There are plenty of ‘phish’ in the sea

Fraud and scams in the banking sector

febelfin

2020: too many 'phishers' in the sea

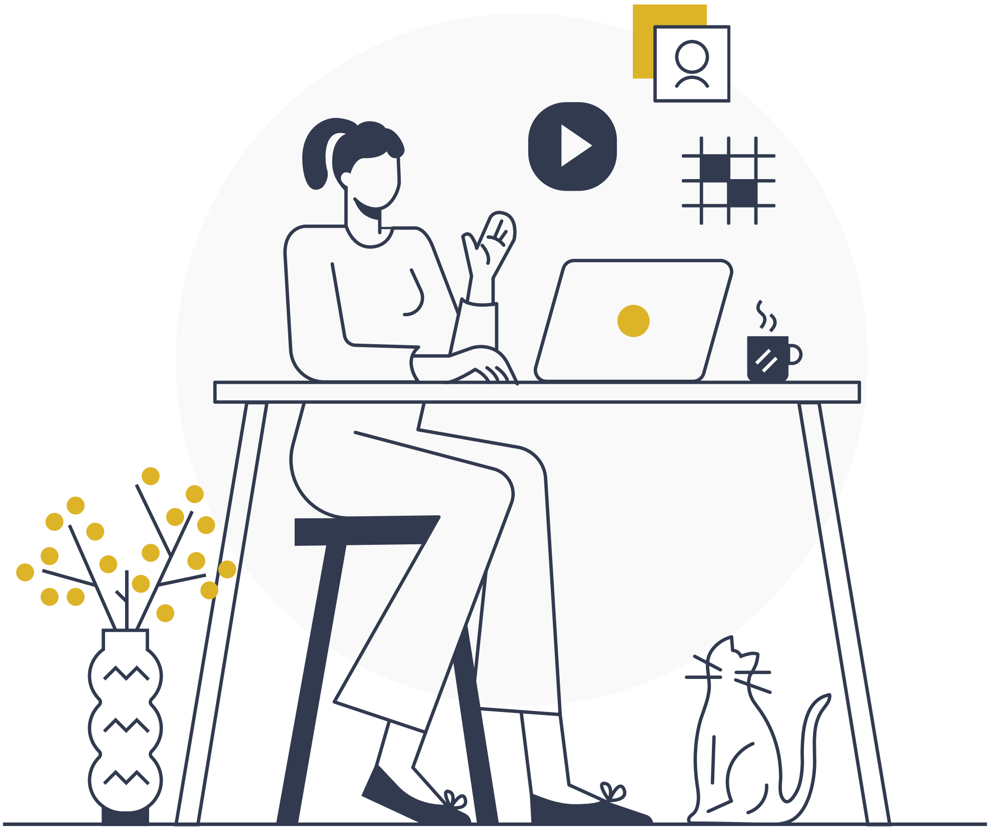
2020 was a year of unprecedented challenges: the pandemic drastically changed our daily lives and the lockdown measures had a significant impact on the economy. While families and businesses struggled, criminal gangs quickly capitalised on this by adapting their fraudulent practices to our changing lifestyles. Scams played on people's emotions and fear of the pandemic, with fraudsters posing as employees of trusted organisations such as health institutions, government agencies and banks. And coronavirus-related messages (about masks, promised benefits, and so on) attracted attention and thus increased the 'click rate'.

In 2020, internet users forwarded exactly 3,225,234 messages to the email address verdacht@safeonweb.be. At more than 8,800 a day, this was almost double the previous year's figure (1,7 million reports).
Source: Centre for Cyber Security Belgium (CCB)

Criminals also capitalise on the increase in online shopping and working from home by posing as couriers, e-commerce platforms or network providers. And they are recruiting 'money mules' to launder stolen money by placing fake advertisements on job boards and social media, targeting people looking for work or wanting to make easy money during the pandemic.

In 2020, Safeonweb detected 667,356 fraudulent links. Source: CCB

With fraudulent practices becoming increasingly sophisticated, fraudsters are using technology and the internet to develop an even more convincing approach. This has led to a continuous increase in fraud, with people even being persuaded to transfer money to a criminal. Examples include safe deposit account fraud or friend-in-need scams, two fraud techniques that emerged last year.



SOME INTERESTING FACTS

Fraudsters prefer to target **people** more often than systems. If you examine successful fraud cases of recent years, this is the constant theme. It is thus the simplest strategy for cybercriminals. Why would they attack complex firewalls and antivirus systems if there is an easier route to take? 9 out of 10 successful data breaches are caused by human error. 'People don't think, they click' is still very much the case in 2020.

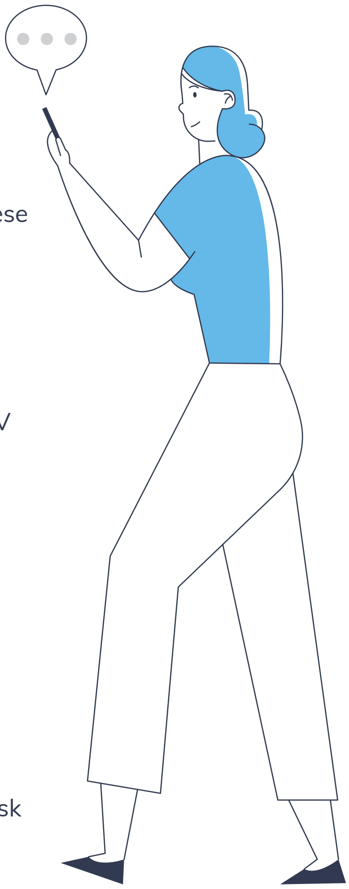
Phishers don't need to identify 'weak' profiles. Regardless of age, language, gender and education, anyone can become a victim of phishing.

The **shorter** and more to the point the content of an email is, the greater the chance that the recipient will open the malicious URL or attachment, especially when the recipient is being asked to help. For cybercriminals, phishing emails are not a question of rocket science or in-depth epistles: they are simply about asking the right question at the right time. And being obliging... people are only too willing to help, and enter their data.

Fraudsters like to take advantage of **current events**: even if the news is fake or contrived: people want to be the first to know the news and react too quickly. It is not only breaking news that works. Government or business news works just as well.

Unfortunately, fraudsters **never take time off**: while most of us slow down during the holiday months, fraudsters just go up a gear.

When a fake message comes from someone the recipient knows (or thinks they know), as many as 30% click on a link. The more preliminary research the fraudster does and the more personal the content, the greater the chance that recipients will 'bite'.



Fragile on **mobile**: recipients are most susceptible to phishing when they open these messages on their mobile phones. People read emails and click on a link quicker on their smartphone. They are also often busy with other things such as watching a TV programme.

Thursday is phishing day: that's when you're most at risk of being phished.

Source: Whitepaper Phished

2020: A year expressed in fraud and scams

JANUARY – FEBRUARY

Bank card phishing by letter (send your cut-up bank card with your PIN code)

FROM MARCH ONWARDS

(Start of coronavirus payments by email, text message)

- Friend-in-need fraud on WhatsApp
- Safe deposit account fraud
- Fraud with CardStop, ITSME text message
- Phishing email from FPS Finance (tax refund, FPS Economy: apply for your coronavirus benefit here)

SEPTEMBER

- Safe deposit account fraud

OCTOBER

- Phishing Bpost package
- Smishing Card Stop text message

NOVEMBER

- WhatsApp fraud
- Phishing card reader update
- Black Friday and Cyber Monday: annual phishing party gets out of hand

DECEMBER

- Phishing Bpost package
- Smishing Card Stop text message
- Bank card phishing by letter (send your cut-up bank card with your PIN code)

More information on the above types of fraud can be found at **www.febelfin.be**

FRAUD AND SCAMS: THE BANKING SECTOR'S TOP PRIORITY IN 2021

In 2020, we witnessed a huge rise in all forms of online fraud, including phishing. In phishing, victims give their personal bank codes to fraudsters – usually by clicking on a link that leads to a fraudulent website – allowing the fraudsters to perform transactions in the victim's name. Our statistics show that around 67,000 fraudulent transactions occurred through phishing in 2020, totalling a net amount of roughly €34 million. Unfortunately, fraud does not stop when a new year is ushered in. All signs point to a continuation of this rising trend in 2021.

The findings of a recent study by Febelfin (March 2021) conducted with the research agency IndiVille1 are also cause for concern:

34% **of the population** received a **phishing message in the past month**. A total of 56% received such a message in the past six months. This shows the enormous scale of the problem. You have to be constantly alert to fraud.

Belgians are still **not adequately aware of the concept of phishing.** **12%** of the population has **never heard of phishing**.

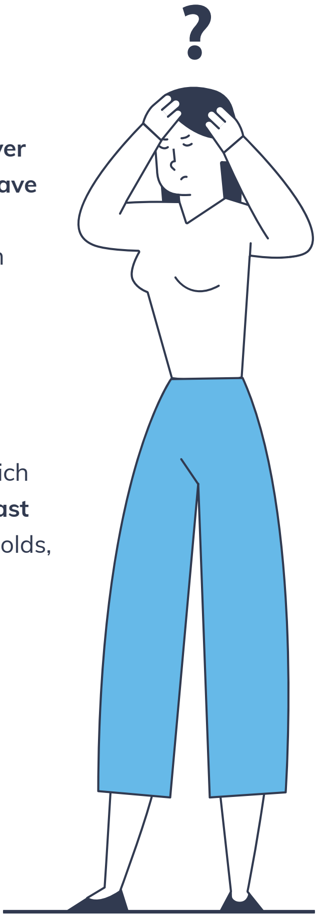
30% of **young people** (aged 16–30) have **never heard of phishing**.

26% **have shared financial data** and felt guilty about it. Last year this figure was 23%.

3% **of the population would pass on** their **bank codes if their bank asked them to.** The fact that 8% of young people would do this is not a good sign.

3% **of those who have ever received a phishing message have responded to it.** Young people are more vulnerable; 5% of them responded to the message.

7% of Belgians **shared financial information** about which they felt uncomfortable in the **past six months**. Among 16–30 year olds, this figure is a worrying 17%.



[1] Survey by Febelfin conducted with IndiVille among 2,045 respondents aged between 16 and 79 from 3 to 5 March 2021.

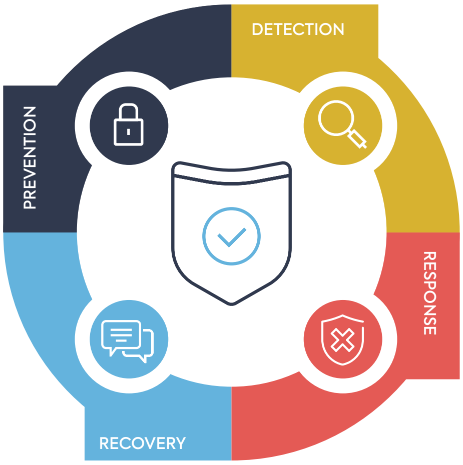
Figures from the most recent **Unisys Security Index™** also show that Belgians' concern about cybercrime has decreased. Now that is worrying! Concerns about internet security have decreased globally by 7 points (from 179 to 172 points) compared to last year. Belgium follows the general trend, but concern here drops much more steeply (from 160 to 141 points). Belgians are also less concerned about hacking and computer viruses, with only 44% compared to 54% last year.

These are reasons enough to assume that permanent campaigns and raising awareness in this regard are absolutely necessary among different target groups, especially **young people**. The assumption that young people are more digitally literate does not seem to be correct when it comes to knowing about the dangers of online fraud. **The banking sector thus considers the fight against fraud and scams a top priority in 2021** and will continue to focus on **awareness campaigns aimed at specific target groups** in **conjunction with the authorities and various stakeholders**.

HOW WILL BANKS COMBAT PHISHING?

Prevention:
- Authentication
- Raising client awareness

Recovery:
- Contacting the banks concerned
- And the traders



Detection:
- Proactive monitoring
- Early detection through a fraud hotline

Response:
- Blocking websites
- Fraud investigation
- Adapting logic/procedures for fraud detection
- Controlling false-positive rates

Authentication and detection

Banks have built in various systems to ensure transactions are secure and to prevent or contain phishing fraud as much as possible. For example, **two-step authentication** has been required for online and mobile banking for the past decade. Clients identify themselves with two elements – a card or telephone, a PIN code, a fingerprint or a face scan – to initiate e-payments. The Belgian banking sector led the way in this regard. The use of new biometric techniques is something to look out for in the near future.

Banks also invest in intensive monitoring and reverse a lot of the damage in this way. These efforts yield remarkable results: the banks detect and either block or recover more than 75% of all fraudulent transfers that have used a phished response code. Some banks are already using artificial intelligence to detect fraud.

Delicate balance between ease of use and security

Guaranteeing **smooth and fast payment transactions and efficient fraud detection is a difficult and delicate balance**. It requires **continuous investment in personnel and infrastructure** from the banking sector. But the **client expects ease of use and fast payments** too (such as instant payments with the money in the recipient's account within seconds). A bank needs time to investigate thoroughly if an anomaly is detected. Each fraud team has its own rules and procedures for this purpose. Reconciling security and ease of use thus poses challenges for the sector: a real balancing game.

> **“ 33% of Belgians find the security steps (such as entering a card number, having a card reader at hand) when purchasing online unnecessary and experience this more as a hindrance. This attitude is concerning because these steps are built in precisely to protect the consumer”, explains Karel Baert, CEO Febelfin.**

Keep repeating

There is also a strong focus on raising awareness through campaigns, with the sector calling on everyone to be vigilant against phishing and online fraud. Campaigns with tips, both on social media and on TV and radio, have reached a large target audience. But as the number of fraud cases show, there is still work to be done. Awareness campaigns therefore remain necessary. Let's jointly repeat the vital message never to share your personal codes (PIN and response code) as much as possible.

1 MESSAGE: NEVER GIVE YOUR CODES TO ANYONE AND DO NOT CLICK ON A LINK

The coronavirus crisis and many digital contacts are an opportunity for fraudsters to scam people. The different forms of phishing are numerous and complex. Fraudsters not only use different channels – such as email, letter, phone, text message (SMS), social media and WhatsApp – but also commit the fraud in the name of different organisations and institutions such as banks, public administrations, telecommunication operators, utility companies and so on. The list is long. Because of the wide variety of channels, **everyone is a potential victim**.

While the ingenuity of fraudsters might be impressive, phishing is still **easy to prevent**:

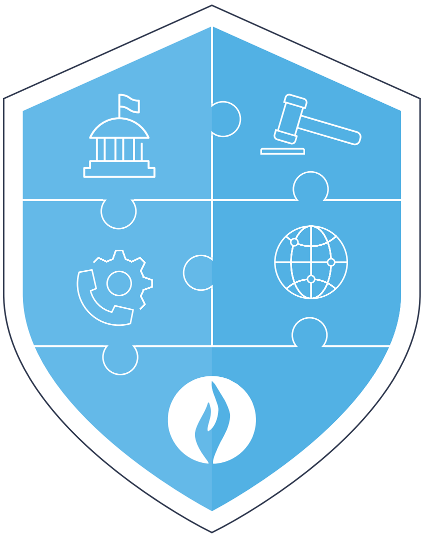
Never provide your personal codes (PIN and response code) in reply to an email, phone call, text message, social media or WhatsApp message.

Also never click on any link you receive. Instead, always type the address of the desired bank website in your browser or use your mobile banking app. Only then can you be sure that nothing is wrong.

To summarise: digital payment and banking is and remains secure, as long as you keep your personal codes to yourself and remain vigilant. After all, you wouldn't just hand over your wallet, would you?

New initiatives

It is crucial to be able to intervene quickly because money is often channelled from one bank account to another in a short space of time through money mules. The 'mule stop process' was thus introduced in mid-2020 so that the victim's bank can efficiently request the mule's bank to block the transferred fraud amount.



Given the nature of the problem, this is tackled not only by technical working groups with financial experts exchanging information to detect as much fraud as possible, but the sector is also working on partnerships with other stakeholders. These partnerships include ongoing initiatives with telecommunications operators, internet service providers, the public prosecutor's office, the police, government agencies and the judiciary to tackle phishing in all scales and forms and to spread the awareness message as widely as possible. They must be even more structured and automated in future. This will contribute greatly to how quickly fraud can be detected and prevented.

The enormous willingness of the banking sector to tackle fraud is an established fact.

It is not yet possible to exchange personal data about fraud because of privacy and other legislation. Banks remain very cautious in this area because they are bound by extremely strict regulations through supervisory authorities and legislation.

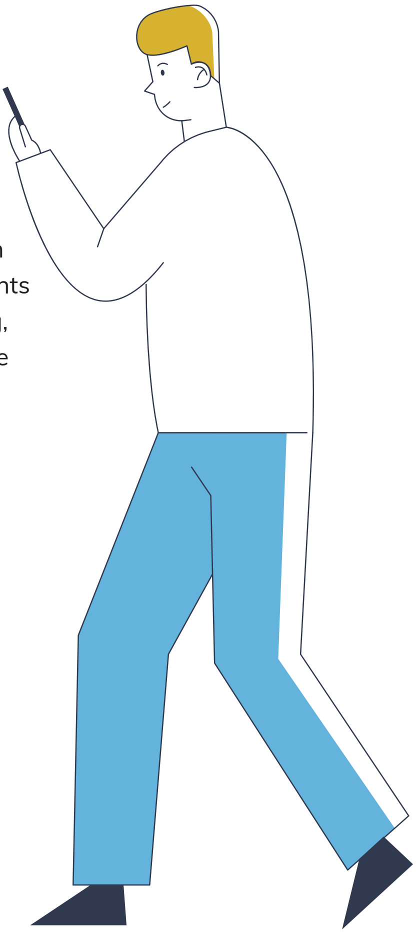
Febelfin is investigating the possibility of establishing a system for exchanging the identity data of money mules between financial institutions on a statutory basis.

Can science provide a solution?

Why do people keep clicking on links or falling for other forms of fraud? According to behavioural science, this is because our brain switches to fast thinking at that moment and we no longer think rationally. Fraudsters cleverly exploit some of the mechanisms that occur then:

- **Loss aversion:** fear of losing out
- **Social influence:** change in attitude or behaviour caused by external pressure, real or perceived
- **Unrealistic optimism:** we always think phishing will never happen to us
- **Discounting:** people are always eager to receive large discounts or limited editions
- **Availability heuristic:** type of shortcut with direct examples in our memory

But the same mechanisms can be used to develop behavioural techniques that subtly encourage people to behave in a certain way, also known as nudging. Although few scientific experiments have been developed to date using nudging to reduce phishing, the first steps are being taken in this direction in the UK and the Netherlands. Febelfin is monitoring this closely and is keen to investigate it further.



febelfin academy

Always stay focused

Febelfin Academy, our in-house academy, has developed a broad range of training courses for all ‘target groups’ within the financial institution – from commercial assistants to product experts to directors. This ensures that everyone in the sector stays focused. Febelfin Academy cooperates closely in this regard with both the business world (experts from financial institutions) and international lecturers and organisations (such as the IMF).

Here is a selection of the courses on offer:

- General awareness of all employees of financial institutions: e-learning based on concrete situations with exercises and simulations, both private and professional.

  Cyber security: Do’s & Don’ts (EN) – e-learning

- Training of experts in fraud/cyber: advanced training with certification

  Business and digital transformation skills (The Master Channel) – online courses

  Certified Fraud Examiner (CFE) course – in cooperation with the IMF

- Training for product managers in relation to payments: PSD2 and SCA

  PSD2 & Open banking: impact on the financial ecosystem and new challenges

- Risk management: cyber security is clearly one of the main new risks for our members and features prominently in risk management courses – especially now in coronavirus times – with risk and compliance managers as its target group.

  COVID-19: New challenges in Risk Management – Live Webinar

  Masterclass in Risk Management

- Board effectiveness: executive programme for board members focusing on cyber risks and how to deal with them as a board member – what questions to ask to guard against cyber risks.

  Executive program – The Board of Directors in the Financial Sector

A LARGE FISHING NET IS NEEDED

But the banking sector is reaching the **limits** of what it can do alone. In recent years, we have seen the largest catalysts for fraud move outside the banking sector to other sectors – a trend that has only increased because of the COVID-19 pandemic. Criminals are increasingly bypassing banks' sophisticated security systems.
Even so, we must also ensure that this fraud is stopped.

Phishing is not only a banking-sector problem, but also a **social phenomenon**. We are at a tipping point. **All sectors** must jointly assume **responsibility** in this battle, including telecommunications and online trading platforms. Only together can we try to stop fraud as much as possible. There is still much room for far-reaching cooperation, not only sectoral but also cross-border.

The links between fraud, organised crime and terrorism are a major and growing threat to national security. The criminal gangs involved use the proceeds of fraud to finance other harmful and illegal activities, causing untold suffering and damage to our society. It is therefore crucial for the government to assume responsibility for this issue and look at how to create an appropriate legislative framework. Sufficient resources and capacity must also be made available so police forces can do their job and shut down these criminal gangs at the top.

Everyone is involved in the fight against cyber fraud. Secure payments are a shared responsibility: the banking sector ensures a secure digital infrastructure, the client is informed and alert, the police and the public prosecution service prosecute the crime, and the government provides the right statutory framework. If we can maintain this balance, the damage can be limited. **Only together can we win this battle, because each incident is one too many.**

febelfin

Belgian Financial Sector Federation

www.febelfin.be