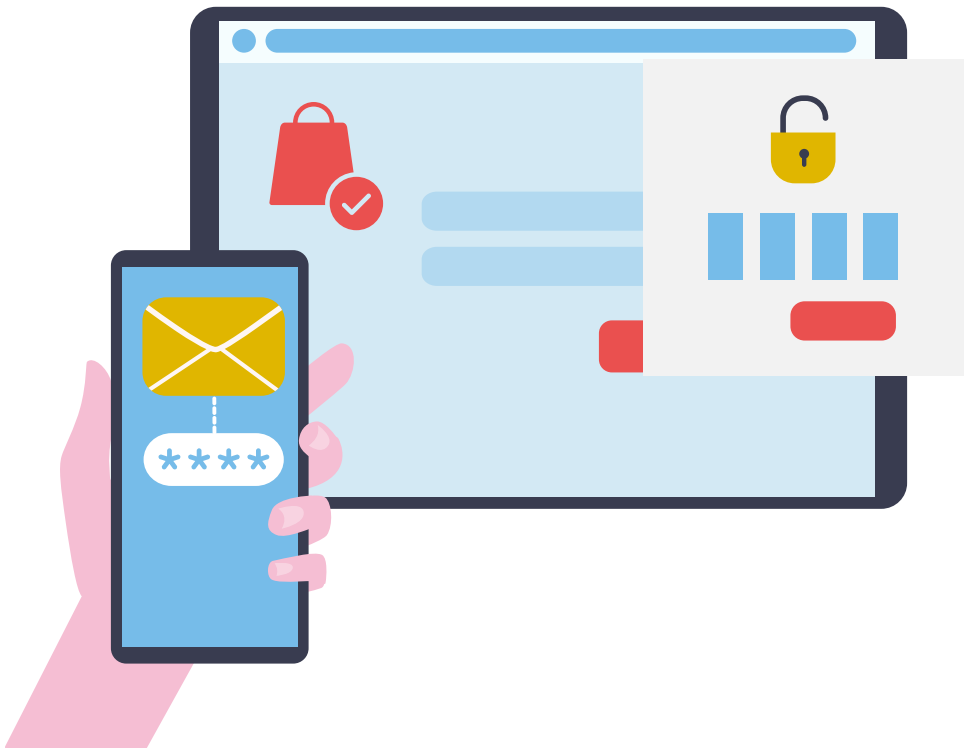
Thankfully, most Belgians do not view the various security steps (2-step verification or multi-step confirmation of your identity) for online purchases, such as entering card reader response codes or your itsme code, to be excessive. This is another improvement, as was the case last year. That's a good thing.

I find it unnecessary to have to go through several steps when shopping online



Source: Indiville

Yet one in five Belgians still consider these security measures more of an obstacle than a means of protection. Among young people, the group who find these steps more annoying is somewhat larger (31%). That's why it is and will remain important to make every effort to better inform young people and change their attitudes towards online safety measures. We must therefore ensure they are seen as necessary protection from online risks, not a hindrance.



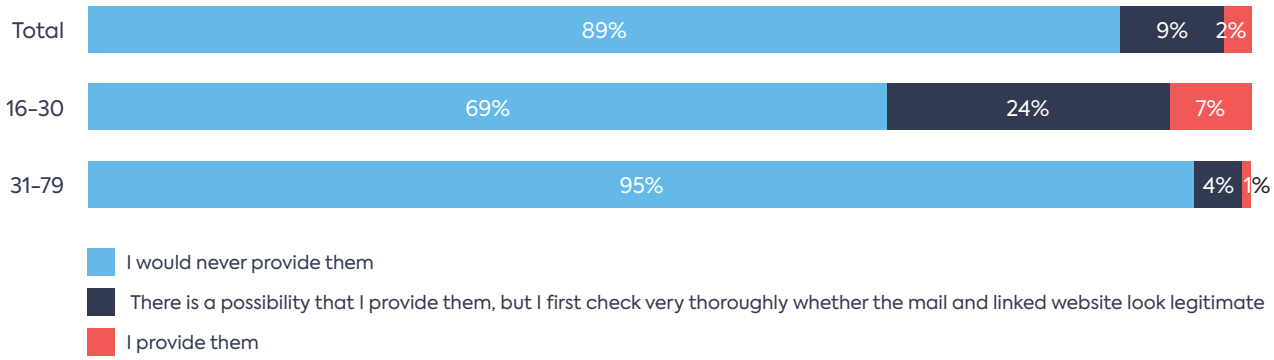
Fewer people share codes or send their bank card!

There is also good news to share. We are all better at not giving out bank codes and not returning bank cards:

89% of Belgians would not share their codes with the bank under any circumstances.

However, 2% of the population, and 7% of young people, would not hesitate to give their bank code if the bank asked for it. Although this percentage is still too high, it is an improvement for the second year in a row (2023: 10%; 2022: 13%).

If the bank asks for my bank codes ... by e-mail, text, whatsapp, phone ...

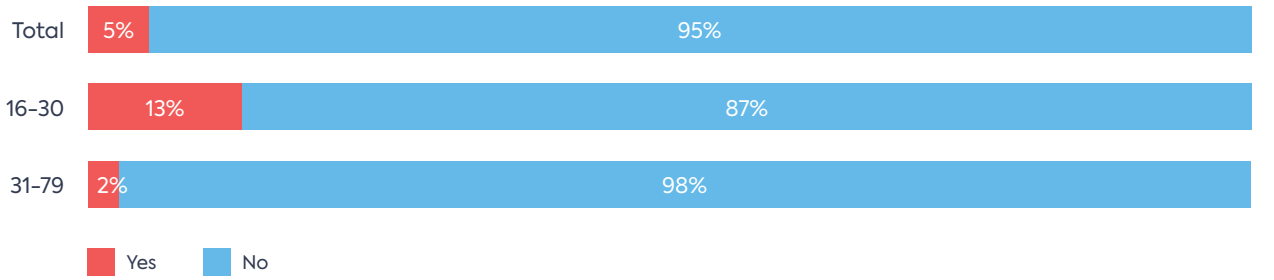


Source: Indiville

95% of Belgians would not return their bank card to the bank under any circumstances. Again, young people do slightly less well in this regard than the rest of the population. Although

13% would return their card if asked by the bank, this is again better than last year (2023: 17%).

Would you return your bank card if your bank asks for it by e-mail, text, whatsapp, phone, letter ...?

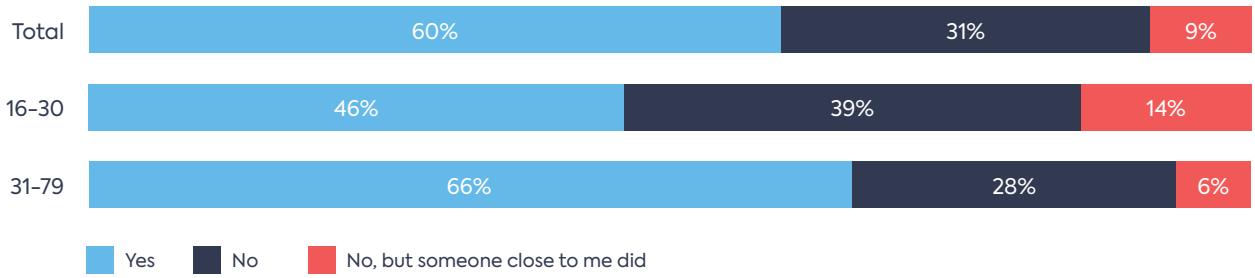


Source: Indiville

Action is also taken more often when online fraud is suspected

We see a positive trend in terms of actions taken when fraud is suspected. 60% of phishing victims knew what to do and 91% acted when they suspected actual or attempted online fraud, such as checking their account or contacting Card Stop.

Did you know what steps to take or where to go for help?



Source: Indiville

53% checked their accounts carefully, 30% called the bank, and 26% called Card Stop. Although on average young people are less aware of what best to do if they suspect fraud, they are now in the habit of checking their accounts more often than in previous years (2024: 51%; 2023: 44%, 2022:34%). This is a step in the right direction.

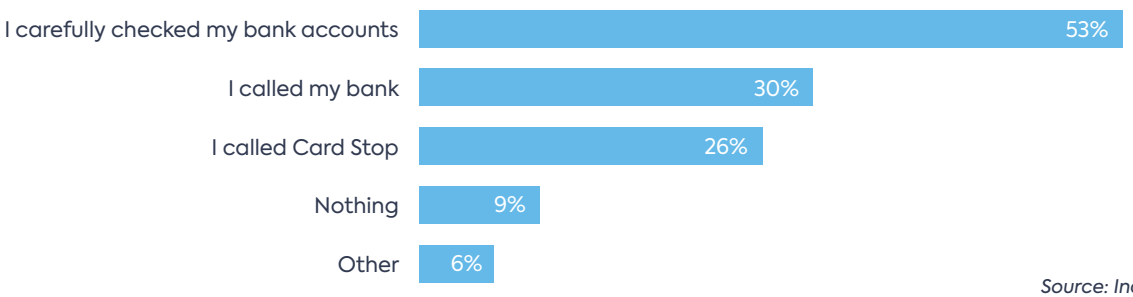
DO YOU KNOW THE CARD STOP NUMBER?

You can reach Card Stop on **078 170 170** if you want to block your payment card after theft, loss or attempted fraud.

ARE YOU A VICTIM OF ONLINE FRAUD?

Contact your bank as well. Banks have dedicated fraud departments that can be contacted 24/7. You can find all the contact details on **the Card Stop website** (only in Dutch/French).

What did you do with this feeling?



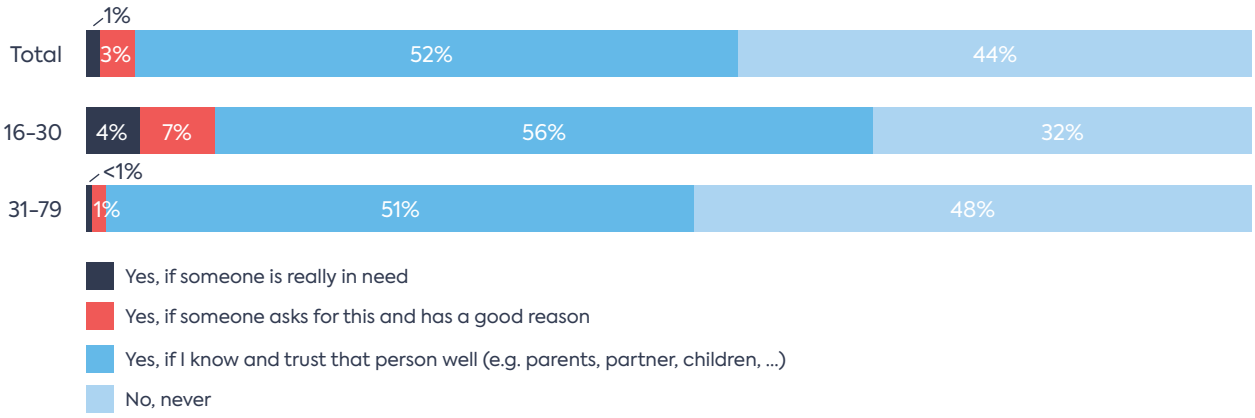
Source: Indiville

Awareness about the issue of 'money mules' is still too low

Has anyone ever approached you and asked if you would like to make some quick and easy money by lending your bank account and/or bank card for a while? For young people in particular, the temptation remains strong.

4% of the Belgian population would give their bank card and PIN code to someone they do not know, in exchange for money. 11% of young people would do so. Although this is an improvement compared to last year, it is obviously still too high.

Would you give your bank card and PIN code to someone else?



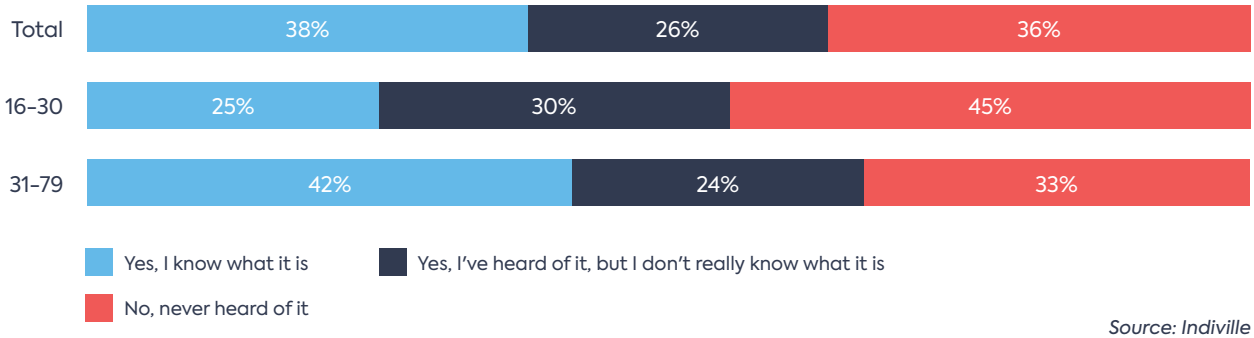
Source: Indiville

WHAT IS A MONEY MULE?

A money mule is someone who lets criminals use their bank account and/or bank card and PIN code for money laundering. This allows the criminal to deposit the proceeds of crime in the money mule's bank account for subsequent withdrawal (using the money mule's bank card and PIN code) or a transfer to other accounts. The scammers thus get off scot-free. Read more about this in our **online file**.

While almost 40% of Belgians know what a money mule is, only 25% of young people do. 45% of young people have never even heard of the phenomenon of phishing.

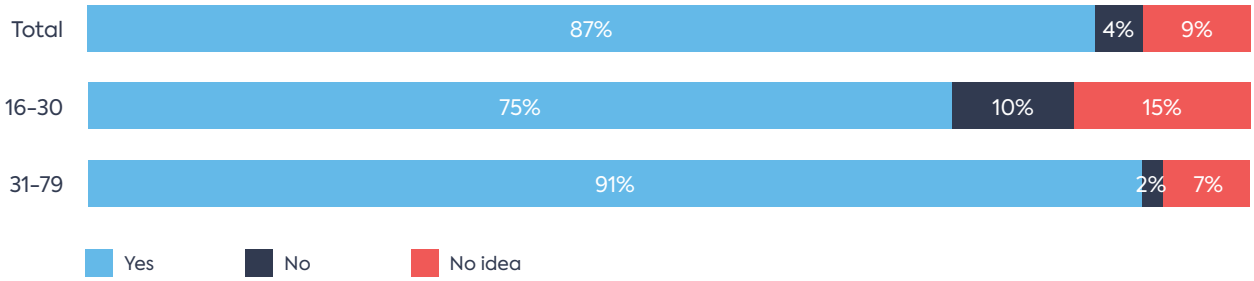
Do you know what a money mule is?



Source: Indiville

Young people are also often unaware that it is a criminal offence to act as a money mule. Yet the consequences are severe, ranging from prison sentences and fines to compensation for the victims, and more.

Do you think being a money mule is punishable?



Source: Indiville

Furthermore, 3% say they have been approached by a fraudster asking them to be a money mule and 5% know people who have been asked. This percentage is also higher among young people: 6% have already been approached themselves and another 12% know someone else this has happened to.

Have you ever been approached to become a money mule yourself?

Explaining the phenomenon of 'money mules', especially to young people, and making them aware of the risks and criminality involved, therefore remains essential. After all, they are a prime target for this type of fraud.

THE FINANCIAL SECTOR IS CONSTANTLY DEVELOPING NEW INITIATIVES TO COMBAT ONLINE FRAUD

E-learning voor digitale begeleiders

In 2023, Febelfin launched a new e-learning course for those guiding people through their first steps in the digital world. Through the e-learning course, we offer these digicoaches the necessary tips and tricks and handy tools to help less digital-literate consumers. Special attention is given to online safety and the different forms of online fraud.

The e-learning course has been a great success, with nearly 400 volunteers and professionals completing it so far. This success again highlights the relevance of raising awareness and training among different target groups and stakeholders.

IBAN-name check

The sector is also doing its utmost to facilitate the introduction of the **IBAN-name check**. This tool deters certain types of transfer fraud, such as invoice fraud. When a transfer order is entered, the client's bank checks with the beneficiary's bank that the account number (IBAN) and the beneficiary's name match. If this is not the case, the bank will warn the client through the IBAN-name check of a possible fraud or scam. Banks are therefore doing their utmost to facilitate its introduction.

The incident warning system

The **incident warning system** is a project in which banks could share information on payment incidents to further protect customers from suspicious incidents.
The identification of suspicious acts could be shared among banks so that they can take into account the identified risks.
Sharing such information will happen in accordance with the Personal Data Protection Act.

The financial sector advocates for the realisation of this project that will contribute to an even more effective fight against online incidents and the issue of money mules.

Customised workshops and information sessions for different target groups

To raise more awareness of young people as a significant and vulnerable target for cybercriminals, we continued to work with schools, youth organisations and local partners last year.

Our mobile escape game, The Hacker Hotline, travels across the country each week to warn young people in a fun and accessible way about the risks of online fraud and to give tips on how to avoid falling into the trap.

We also continue to hold information sessions on online fraud forms, with a particular focus on 'money mules'. Febelfin participated in the 'Safety Day' organised by the Knokke-Heist police and fire brigade. We delivered workshops there on online fraud and money mules to the various local secondary schools, reaching over 1,000 students.

To reach and inform as many vulnerable groups as possible, we continue to offer information sessions on secure digital banking to other target groups, such as senior citizens. During these sessions, we will answer all their questions about digital banking and its security, together with representatives from various banks.

Febelfin also collaborated on an E-learning 'Cybersecurity' course with the Flemish Service for Employment and Vocational Training (VDAB) that will be offered to everyone who has a VDAB account.

'Cybersecurity' stakeholder event

Febelfin organised a cybersecurity stakeholder event in cooperation with the BIN knowledge centre and the federal departments of the Governors of Flemish Brabant and Antwerp. Together, we sought answers to pressing questions such as 'How can we work more closely together as stakeholders?' and 'How can we better share critical cybersecurity information with our local target groups?' This allowed inspiring ideas to be exchanged and cybersecurity was once again placed high on the agenda.

Annual awareness campaign about money mules

Aware of the dangers of the phenomenon known as money mules, Febelfin is committed to raising awareness through an annual press release, roadshows for young people and free educational material. Read more about this on page 10 of this storytelling brochure.

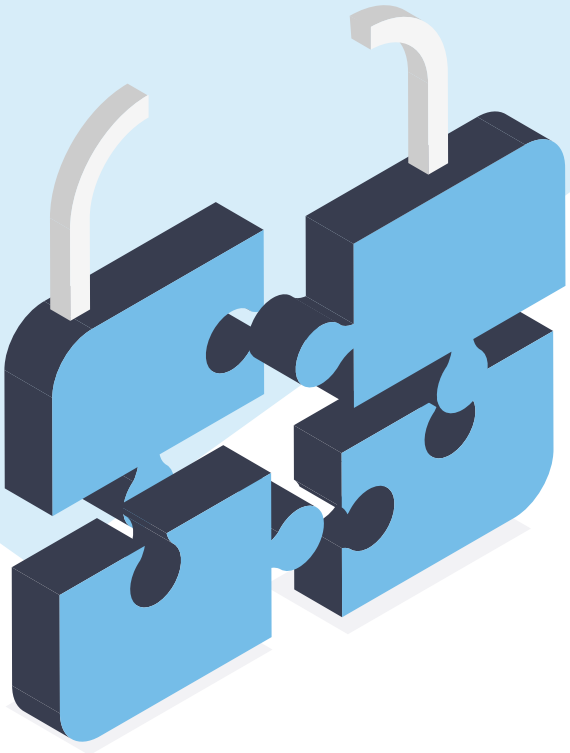
COLLABORATION BETWEEN STAKEHOLDERS REMAINS CRUCIAL

The sector recognises that we can only succeed in the fight against phishing and online fraud by working together. Ongoing cooperation with the various stakeholders, government and grassroots organisations is and will continue to be necessary. Febelfin will therefore propose to other stakeholders that we pool our expertise and resources to work on joint campaigns in the future.

As the techniques of online fraudsters continue to evolve through technological developments such as AI and deep fakes, we will continue to face many challenges. It is crucial that we continue to monitor these developments together and have the necessary flexibility to adapt.

It is only by developing a shared vision and strategy between all stakeholders on how to continue the fight against cybercrime and keep the economy running safely that we can work together to ensure that everyone feels secure in the digital world of today and tomorrow.

Febelfin made some recommendations in its political memorandum on cybersecurity, which you can find here.



Belgian Financial Sector Federation

www.febelfin.be