febelfin

If it smells phishy, it probably is!

IF IT SMELLS PHISHY, IT PROBABLY IS

Online fraud remains a persistent problem. In 2024, cybercriminals continued to actively send phishing messages, pretending to be a trusted person or organisation, such as a bank or government agency. Fortunately, the banking sector was able to detect, block, or recover 75% of fraudulent transactions resulting from phishing. Still, scammers managed to steal €49 million through phishing.

€ 49 million obtained in 2024

Online fraud continues to evolve— in increasingly devious ways. What once began with simple phishing emails has now grown into more sophisticated scams where people are persuaded to transfer money themselves. It often starts with a convincing phone call, a professional-looking website, or an urgent request via a trusted app like itsme®. Before you know it, it feels like you're speaking with your bank or being offered a golden investment opportunity.

Investment fraud, bank helpdesk fraud, and misleading requests via digital platforms are becoming more refined. And although many efforts have been made to warn people, awareness among a large part of the population still lags behind. As in previous years, many Belgians remain insufficiently protected against these modern forms of deception.

Fortunately, more people are reacting alertly when they suspect fraud—for example, by immediately contacting their bank or checking their account balance and transactions. At the same time, general knowledge about phishing and money mules is increasing. The number of people who share their PIN or send their bank card to a provided address is also decreasing. These insights underline the importance of continued awareness. Anyone can become a target of online fraud. Young people, in particular, seem vulnerable, partly due to their often casual attitude towards online safety..

That's why the sector continues to invest in innovative initiatives and strong collaborations to effectively tackle online fraud. By joining forces with partners from various domains—technology, financial institutions, government, and education—we are building a strong front against cybercrime. Through targeted campaigns, smart tools, and ongoing awareness, we aim not only to respond to fraud but to prevent it more often. Because only together can we strengthen everyone's digital security.

Discover all the details in our storytelling with the most recent figures and an overview of some new initiatives of the sector.

THE CATCH BY PHISHERS REMAINS LARGE

They arrive as innocent messages. A notification from your bank, a warning from the police, an update from your health insurer or water company. Everything seems familiar—until you take a second look. Behind names like De Christelijke Mutualiteit (Christian Mutuality), RIZIV, De Watergroep or the federal police, there's often a scammer with a plan.

Phishing has become one of the most commonly used forms of online fraud. Safeonweb, the reporting centre of the Cybersecurity Centre Belgium, receives nearly 26,000 reports of suspicious messages daily. That's almost 9.5 million per year—a staggering figure that shows how persistent this form of fraud is.

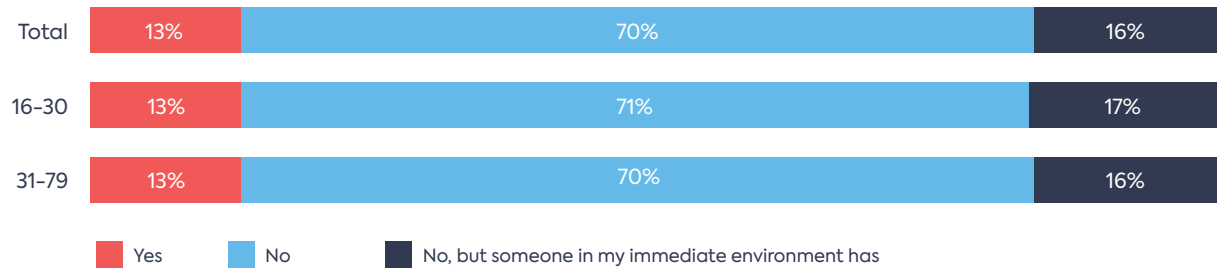
And although banks manage to detect, block, or recover 75% of fraudulent transfers, phishing remains a lucrative practice. In 2024 alone, around €49 million was stolen through this method. It shows how convincing these attacks have become—and how important it is to stay alert..

A study by Febelfin in collaboration with research agency Indiville[2] confirms the vastness of this type of fraud.

A current threat

The study shows that 13% of Belgians have ever been the victim of phishing.

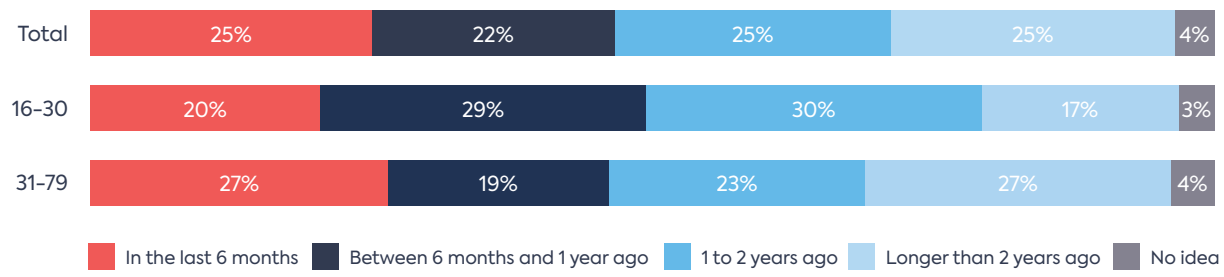
Did you become a victim of phishing?



Source: Indiville

When asked when respondents fell victim, the data shows phishing remains a current issue.

Hoelang was dit geleden?



Source: Indiville

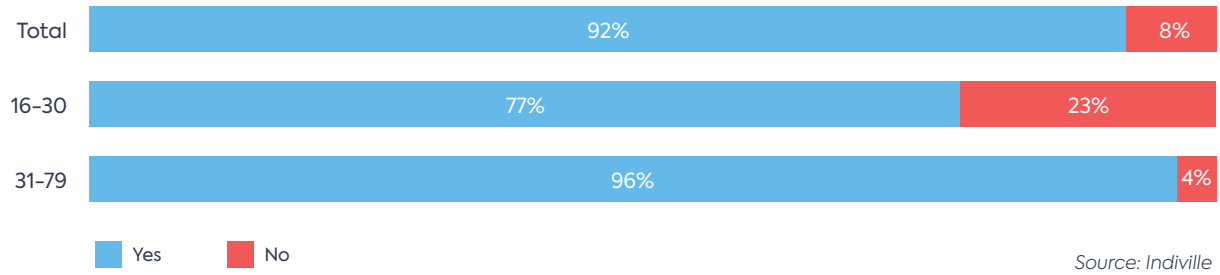
[1] Source: Safeonweb july 2025
[2] IndiVille research, 20 January – 9 February 2025, based on a representative sample of the Belgian population , n: 2,149 NL/FR surveys, aged 16–79. Maximum margin of error: 2.1%

Knowledge about this type of fraud

Although many people are aware of the danger, knowledge about phishing still needs improvement. Did you know 8% of Belgians have never heard of phishing? Among young people (16–30), this rises to 23%. Older people are generally better informed: only 4% have never heard of phishing.

This shows that awareness initiatives aimed at older adults—such as info sessions on safe online banking and payments (see p.12) —are paying off.

Have you ever heard about phishing?



Source: Indiville

Important pitfalls, especially for young people

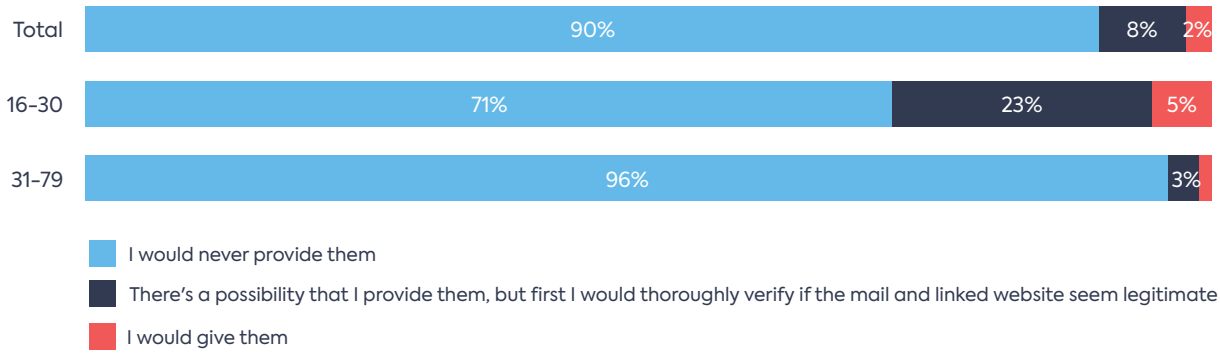
Sharing bank codes & financial information

Most Belgians now know: you should never share your bank codes. Regardless of age, 9 out of 10 respondents say they would never share their codes under any circumstances. Still, a small minority—2%—would do so without hesitation.

Among young people, the picture is less reassuring. 23% say they might share their bank codes if asked via email, SMS, or another digital channel—after carefully checking the message and linked website. 5% would share their codes without any verification.

The good news: in 2022, 13% of young people said they would share their codes without hesitation. That figure has now dropped to 5%, showing that awareness campaigns are working—though vigilance remains essential.

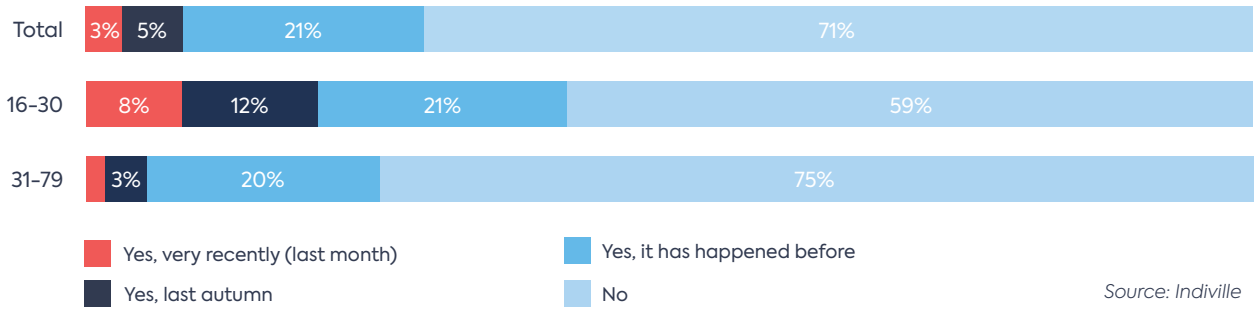
If the bank asks for bank codes via e-mail, sms, whatsapp, telephone ...



Source: Indiville

Additionally, young people are more likely to share financial information online that they feel uncomfortable about. 8% of all respondents did so in recent months. Among young people, this rises to 20%.

Have you ever provided financial information online that you felt uncomfortable about?



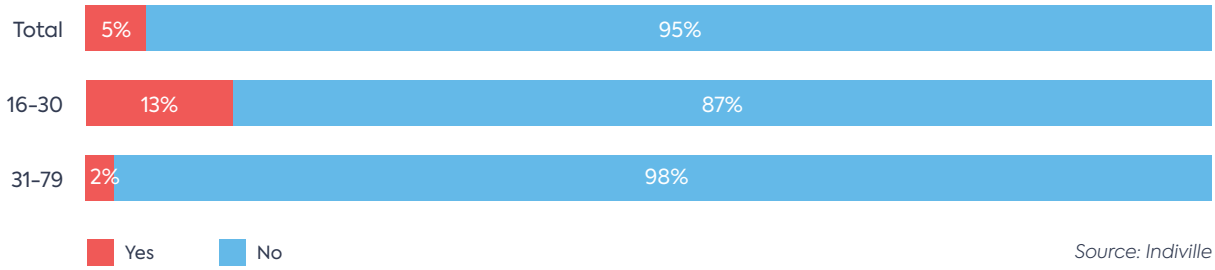
Source: Indiville

Sending bank cards

Imagine receiving a call or message from your 'bank' saying your card is about to expire and asking you to send it in along with your PIN. Most Belgians would say no, of course. 95% of respondents say they would never send their bank card, even if urgently requested by a supposed bank.

Among young people, 13% say they would be inclined to send their card—an alarming figure that hasn't improved since last year. This highlights the need to continue informing young people about the risks. Scammers are getting smarter, and a moment of doubt can be enough.

Would you send your bank card if the bank asks this via e-mail, sms, whatsapp, telephone, letter ... ?



Source: Indiville

WHAT DO YOU UNDERTAKE IF YOU FALL INTO A PHISHING TRAP?

Knowledge of the steps to take

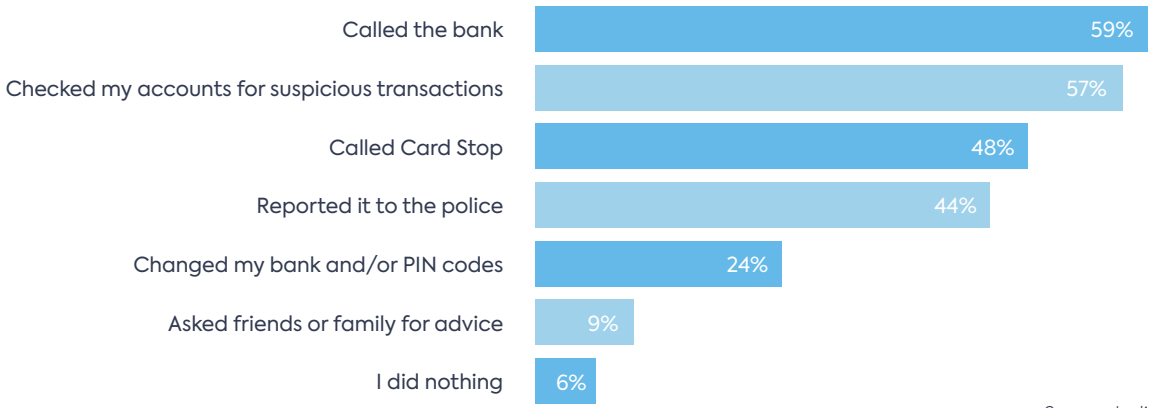
It's a question no one wants to ask themselves, but one you should know the answer to. Because even with all the warning campaigns and prevention tips, it can still happen: one click, a moment of inattention, and you're a victim.

Fortunately, more and more people know what to do when things go wrong. The study shows that 64% of victims immediately knew what steps to take or where to seek help. Another 6% didn't know themselves but were able to get good advice from someone in their network.

Still, there's work to be done—especially among young people. In the age group of 16 to 30, a striking 39% said they didn't know what to do after a successful phishing attempt. In comparison, among those aged 31 to 79, that figure is 27%. This shows that knowing what to do after phishing is at least as important as preventing it.

Because those who know what to do can act quickly. And quick action often makes the difference between limited loss and major damage.

Which of the following steps did you take?



Source: Indiville

To better guard people against online fraud, Febelfin—together with the local police and partners such as SAAMO, CAW, and other stakeholders—has developed a new flyer. This handy guide brings together all the essential information in one place: what to do in case of online fraud, where to seek help, and how to better protect yourself. It's a practical tool that helps people navigate a confusing situation in an accessible way.

DOWNLOAD THE FLYER →

The importance of ongoing awareness

The numbers speak for themselves: more and more people recognise the signs of phishing. There has clearly been progress in awareness around online fraud. But it remains crucial to continue building knowledge and digital resilience—especially among young people, who often live in an online world where risks aren't always visible.

That's why the financial sector is fully committed to targeted actions. Not only by teaching young people how to recognise and avoid phishing, but also by supporting victims with clear steps and accessible help. Because the faster someone knows what to do, the smaller the damage.

In this context, Febelfin launched a striking **campaign** about fraud in online games—a theme that directly appeals to young people. Additionally, the educational platform **Klassebank** was launched, where teachers can find guest lessons and teaching materials on financial topics, including online fraud. The goal? To empower young people in their digital choices and give them the knowledge they need to navigate safely in an increasingly complex online world.

klasse bank

WATCH THE VIDEO (ONLY IN DUTCH/FRENCH) →

PHISHING MAY BE THE MOST WELL-KNOWN FORM OF ONLINE FRAUD, BUT IT'S FAR FROM THE ONLY ONE

Other forms of online fraud still not well known

Online scammers are not standing still.
In addition to phishing, they increasingly use other forms of online fraud to deceive victims. Think of Help request fraud, where someone pretends to be a friend in need. Investment fraud, promising quick profits. Bank and computer helpdesk fraud, which are gaining ground. Recent scams involving the itsme® identification app, where fraudsters ask victims to approve actions that actually benefit the scammer.

Examples of itsme® fraud:

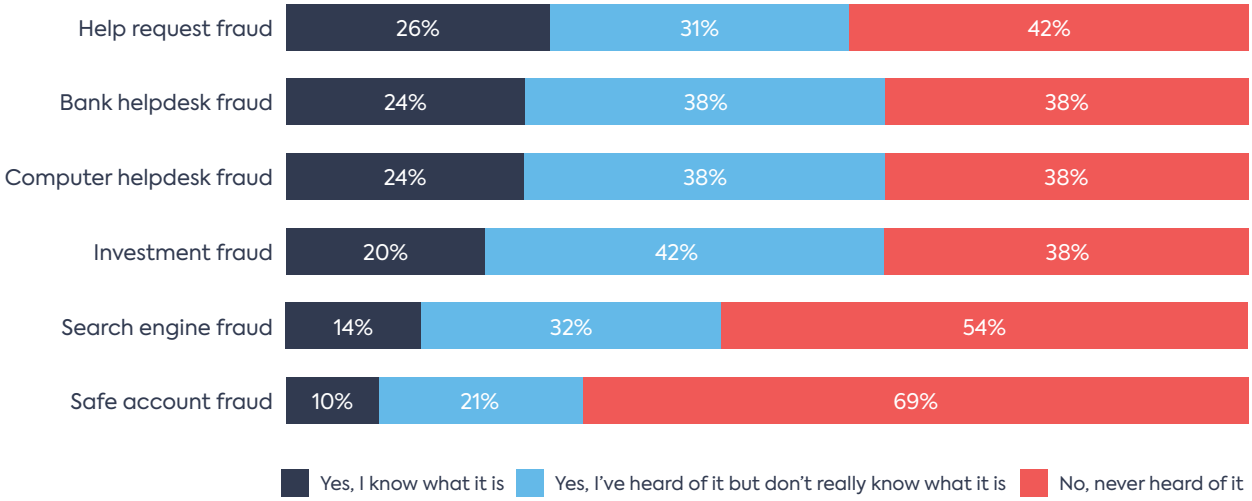
- Victims are told that suspicious payments have been detected and that they can cancel them via itsme®. In reality, they are approving the fraudster's transactions.
- A fake bank employee asks the victim to confirm their identity via itsme®, but in doing so, the victim unknowingly grants access to their online banking environment.

DISCOVER SEVERAL TIPS TO PREVENT THIS TYPE OF FRAUD →

Research shows that these types of fraud are still poorly understood by the general public. Only 1 in 5 Belgians knows exactly what these fraud types involve. A third has heard of them but doesn't fully understand. Nearly half are completely in the dark. Notably, this lack of knowledge is not age-related—young or old, most people are unfamiliar with these scams.

Some types of fraud are almost entirely unknown. 69% have never heard of safe account fraud and 54% are unaware of search engine fraud. Even investment fraud, which often appears in the news, is only fully understood by 20% of respondents.

Do you know what these types of fraud are?



Source: Indiville

This shows there's still a lot of work to be done. After all, how can you protect yourself from something you don't know exists?

The financial sector continues to communicate and develop initiatives to raise awareness about these types of fraud.

TIP

In Febelfin's online file, the various types of online fraud are clearly explained, and you'll find valuable tips on how to protect yourself.

READ MORE →

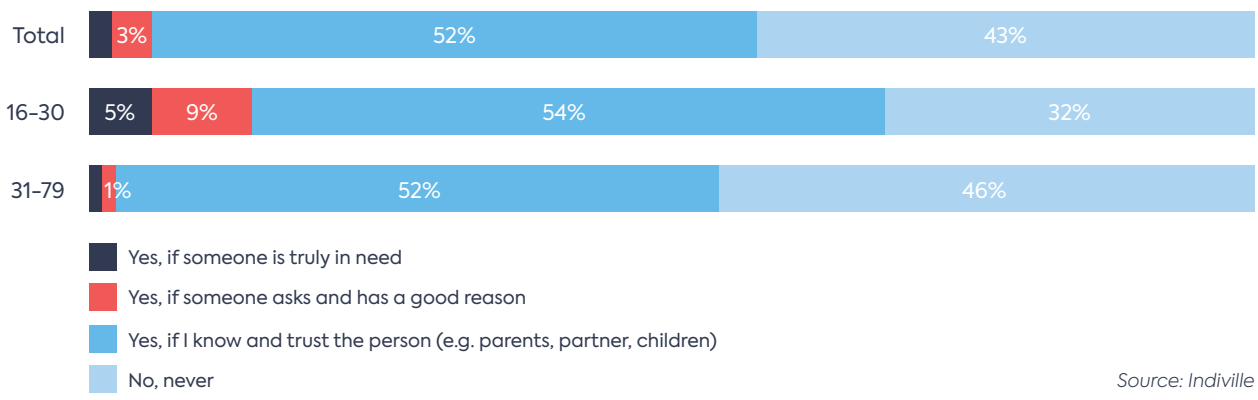
MONEY MULES

Quick cash? Sounds good, right? A stranger asks to borrow your bank card or account for a moment. Easy money, it seems. But behind that innocent request often lies something much more serious: you become a money mule—and thus an accomplice to fraud.

People still fall into the trap. Research shows that 14% of young people are willing to share their bank card and PIN for money—a slight increase compared to 2024. Among the general population, this figure is 5%.

What starts as a quick deal can end with a criminal record. That's why Febelfin continues to warn: don't be misled.

Would you provide your bank card and PIN to someone else?



Source: Indiville

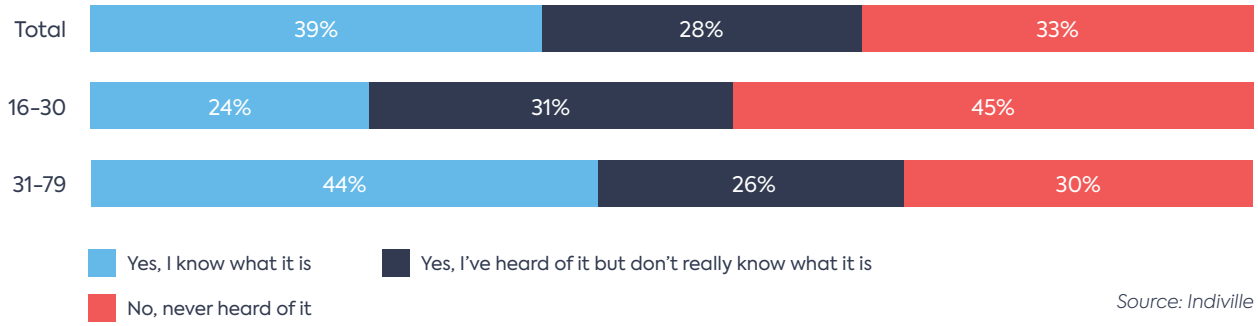
WHAT IS A MONEY MULE?

A money mule is someone who allows their bank account and/or bank card and PIN to be used by criminals to launder money. This allows the criminal to deposit illegally obtained money into the money mule's bank account and then to withdraw it (using the money mule's bank card and PIN) or transfer it to other accounts. In this way, the fraudsters stay out of the loop. Read more about it in our **online file**.

What is a money mule? Many young people have no idea

While nearly 40% of Belgians know what the term means, among young people that figure drops to just 24%. A striking 45% have never heard of it.

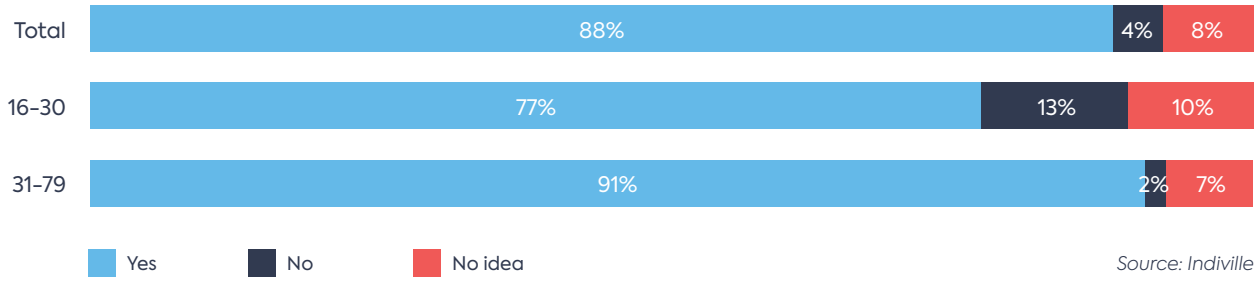
Do you know what a money mule is?



Source: Indiville

What many don't realise is that lending your bank account or card for criminal purposes is a punishable offence—with serious consequences such as fines, prison sentences, and having to repay victims.

Do you think being a money mule is a criminal offence?



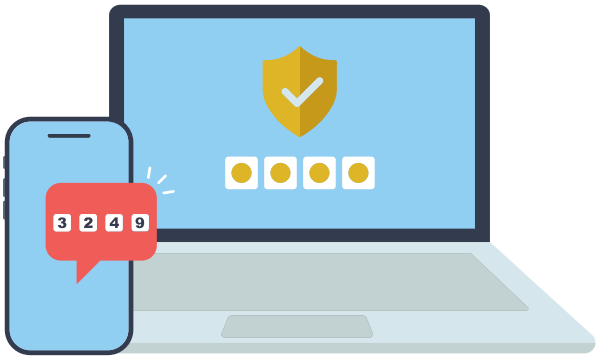
Source: Indiville

Yet the phenomenon remains under the radar. The study shows that 4% of Belgians have been approached to become a money mule. Another 4% know someone who has. Among young people, the numbers are even higher: 7% have been approached and 12% know someone who received such a proposal.

Have you ever been approached to become a money mule?

These figures have remained stable for years, and that's concerning. Young people continue to be a major target for this type of fraud. That's why it's essential to keep informing them about what a money mule is—and especially, what the risks are.

ONLINE SHOPPING: FAST, EASY... AND SAFE?

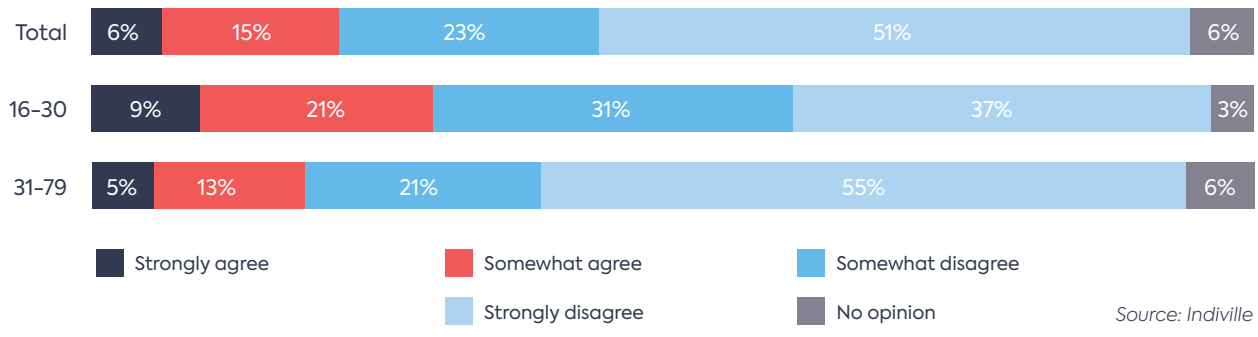


For many Belgians, extra security steps during online purchases—such as entering an additional code, using a fingerprint, or a card reader—have become second nature. They know those few seconds offer extra protection against fraud.

However, not everyone sees it that way. The study shows that 1 in 5 Belgians considers these steps more of a burden than a safeguard. Among young people, this perception is even stronger: 30% find them cumbersome, compared to 18% of older generations.

And that's not without risk. Those who view security as unnecessary are often less alert to online scams. That's why it remains important to explain why that extra click or code is needed—especially to young people, 3 in 10 of whom still don't fully grasp the importance of these digital safeguards.

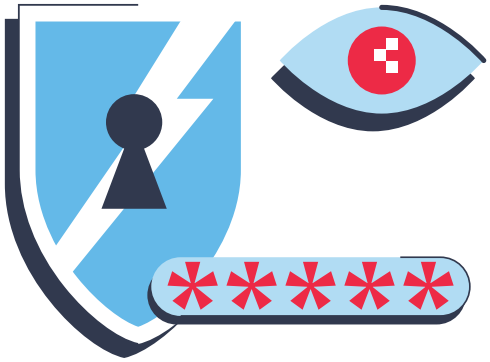
I find it unnecessary to go through multiple steps when making online purchases



Source: Indiville

THE FIGHT AGAINST ONLINE FRAUD IS NOT A SOLO MISSION, BUT A SHARED RESPONSIBILTY.

Online fraudsters are getting smarter—and so must we. To reduce online fraud, it's essential that all stakeholders continue to raise awareness among the public. A vigilant and informed consumer is less likely to fall victim. The fight against financial crime is a **shared responsibility**, involving consumers, the telecom sector, and social media platforms. Only through **intensive collaboration**, supported by (European) legislation, can we turn the tide.



It doesn't stop there. Compliance with data protection and cybersecurity laws by all players in the chain—e-commerce merchants, online (social) media platforms, telecom providers—is crucial to combat online fraud and protect consumers. **These actors also have a societal responsibility.** The European Commission (EC), European Council, and European Parliament recognise this. As part of the revision of PSD2, the EC has proposed a Payment Services Regulation (PSR) to ensure liability frameworks and address these challenges. It includes additional tools to combat fraud and calls on all players in the chain to contribute.

In short, fraud prevention is not just the task of banks. **Banks need support from all ecosystem players to fight fraudsters**. Consumers, telecom providers, e-commerce merchants, social media platforms, and banks must work together to protect citizens from increasingly devious online scams.

Febelfin made several recommendations regarding cybersecurity in its political memorandum.

READ THE MEMORANDUM →

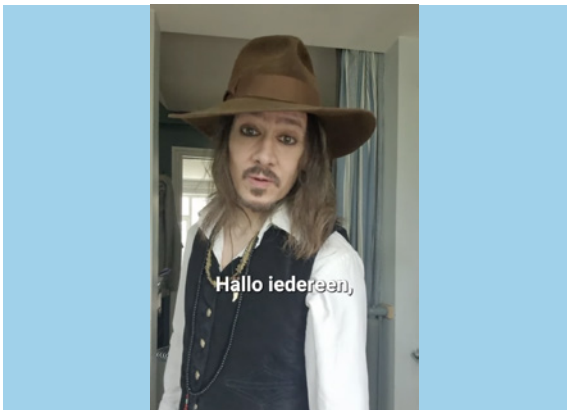
Febelfin didn't sit still last year

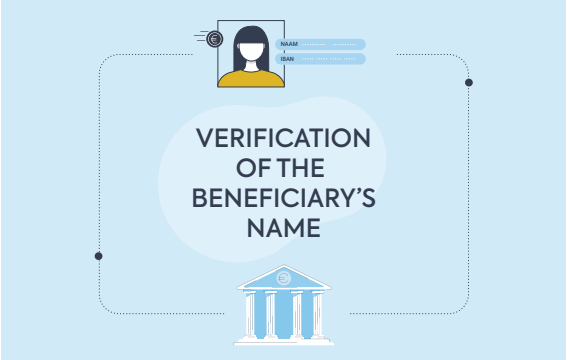
Febelfin launched **numerous initiatives**, always in collaboration with strong partners—because that's where its strength lies. Together with the local police, SAAMO, and CAW, Febelfin developed an accessible **flyer** with essential information for victims of online fraud. Thanks to a test panel assembled by SAAMO, they ensured that even vulnerable groups could understand and use the information.

Throughout the year, Febelfin organised **info sessions on safe online banking**. More than 450 digital helpers completed the e-learning, now equipped with knowledge about the latest fraud types and available educational materials.

We also responded to current events

In October, we collaborated with Safeonweb on two-factor authentication. We raised awareness about **social engineering via itsme®** and launched the striking **Johnny Depni campaign** (only in Dutch/French) on dating fraud, which prompted many testimonials. Our **youth campaign** with Andy Peelman (only in Dutch/French) was a hit: over 2 million young people watched the video in which he warns against sharing personal data in exchange for free game coins.





We also made progress in the technical field

We started to gradually implement the **Verification of the beneficiary's name** - a smart tool that alerts customers when the name and account number of a beneficiary do not match. This free service increases trust in transfers and helps prevent fraud.

And we continue!

The financial sector remains committed to developing new, targeted initiatives. Because only together can we make a difference in the fight against online fraud.

Belgian Federation of the Financial Sector
Koning Albert II-laan 19, 1210 Brussels
www.febelfin.be