febelfin

Phishing & andere kapers op de kust

Online fraude blijft alomtegenwoordig. Ook in 2023 bleven cybercriminelen massaal phishingberichten uitsturen en zich voordoen als een naaste of een vertrouwde organisatie, zoals een bank of overheidsdienst. In 2023 werden 75% van alle frauduleuze overschrijvingen naar aanleiding van phishing door de banksector geblokkeerd of teruggevorderd. Ondanks deze inspanningen kon toch 40 miljoen euro[1] buit gemaakt worden door middel van phishing.

Bijkomend zien we dat andere online fraudevormen waarbij de klant gemanipuleerd wordt om zelf een frauduleuze betaling te doen, sterk blijven toenemen, denk maar aan beleggingsfraude of bankhelpdeskfraude.[2] Alarmerend is dat de bevolking over het algemeen nog onvoldoende op de hoogte is van deze nieuwe fraudevormen.

Gelukkig is er ook goed nieuws. Ondanks de vele pogingen en geslaagde gevallen van online fraude, zien we een positieve evolutie wat betreft de acties die worden ondernomen bij vermoeden van online fraude. In 2023 ondernam 91% van de potentiële slachtoffers actie bij een dergelijk vermoeden. Er valt ook een daling op te merken in het aantal personen dat pincodes deelt en zijn/haar bankkaart opstuurt naar een welbepaald adres. De bevolking is bovendien ook beter op de hoogte van het fenomeen geldezels.

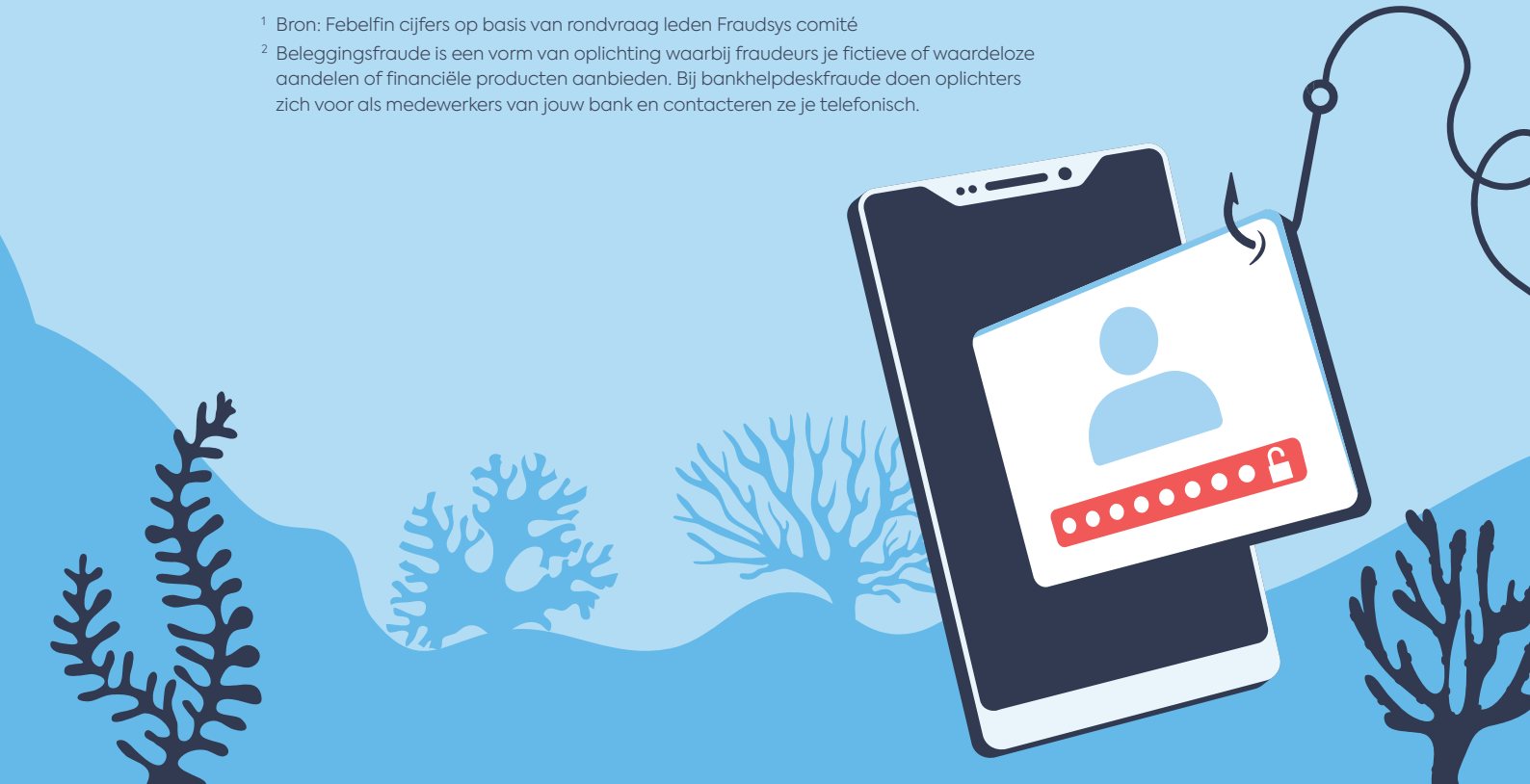
Al deze bevindingen tonen aan dat we blijvend moeten inzetten op permanente sensibilisering. Iedereen kan het doelwit worden van online fraude. We zien dat vooral jongeren steeds vaker in het vizier komen van de fraudeurs door hun laksere houding als het gaat om online veiligheid.

Daarom blijven we als sector inzetten op nieuwe initiatieven en partnerschappen om samen de strijd aan te gaan tegen online fraude.

Hoe is het gesteld met de kennis van de bevolking ten opzichte van online fraude? Welke fraudevormen zijn actueel, hoe 'veilig' gedragen we ons bij online aankopen en geven we nog altijd zo gemakkelijk onze codes door? Welke inspanningen deed de sector en wat zijn onze prioriteiten voor de toekomst? Lees er alles over in deze storytelling met de meest recente cijfers.

[1] Bron: Febelfin cijfers op basis van rondvraag leden Fraudsys comité

[2] Beleggingsfraude is een vorm van oplichting waarbij fraudeurs je fictieve of waardeloze aandelen of financiële producten aanbieden. Bij bankhelpdeskfraude doen oplichters zich voor als medewerkers van jouw bank en contacteren ze je telefonisch.



HET ‘PHISHNET’ BLIJFT GROOT

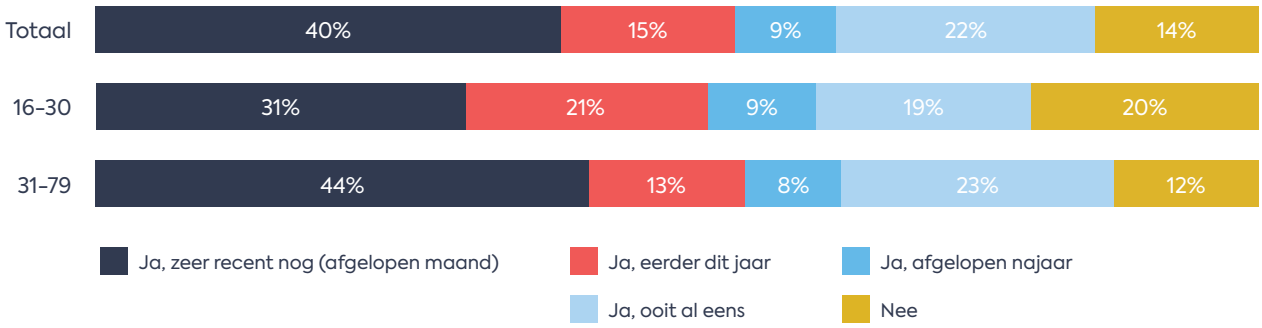
€ 40 miljoen buit in 2023

Ondanks alle sensibiliseringsinitiatieven blijft phishing een populaire fraudetechniek voor cybercriminelen.

Hoewel 75% van frauduleuze overschrijvingen naar aanleiding van phishing werden geblokkeerd of teruggevorderd door de banken, kon men in 2023 (net zoals in het voorgaande jaar) ongeveer 40 miljoen euro[3] buit maken door phishing.

Een recent onderzoek van Febelfin in samenwerking met onderzoeksbureau Indiville[4] bevestigt hoe omvangrijk phishingpogingen blijven. Meer bepaald ontving 55% van de bevolking dit jaar al minstens 1 phishingbericht en in 40% van de gevallen gebeurde dit heel recent. Deze cijfers zijn vergelijkbaar met die van vorig jaar.

Heb je al eens een phishingbericht ontvangen? Wanneer gebeurde dit voor het laatst?



Bron: Indiville

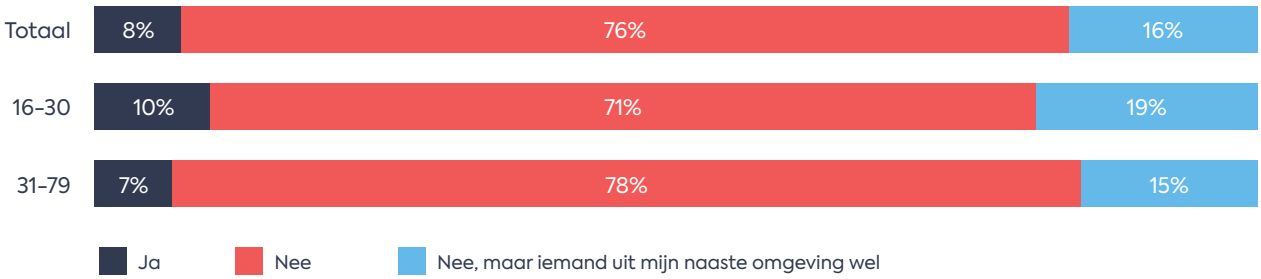
Cybercriminelen blijven dus massaal veel phishingberichten uitsturen. In 2023 werden er bijna 10 miljoen berichten door particulieren doorgestuurd naar het meldingspunt verdacht@safeonweb.be. In 2022 waren dat er 6 miljoen. Dagelijks worden er gemiddeld 27.000 berichten doorgestuurd.

Uit het onderzoek blijkt dat 8% ooit slachtoffer werd van phishing. Jongeren zijn kwetsbaarder (10%). Ook kennen ze vaker iemand die al slachtoffer is geworden (19%, 2022: 15%).

[3] Bron: cijfers Febelfin op basis van rondvraag leden Fraudsys comité

[4] IndiVille onderzoek, 1 – 18 maart 2024, op een representatief staal van de Belgische bevolking n: 2109 NL/FR enquêtes, leeftijd 16-79. Maximale foutenmarge: 2,1%

Ben je al slachtoffer geworden van phishing?



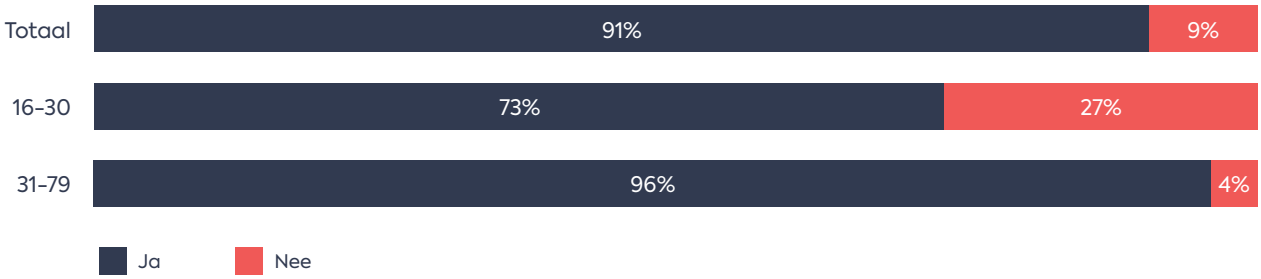
Bron: Indiville

Kennis over phishing moet beter

Over het algemeen heeft 9% van de Belgische bevolking nog nooit gehoord van phishing. De oudere leeftijdsgroep is iets beter op de hoogte van deze fraudevorm en van hen heeft slechts 4% er nog nooit van gehoord.

Bij de jongeren is echter bijna één derde niet bekend met de term 'phishing'. Dit is een minder goed resultaat dan een jaar geleden, en bijzonder verontrustend.

Heb je ooit al gehoord van phishing?



Bron: Indiville

Dit cijfer toont aan dat het cruciaal is om jongeren te blijven informeren en waakzaam te maken voor phishing. Zij vormen namelijk nog steeds een belangrijk doelwit voor cybercriminelen. Febelfin stelt dan ook alles in het werk om haar communicatie aan te passen aan deze doelgroep. Zo lanceerden we in november 2023 in samenwerking met Safeonweb en de Cyber Security Coalition de phishing campagne 't zit hem in de details'. Daarenboven werd de mobiele escape game, The Hacker Hotline, in het leven geroepen waarmee Febelfin wekelijks het hele land doorkruist om jongeren te informeren.

Het maakt hen op een ludieke manier bewust voor de gevaren van online fraude en leert hen hoe ze zichzelf kunnen wapenen tegen deze fraudevorm.

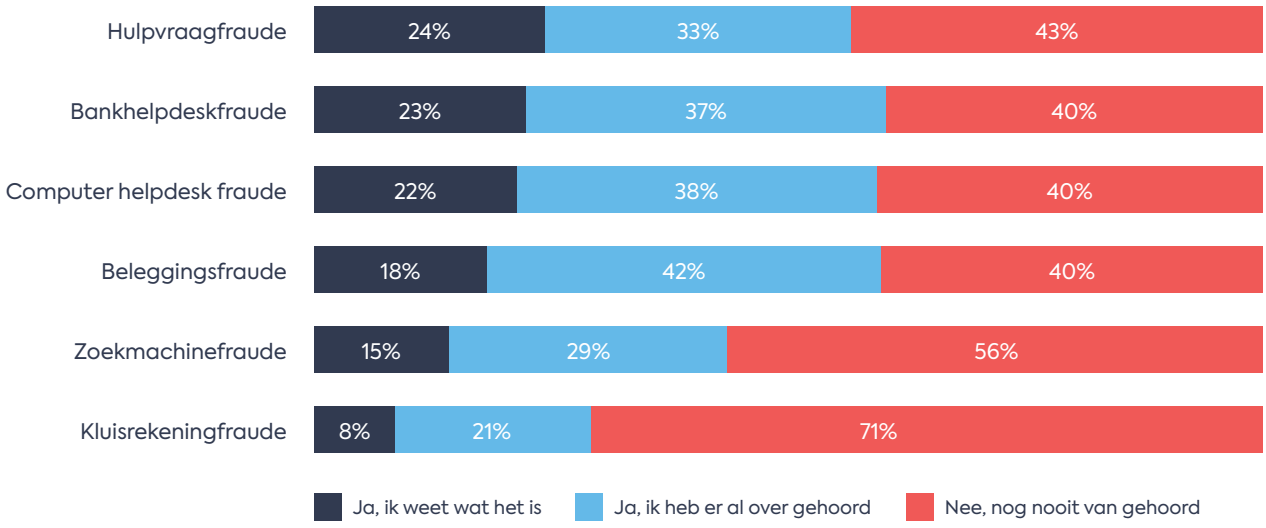
ANDERE KAPERS OP DE KUST

Andere vormen van online fraude zijn in opmars

Online fraudevormen waarbij het slachtoffer zelf een overschrijving uitvoert op aangeven van de cybercrimineel zijn verder gestegen. Het gaat hierbij onder meer over factuurfraude, CEO-fraude, vriendschapsfraude, hulpvraagfraude, bank- en computer helpdesk fraude, beleggingsfraude en kluisrekeningfraude. Deze zijn over het algemeen weinig tot onbekend bij de Belgen.

Zo weet gemiddeld gezien slechts iets minder dan 1 op de 5 Belgen wat de fraudevormen inhouden, heeft 33% er al eens over gehoord, maar tast bijna de helft van de bevolking volledig in het duister. Jongeren lijken gemiddeld iets beter op de hoogte te zijn van deze vormen van fraude dan de andere leeftijdsgroep (17% versus 21%). Maar in beide groepen blijft dit aandeel laag.

Weet je wat deze vormen van fraude zijn?



Bron: Indiville

De financiële sector blijft hierover dan ook communiceren en initiatieven ontwikkelen om te waarschuwen voor deze types van fraude.

TIP

Zie je ook het bos door de bomen niet meer, neem dan een kijkje in het **online dossier** op de Febelfin website en ontdek verschillende types van online fraude.

Meer meldingen van bankhelpdeskfraude en computer helpdesk fraude

In het afgelopen jaar werden er meer gevallen van bankhelpdeskfraude en computer helpdesk fraude gemeld.

WAT IS COMPUTER HELPDESK FRAUDE?

Bij **computer helpdesk fraude** doen oplichters zich voor als helpdesk medewerkers van een computerfirma en bellen ze je op. Ze vragen je om je computer aan te zetten en hun instructies op te volgen. Want er zou een probleem zijn met je computer. Niets is minder waar: in werkelijkheid hacken ze je en nemen ze je computer over, om hierna je rekeningen te plunderen.

WAT IS BANKHELPDESK-FRAUDE?

Bankhelpdeskfraude is gelijkaardig aan computer helpdesk fraude, maar oplichters doen zich voor als medewerkers van jouw bank en bellen je op met de vraag om jouw computerscherm te delen en persoonlijke codes door te geven, omdat er zogezegd verdachte transacties werden gevonden op jouw bankrekening. Zo slagen ze erin overschrijvingen uit te voeren met jouw rekening en heel wat geld te ontfutselen.

Febelfin publiceert in dat kader verschillende **persberichten** met de oproep om op je hoede te zijn wanneer je wordt gecontacteerd met de vraag om je computerscherm te delen, persoonlijke codes door te geven en online verrichtingen uit te voeren.

Een bankmedewerker of een helpdesk medewerker van een computerfirma zal je nooit vragen naar jouw persoonlijke codes en je daarenboven aanzetten om software te installeren waarmee hij/zij jouw computer vanop afstand kan overnemen.

Let op voor Card Stop-fraude via telefoon

Een ander type van fraude waar we in 2023 en recent meermaals voor waarschuwden is Card Stop-fraude. Hoe werkt het? Mensen worden opgebeld door een gsm-nummer. De stem aan de andere kant van de lijn beweert een medewerker van Card Stop te zijn en informeert dat er verdachte transacties zijn gedetecteerd op een bankrekening. In realiteit gaat het hier om een frauduleuze oproep die niet van Card Stop komt maar van oplichters. Samen met Worldline, herinnerde Febelfin consumenten eraan dat ze best nooit bankcodes delen via sms, e-mail, sociale media of telefoon.

WIST-JE-DATJE

In de sector noemt men deze handelswijze ook vaak gerobotiseerde phonescamming: d.w.z. een robotstem belt massaal veel nummers en vraagt aan de persoon aan de lijn om op een toets te drukken wanneer ze verder geholpen willen worden. Daarna neemt een menselijke operator over die weet dat het potentieel slachtoffer zich al heeft laten misleiden door de gerobotiseerde manipulatie en er dus meer kans is dat men in de val zal trappen, na de menselijke manipulatie.

Hulp aan huis voor bankzaken resulteert meestal in oplichting

Een nieuwe manier van oplichting die we de afgelopen maanden zagen ontstaan zijn “medewerkers van de fraudedienst van een bank”, “medewerkers van Card Stop” of “politie” die telefonisch contact opnemen met ouderen om hen te melden dat er fraude werd vastgesteld op hun rekening. Deze fraudeurs stellen dan voor om bij het slachtoffer thuis langs te gaan om de situatie zogezegd op te lossen. Hierbij hebben ze jammer genoeg maar één doel voor ogen: zo veel mogelijk stelen (bankkaart, cash, juwelen, ...).

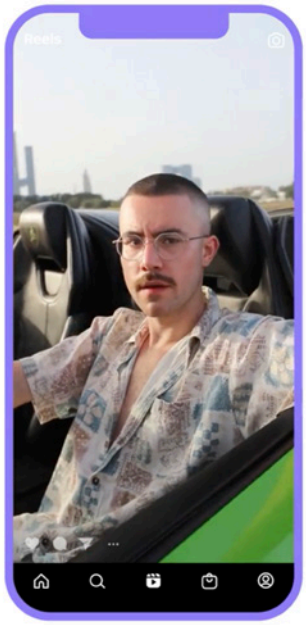
Aangezien senioren uiteraard een kwetsbaar doelwit zijn en we deze gevallen maximaal willen vermijden, communiceerden we hierover samen met de Federale Politie en de FOD Binnenlandse Zaken.

Beleggingsfraude piekt

Beleggingsfraude is in opmars. In 2023 slaagden fraudeurs erin om minstens zo'n 15,48 miljoen (Bron: FSMA) afhandig te maken door middel van beleggingsfraude. Hoewel beleggers iets beter op de hoogte zijn van beleggingsfraude, blijft het over het algemeen een weinig gekende fraudevorm bij de Belg.

In maart 2024 lanceerde Febelfin daarom een campagne over beleggingsfraude in samenwerking met bekende influencer Jonatan Medart met als titel 'Volg je held niet met geld!'.

Vanuit een luxejacht riep hij zijn volgers op om zijn financieel advies te volgen en zich aan te sluiten bij zijn besloten Telegramgroep om naar eigen zeggen 'snel rijk te worden'. Op het einde werd duidelijk dat dit één grote leugen was en maakte Jonatan zijn volgers erop attent dat ze alert moeten blijven voor beleggingsfraude door valse finfluencers op sociale media. Op die manier bereikte Febelfin heel veel jongeren met de essentiële boodschap 'Volg je held niet met geld!'.



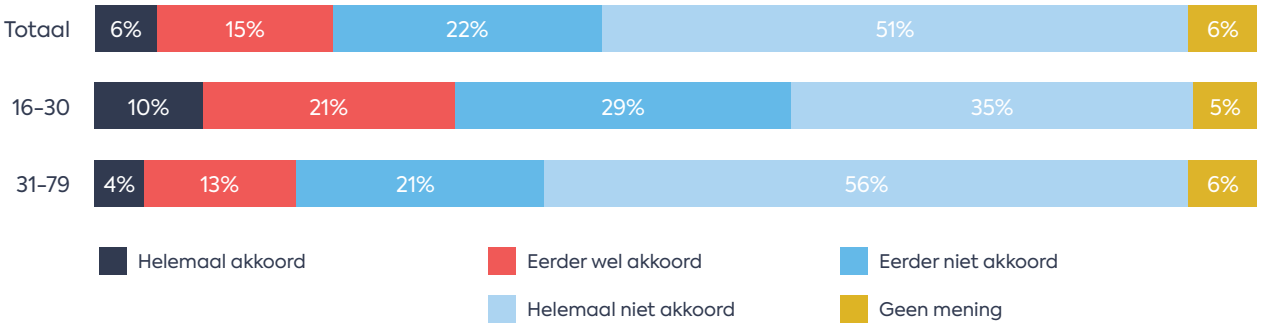
Enkele tips om beleggingsfraude te vermijden:

- **Controleer altijd de identiteit van de aanbieder:** naam, maatschappelijke zetel, vestigingsland, contactgegevens,...
- **Vertrouw nooit een aanbieder die je niet duidelijk kan identificeren.** Als de onderneming buiten de EU is gevestigd, weet dan dat er moeilijkheden kunnen ontstaan wanneer je in een conflictsituatie terechtkomt en gerechtelijke stappen wilt ondernemen.
- **Wees op je hoede voor 'cold calling':** Neemt iemand online of telefonisch contact met je op met een financieel aanbod zonder dat je daar vooraf om hebt gevraagd? Dat is vaak een frauduleuze praktijk.
- **Kijk uit als je contactpersoon je vraagt om geld over te maken** naar een bankrekening in een ander land dan waar de aanbieder gevestigd is.
- Als de **aanbieder een bijkomende betaling** vraagt, is dat vaak een teken van fraude.
- Kortom, als het te mooi is om waar te zijn is het meestal zo.

Hoe staan we tegenover veiligheid bij online aankopen?

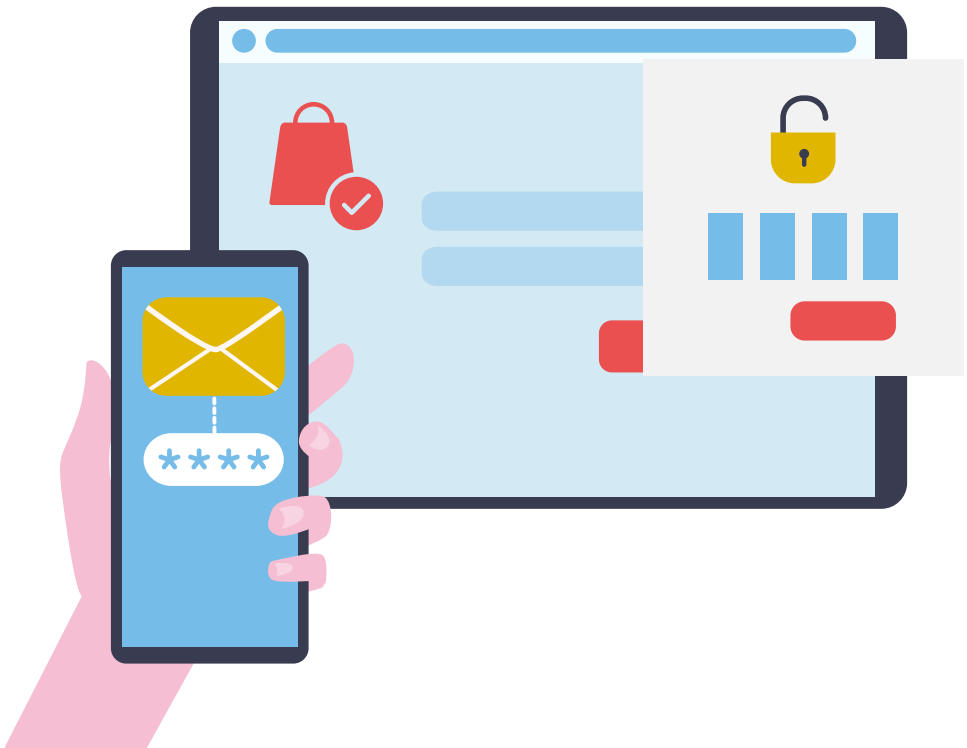
De meerderheid van de Belgen vindt de verschillende veiligheidsstappen (tweestaps-verificatie of het bevestigen van je identiteit door middel van meerdere stappen) bij online aankopen, zoals bijvoorbeeld de responscodes van de kaartlezer of je itsme code ingeven gelukkig niet overbodig. Dit is opnieuw een verbetering, net zoals vorig jaar. Een goede zaak.

Ik vind het overbodig om verschillende stappen te moeten doorlopen bij online aankopen



Bron: Indiville

Toch vormen deze veiligheidsstappen voor 1 op de 5 Belgen eerder nog een obstakel dan een bescherming. Bij jongeren is de groep die deze stappen als hinderlijker ervaren iets groter (31%). Het is en blijft daarom belangrijk volop in te zetten op het beter informeren van jongeren hieromtrent en hun kijk op online veiligheidsstappen te veranderen. We moeten er namelijk voor zorgen dat deze als de noodzakelijke bescherming tegen online risico's worden gezien, in plaats van als een hindernis.

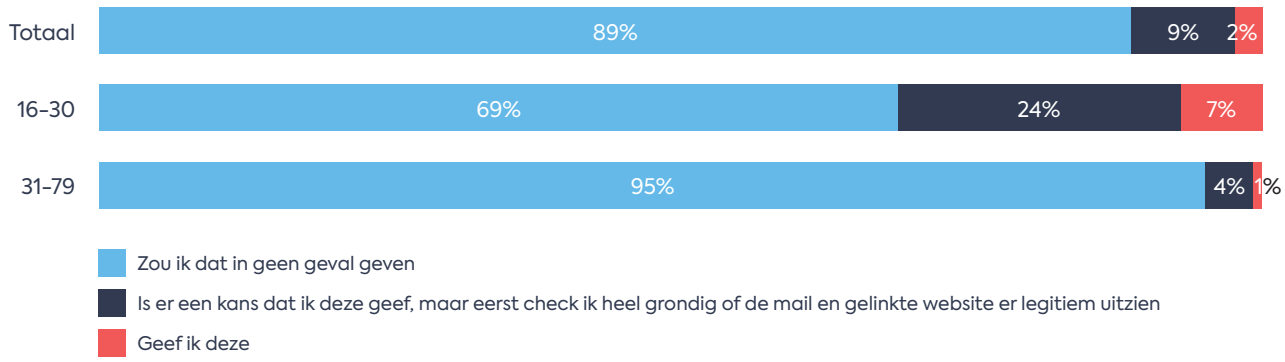


Minder mensen geven codes door of sturen bankkaart op!

Toch valt er ook goed nieuws te melden. We doen het met z'n allen beter wat betreft het niet doorgeven van bankcodes en het niet terugsturen van bankkaarten. 89% van de Belgen zou in geen enkel geval hun codes doorgeven aan de bank.

Maar 2% van de bevolking, en 7% van de jongeren, zou wel zonder aarzelen zijn/haar bankcode geven als de bank daarom zou vragen. Dit blijft te veel, maar is voor het tweede jaar op rij een verbetering (2023: 10%, 2022: 13%).

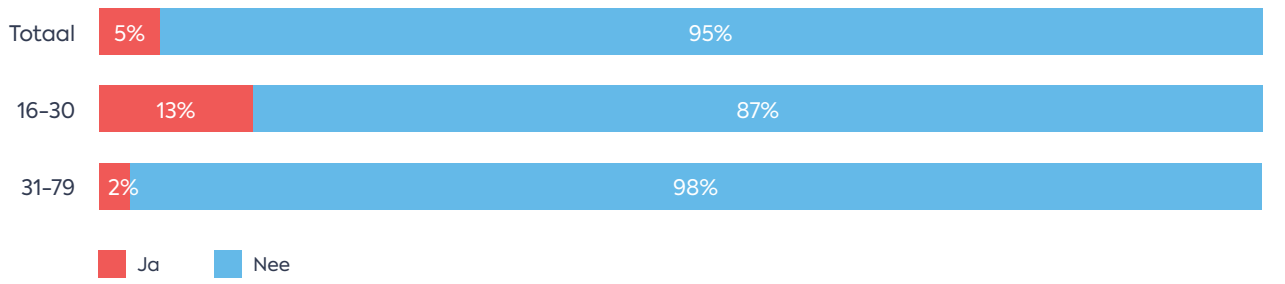
Als je bank via e-mail, sms, whatsapp, telefoon, ... naar mijn bankcodes vraagt ...



Bron: Indiville

95% van de Belgen zou in geen enkel geval hun bankkaart terugsturen naar de bank. Jongeren doen het ook hier iets minder goed dan de rest van de bevolking. 13% zou de kaart terugsturen als de bank hierom vraagt, maar ook hier is dit beter dan vorig jaar (2023: 17%).

Zou je je bankkaart terugsturen als je bank via e-mail, sms, whatsapp, telefoon, brief, ... hierom vraagt?

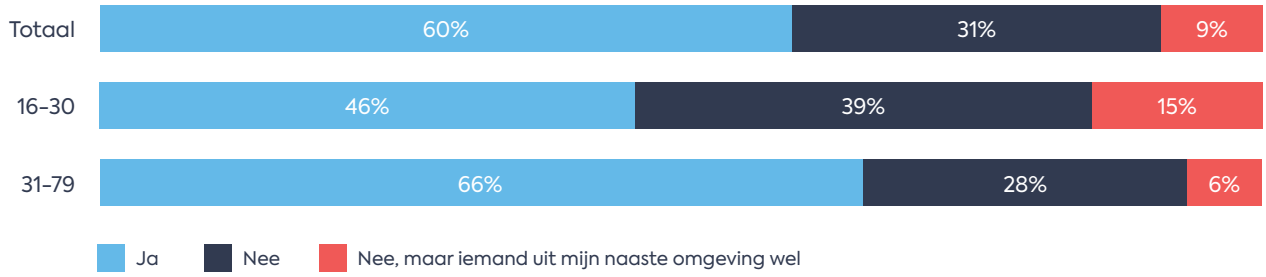


Bron: Indiville

Er wordt ook vaker actie ondernomen bij vermoeden van online fraude

We zien een positieve evolutie wat betreft de acties die worden ondernomen bij vermoeden van fraude. 6 op de 10 slachtoffers van phishing wisten wat ze moesten doen en 91% ondernam actie bij vermoeden van (pogingen tot) online fraude, zoals het controleren van hun rekening of contact opnemen met Card Stop.

Wist je welke stappen je moest ondernemen of waar je terecht kon voor hulp?



Bron: Indiville

53% controleerde aandachtig zijn/haar rekeningen, 30% belde naar de bank en 26% naar Card Stop. Hoewel jongeren gemiddeld gezien minder goed op de hoogte zijn van wat ze het best kunnen doen bij vermoeden van fraude, hebben ze nu wel vaker de reflex om hun rekeningen te controleren dan in de voorgaande jaren (2024: 51%, 2023: 44%, 2022:34%). Dit is dus een stap in de goede richting.

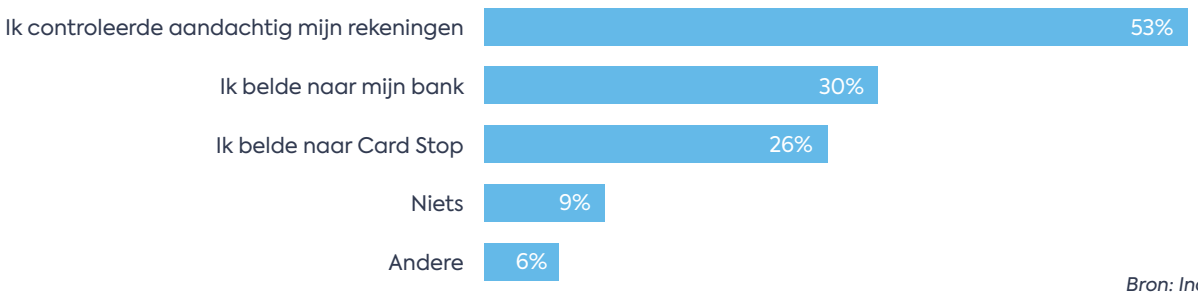
KEN JE HET NUMMER VAN CARD STOP?

Je kunt Card Stop bereiken via het nummer **078 170 170** als je jouw betaalkaart wilt blokkeren na diefstal, verlies of poging tot fraude.

BEN JE SLACHTOFFER VAN ONLINE FRAUDE?

Neem ook contact op met jouw bank. Banken hebben speciale fraudeafdelingen die 24/7 bereikbaar zijn. Je vindt alle contactgegevens op **de website van Card Stop**.

Wat deed je met dit gevoel?



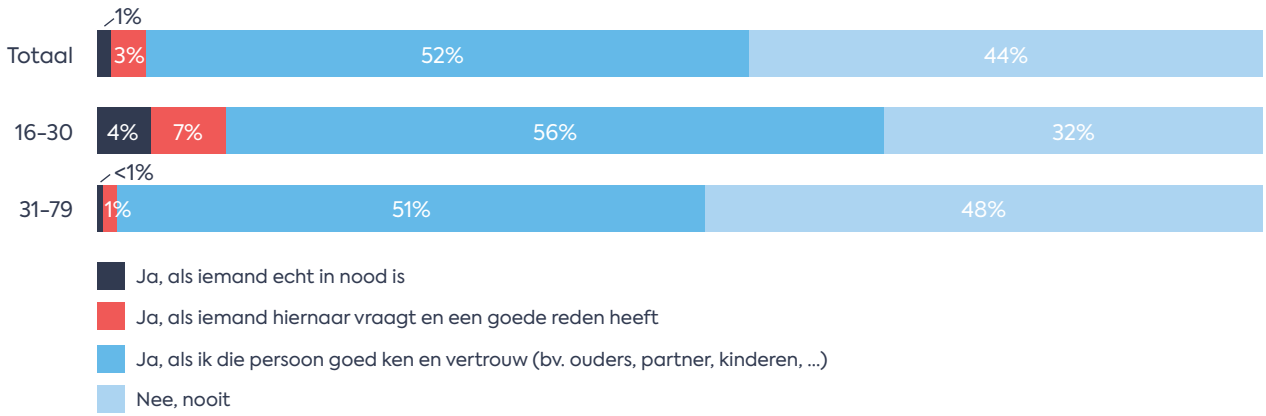
Bron: Indiville

Problematiek van ‘geldezels’ nog te weinig gekend

Iemand die je benadert met de vraag of je snel en makkelijk geld wilt verdienen door je bankrekening en/of bankkaart even uit te lenen? Vooral voor jongeren blijft de verleiding groot.

4% van de Belgische bevolking zou zijn/haar bankkaart en pincode doorgeven aan iemand die ze niet kennen, in ruil voor geld. 11% van de jongeren zou dit doen, wat een verbetering is ten opzichte van vorig jaar, maar uiteraard nog steeds te hoog ligt.

Zou jij je bankkaart en pincode afgeven aan iemand anders?



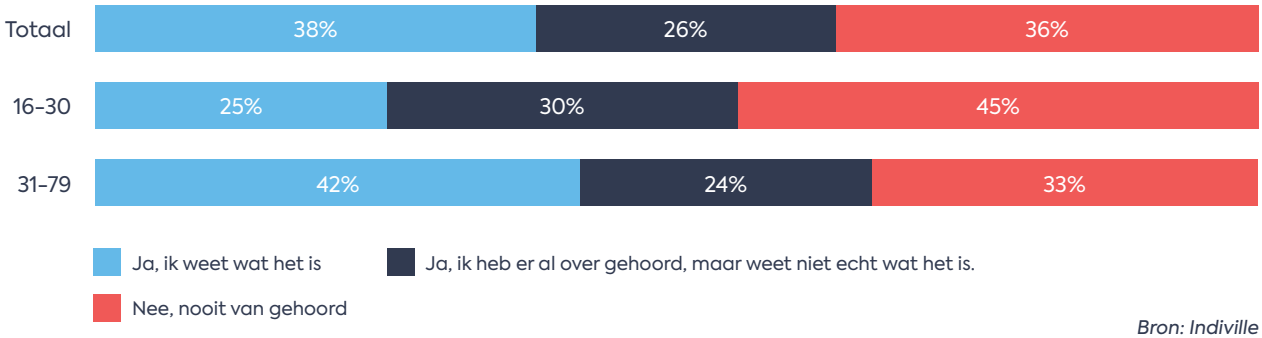
Bron: Indiville

WAT IS EEN GELDEZEL?

Een geldezel is iemand die zijn bankrekening en/of bankkaart en pincode laat gebruiken door criminelen om crimineel geld wit te wassen. Daardoor kan de crimineel misdaadgeld op de bankrekening van de geldezel storten om het vervolgens af te halen (met de bankkaart en de pincode van de geldezel) of door te storten naar andere rekeningen. Zo blijven de oplichters buiten schot. Lees er meer over in ons **online dossier**.

Bijna 40% van de Belgen weet wat een geldezel is, maar bij de jongeren bedraagt dit aandeel slechts 25%. 45% van de jongeren hebben zelfs nog nooit van het fenomeen gehoord.

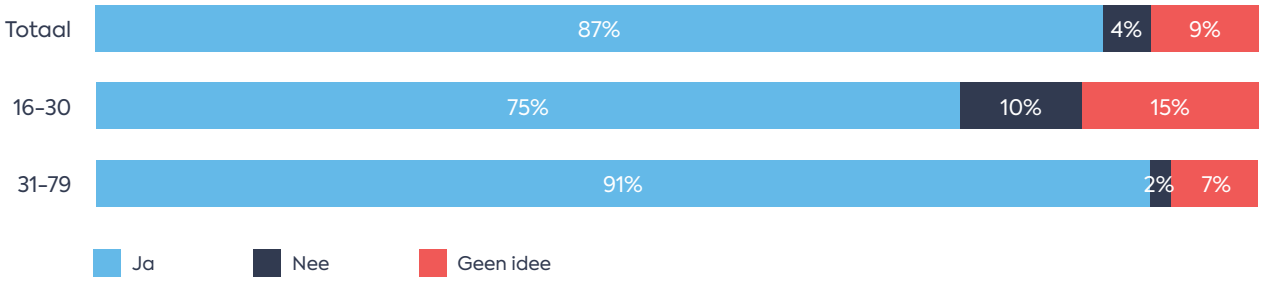
Weet jij wat een geldezel is?



Bron: Indiville

Jongeren weten in vele gevallen ook niet dat het strafbaar is om als geldezel dienst te doen. Nochtans zijn de gevolgen groot, gaande van celstraffen, geldboetes tot terugbetaling van het slachtoffer, ...

Denk je dat je als geldezel strafbaar bent?



Bron: Indiville

Daarnaast zegt 3% ooit benaderd te zijn geweest door een fraudeur met de vraag om geldezel te worden en kent 5% mensen die deze vraag kregen. Ook dit percentage ligt hoger bij jongeren: 6% werd zelf al benaderd en nog 12% kent iemand anders die dit overkwam.

Ben je ooit zelf al benaderd geweest om geldezel te worden?

Het blijft dus essentieel om het fenomeen 'geldezels' uit te leggen, zeker aan jongeren, en mensen bewust te maken voor de risico's en strafbaarheid die ermee gepaard gaan. Zij zijn immers een belangrijk doelwit voor dit type fraude.

DE FINANCIËLE SECTOR ONTWIKKELT STEEDS NIEUWE INITIATIEVEN IN DE STRIJD TEGEN ONLINE FRAUDE

E-learning voor digitale begeleiders

In 2023 lanceerde Febelfin een nieuwe e-learning voor zij die mensen begeleiden bij hun eerste stappen in de digitale wereld. Deze digicoaches bieden we via de e-learning de nodige tips & tricks en handige tools om minder digitaalvaardige consumenten te helpen. Er wordt daarbij speciale aandacht besteed aan online veiligheid en de uitleg van de verschillende online fraudevormen.

De e-learning is een groot succes: tot nu toe volgden bijna 400 vrijwilligers en professionelen de e-learning. Dit succes maakt nogmaals de relevantie van sensibilisering en opleiding duidelijk bij verschillende doelgroepen en stakeholders.

IBAN-naamcontrole

Daarenboven stelt de sector alles in het werk om de invoering van de **IBAN-naamcontrole** mogelijk te maken. Dit is een hulpmiddel om bepaalde vormen van fraude met overschrijvingen, zoals factuurfraude, tegen te gaan. Tijdens de invoering van een overschrijvingsopdracht controleert de bank van de opdrachtgever namelijk bij de bank van de begunstigde of het rekeningnummer (IBAN) en de naam van de begunstigde overeenstemmen. Indien dit niet het geval is, zal de bank dit d.m.v. de IBAN-naamcontrole aan de klant melden, als waarschuwing voor fraude of oplichting. De banken stellen dan ook alles in het werk om de invoering hiervan mogelijk te maken.

Het incidentenwaarschuwings-systeem

Het **incidentenwaarschuwingssysteem** is een project waarbij banken informatie over incidenten in het kader van betalingen zouden kunnen uitwisselen om klanten nog beter te beschermen tegen verdachte incidenten.
De identificatie van verdachte handelingen zou kunnen worden gedeeld onder de banken zodat ze kunnen rekening houden met de geïdentificeerde risico's.
Het delen van zulke informatie zal conform de persoonsgegevensbeschermingswet gebeuren.

De financiële sector pleit voor de verwezenlijking van dit project dat zal bijdragen aan een nog effectievere bestrijding van online incidenten en de problematiek van geldezels.

Workshops en infosessies op maat voor verschillende doelgroepen

Om de bewustmaking van jongeren, als belangrijk en kwetsbaar doelwit voor cybercriminelen, verder te vergroten werkten we het afgelopen jaar ook verder aan onze samenwerking met scholen, jongerenorganisaties alsook lokale partners.

Onze mobiele escape game, The Hacker Hotline, doorkruist wekelijks het hele land om jongeren op een leuke en laagdrempelige manier te waarschuwen voor de risico's van online fraude en tips mee te geven om niet in de val te lopen.

Ook onze infosessies over online fraudevormen, met een speciale focus op de fraudevorm 'geldezels', worden verdergezet. Febelfin werkte mee aan de 'Veiligheidsdag', georganiseerd door de politie en brandweer in Knokke-Heist. Daar boden we de verschillende lokale middelbare scholen, met meer dan 1.000 leerlingen, workshops aan over online fraude en geldezels.

Aangezien we de verschillende kwetsbare bevolkingsgroepen zo veel mogelijk willen bereiken en informeren, blijven we daarenboven infosessies aanbieden over veilig digitaal bankieren aan andere doelgroepen zoals senioren. Samen met vertegenwoordigers van de verschillende banken, geven we tijdens deze sessies een antwoord op al hun vragen rond digitaal bankieren en de veiligheid ervan.

Febelfin werkte ook mee aan een E-learning 'Cyberveiligheid' van de VDAB die zal aangeboden worden aan iedereen die een account heeft bij de VDAB.

Stakeholder event "Cyberveiligheid"

In samenwerking met het BIN kenniscentrum en de Federale diensten van de Gouverneurs van Vlaams-Brabant en Antwerpen, organiseerde Febelfin een stakeholder event over cyberveiligheid. Er werd samen een antwoord gezocht op prangende vragen zoals 'Hoe kunnen we als betrokken stakeholders nauwer samenwerken?' en 'Hoe kunnen we cruciale informatie over cyberveiligheid nog beter verspreiden binnen onze lokale doelgroepen?'. Op die manier werden er inspirerende ideeën uitgewisseld en werd cyberveiligheid nogmaals hoog op de agenda geplaatst

Jaarlijkse sensibiliseringsactie geldezels

Febelfin is zich bewust van de gevaren van het fenomeen geldezels en zet in op bijkomende sensibilisering door een jaarlijkse perscommunicatie om dit onder de aandacht te brengen, maar ook door roadshows voor jongeren en gratis educatief materiaal aan te bieden. Lees er meer over op pagina 10 in deze storytelling.

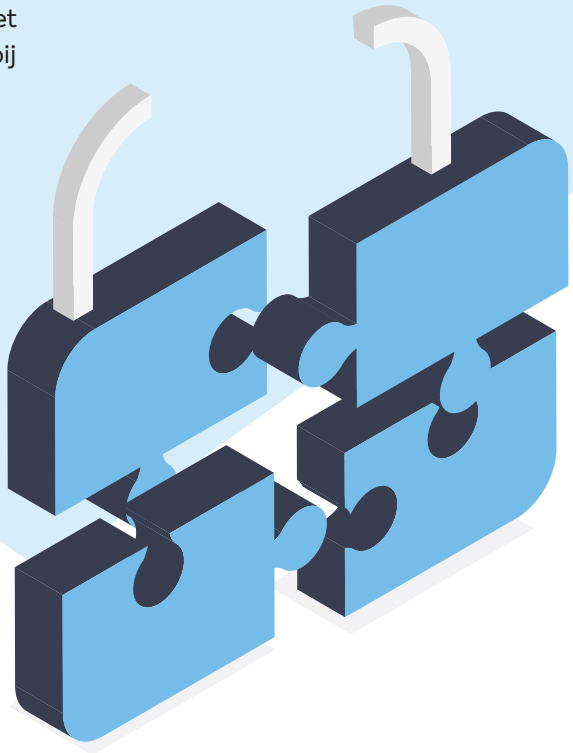
SAMENWERKING TUSSEN VERSCHILLENDE STAKEHOLDERS BLIJFT CRUCIAAL

De sector is er zich ten volle van bewust dat we de strijd tegen phishing en online fraude enkel kunnen laten slagen door de handen in elkaar te slaan. Een continue samenwerking met de verschillende stakeholders, de overheid en veldorganisaties is en blijft in dit kader noodzakelijk. Febelfin zal dan ook aan andere stakeholders voorstellen om expertise en middelen te bundelen om in de toekomst te werken aan gezamenlijke campagnes.

Aangezien de technieken van online oplichters, d.m.v. technologische ontwikkelingen zoals AI en deep fakes, steeds evolueren, zullen we nog met heel wat uitdagingen worden geconfronteerd. Een continue gezamenlijke opvolging van deze ontwikkelingen en het nodige aanpassingsvermogen zijn daarbij cruciaal.

Enkel door het ontwikkelen van een gedeelde visie en strategie tussen alle betrokken partijen over hoe we cybercriminaliteit verder kunnen bestrijden en de economie op een veilige manier draaiende kunnen houden, kunnen we er samen voor zorgen dat iedereen zich veilig voelt in de digitale wereld van vandaag én morgen.

Febelfin deed enkele aanbevelingen in zijn politiek memorandum op vlak van cybersecurity. Deze kan u **hier** terugvinden.



Belgische Federatie van de financiële sector

www.febelfin.be