

**If it smells phishy,
it probably is!**



IF IT SMELLS PHISHY, IT PROBABLY IS

Online fraude blijft een hardnekkig probleem. Ook in 2024 bleven cybercriminelen actief phishingberichten versturen, waarbij ze zich voordeden als een vertrouwde persoon of organisatie, zoals een bank of een overheidsinstantie. Gelukkig kon de banksector 75% van de frauduleuze overschrijvingen als gevolg van phishing detecteren, tegenhouden of terugvorderen. Toch slaagden fraudeurs erin om via phishing alsnog 49 miljoen euro buit te maken.



€ 49
miljoen
buit in 2024

Online fraude blijft zich ontwikkelen – en steeds vaker gebeurt dat op sluwe manieren. Waar het ooit begon met phishing via simpele e-mails, zien we vandaag een groeiend aantal gevallen waarbij mensen zélf worden overtuigd om geld over te maken. Het begint vaak met een geloofwaardig telefoontje, een professioneel ogende website of een dringend verzoek via een vertrouwde app zoals itsme®. Voor je het weet, lijkt het alsof je met je bank of een overheidsinstantie spreekt of een gouden beleggingskans krijgt aangeboden.

Beleggingsfraude, bankhelpdeskfraude, en misleidende verzoeken via digitale toepassingen: het zijn vormen van oplichting die steeds geraffineerder worden. En hoewel er al veel inspanningen zijn

geleverd om mensen te waarschuwen, blijft het bewustzijn bij een groot deel van de bevolking achter. Net als in vorige jaren blijkt dat veel Belgen nog onvoldoende gewapend zijn tegen deze moderne vormen van bedrog.

Gelukkig reageren steeds meer mensen alert bij een vermoeden van oplichting, bijvoorbeeld door onmiddellijk hun bank te contacteren of hun rekeningsaldo en transacties te controleren. Tegelijkertijd neemt de algemene kennis over phishing en geldezels onder de bevolking toe. Ook het aantal mensen dat hun pincode deelt of hun bankkaart opstuurt naar een opgegeven adres, blijft dalen. Deze inzichten onderstrepen het belang van blijvende sensibilisering. Iedereen kan immers het doelwit worden van online fraude. Vooral jongeren blijken kwetsbaar, mede door hun vaak nonchalante houding ten opzichte van online veiligheid.

Daarom blijft de sector volop inzetten op vernieuwende initiatieven en krachtige samenwerkingen om online fraude doeltreffend aan te pakken. Door krachten te bundelen met partners uit verschillende domeinen – van technologie en financiële instellingen tot overheid en onderwijs – bouwen we aan een sterk front tegen cybercriminaliteit. Met gerichte campagnes, slimme tools en voortdurende bewustmaking willen we niet alleen reageren op fraude, maar ze nog vaker voorkomen. Want alleen samen kunnen we de digitale veiligheid van iedereen versterken.

Ontdek alle details in onze storytelling met de meest recente cijfers en een overzicht van enkele nieuwe initiatieven van de sector.

DE VANGST DOOR PHISHERS BLIJFT GROOT

Ze komen binnen als een onschuldig berichtje.

Een melding van je bank, een waarschuwing van de politie, een update van je ziekenfonds of watermaatschappij. Alles lijkt vertrouwd – tot je twee keer kijkt. Want achter die bekende namen zoals de Christelijke Mutualiteit, RIZIV, De Watergroep of de federale politie, schuilt vaak een oplichter met een plan.

Phishing is vandaag uitgegroeid tot een van de meest gebruikte vormen van online fraude. Safeonweb, het meldpunt van het Centrum voor Cybersecurity België, ontvangt dagelijks bijna 26.000¹ meldingen van verdachte berichten. Dat zijn er bijna 9,5 miljoen per jaar – een hallucinant

cijfer dat toont hoe hardnekkig deze vorm van fraude is.

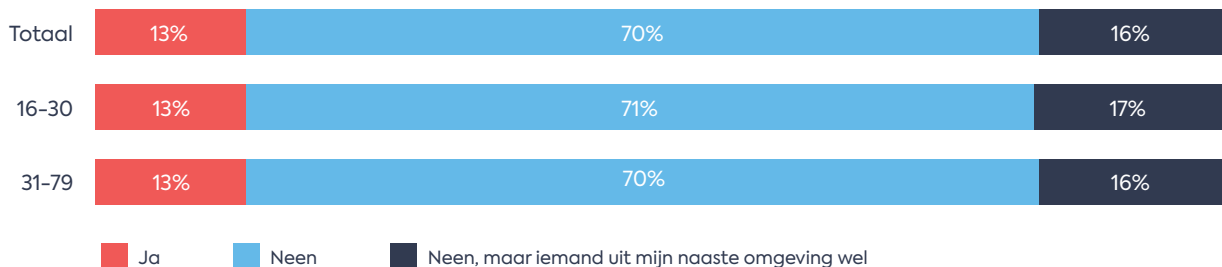
En hoewel banken erin slagen om 75% van de frauduleuze overschrijvingen te detecteren, blokkeren of terug te vorderen, blijft phishing een lucratieve praktijk. In 2024 alleen al werd er via deze methode zo'n 49 miljoen euro buitgemaakt. Het toont aan hoe overtuigend deze aanvallen zijn geworden – en hoe belangrijk het is om alert te blijven.

Een onderzoek van Febelfin in samenwerking met onderzoeksbureau Indiville² bevestigt de omvang van deze fraudevorm.

Een actueel gevaar

Uit het onderzoek blijkt dat 13% van de Belgen ooit slachtoffer is geworden van phishing.

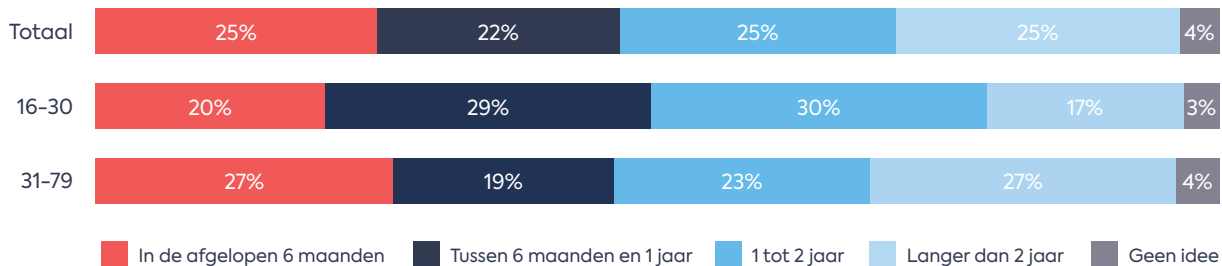
Ben je al slachtoffer geworden van phishing?



Bron: Indiville

Wanneer we kijken naar wanneer de respondenten slachtoffer werden van phishing, zien we dat dit een actueel probleem blijft.

Hoelang was dit geleden?



Bron: Indiville

¹ Bron: Safeonweb juli 2025

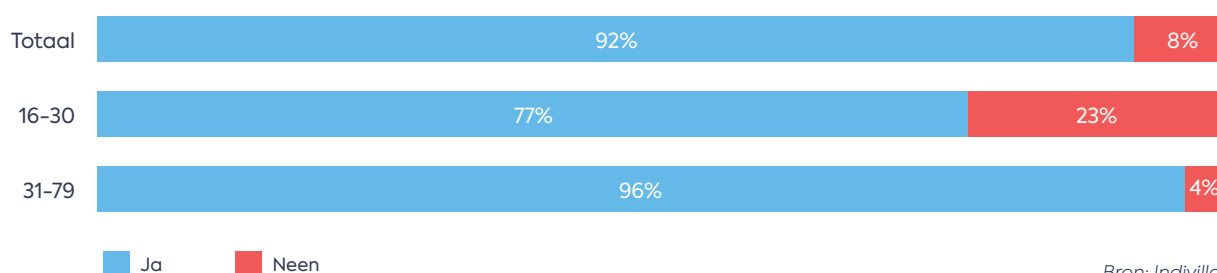
² IndiVille onderzoek, 20 januari – 9 februari 2025, op een representatief staal van de Belgische bevolking n: 2149 NL/FR enquêtes, leeftijd 16-79. Maximale foutenmarge: 2,1%

Kennis over deze fraudevorm

Hoewel veel mensen zich bewust zijn van het gevaar, moet de kennis over phishing beter. Wist je dat 8% van de Belgische bevolking nog nooit van phishing heeft gehoord? Bij jongeren tussen 16 en 30 jaar is dat percentage hoger: 23% kent de term niet. Ouderen zijn daarentegen over het

algemeen beter op de hoogte: slechts 4% van hen heeft nog nooit van phishing gehoord. Dit wijst erop dat sensibiliseringsinitiatieven gericht op ouderen in samenwerking met lokale partners, zoals onze infosessies over veilig online bankieren & betalen (zie p. 12), hun vruchten afwerpen.

Heb je ooit al gehoord van phishing?



Bron: Indiville

Belangrijke valkuilen, zeker voor jongeren

Bankcodes delen & financiële gegevens doorgeven

De meeste Belgen weten het intussen wel: je bankcodes geef je nooit door. Ongeacht de leeftijd zegt 9 op de 10 ondervraagden dat ze hun codes onder geen beding zouden delen. Maar toch zou een kleine minderheid – 2% – dat zonder aarzeling doen.

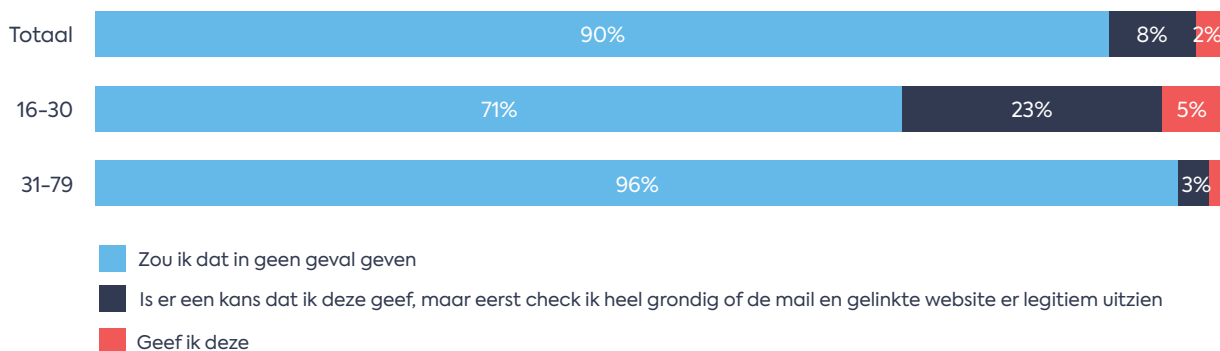
Maar zodra we naar jongeren kijken, komt er een minder rooskleurig beeld naar voren. Zo geeft 23% van hen aan dat ze mogelijk hun bankcodes zouden delen als daarom gevraagd wordt via e-mail, sms of een andere digitale weg – nadat ze het bericht en de bijhorende website zorgvuldig hebben bekeken. En 5% van de jongeren zou hun codes zelfs zonder enige controle doorgeven.

Toch is er ook goed nieuws. Want waar in 2022 nog 13% van de jongeren aangaf hun bankcodes zomaar te delen, is dat cijfer vandaag gedaald

tot 5%. Een duidelijke verbetering, die aantoont dat sensibilisering werkt – al ligt dit percentage nog steeds veel te hoog en blijft waakzaamheid geboden.



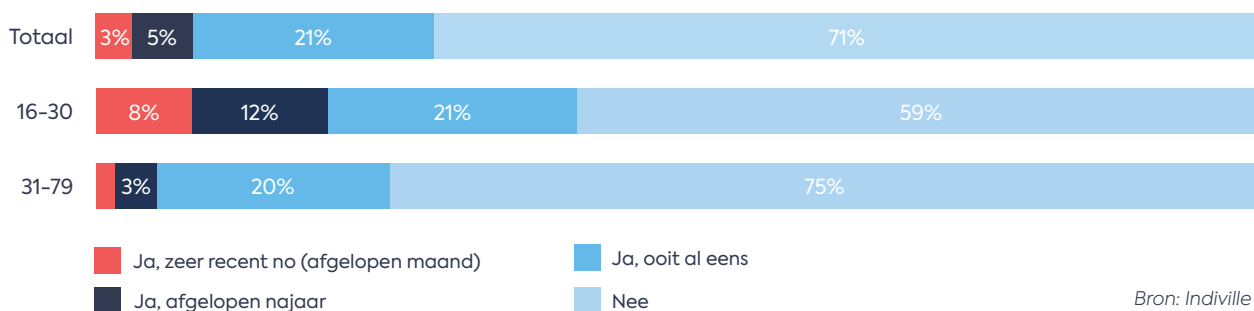
Als je bank via e-mail, sms, whatsapp, telefoon ... naar jouw bankcodes vraagt ...



Bron: Indiville

Daarnaast blijkt uit het onderzoek dat jongeren over het algemeen vaker online financiële informatie waarover ze zich ongemakkelijk voelen delen. 8% van het totale aantal respondenten gaf aan dit in de afgelopen maanden te hebben gedaan, terwijl dit percentage bij jongeren aanzienlijk hoger ligt: 20%.

Heb je ooit al financiële gegevens online doorgegeven waarover je je achteraf ongemakkelijk voelde?



Bron: Indiville

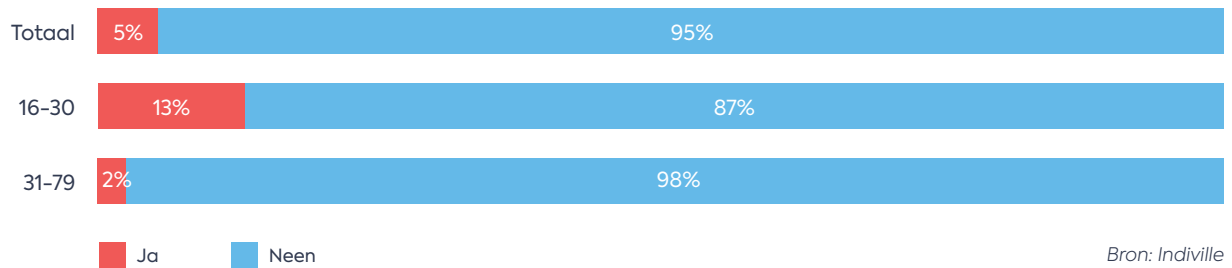
Bankkaart opsturen

Stel je voor: je krijgt een telefoontje of bericht van je 'bank'. Je bankkaart vervalt binnenkort. Om een vlotte overgang te garanderen, stuur je ons best zo snel mogelijk je oude kaart en bijhorende pincode op. Voor de meeste Belgen is het antwoord duidelijk: nee, natuurlijk niet. Uit het onderzoek blijkt dan ook dat 95% van de ondervraagden hun bankkaart nooit zou terugsturen, zelfs niet op dringend verzoek van een zeggende bank.

Maar bij jongeren ligt het verhaal anders. Daar geeft 13% aan dat ze wél geneigd zouden zijn om hun kaart op te sturen. Dat cijfer is alarmerend – vooral omdat het geen verbetering toont ten opzichte van vorig jaar. Het onderstreept hoe belangrijk het is om jongeren te blijven informeren en bewust te maken van de risico's. Want oplichters worden steeds slimmer, en een moment van twijfel kan genoeg zijn.



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



WAT DOE JE ALS JE IN EEN PHISHINGVAL BENT GETRAPT?



Kennis van de te ondernemen stappen

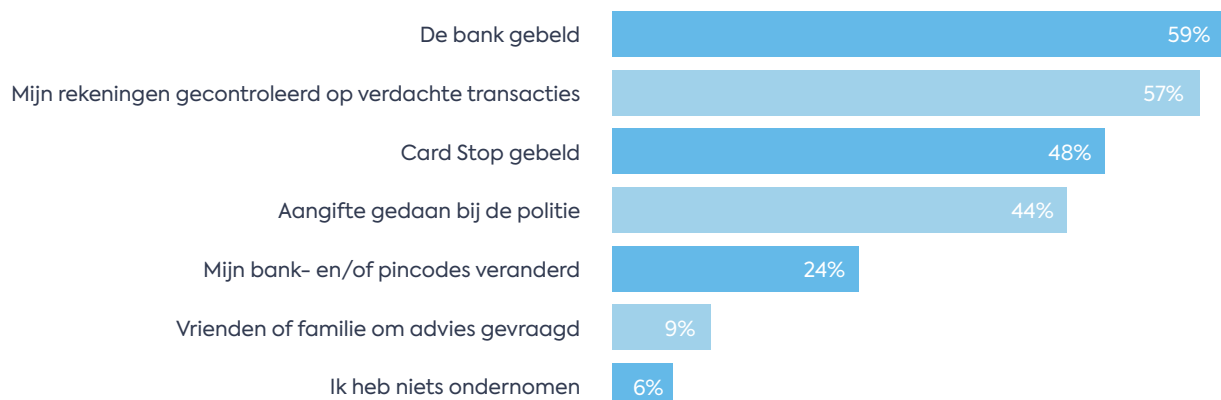
Het is een vraag die niemand zich graag stelt, maar wel eentje waarop je best het antwoord kent. Want zelfs met alle waarschuwingscampagnes en preventietips, kan het toch gebeuren: één klik, één onoplettend moment, en je bent slachtoffer.

Gelukkig zien we dat steeds meer mensen weten wat ze moeten doen als het misgaat. Uit het onderzoek blijkt dat 64% van de slachtoffers meteen wist welke stappen ze moesten ondernemen of waar ze hulp konden zoeken. Nog eens 6% wist het zelf niet, maar kon gelukkig terecht bij iemand in hun omgeving voor goede raad.

Toch is er werk aan de winkel – vooral bij jongeren. In de leeftijdsgroep van 16 tot 30 jaar gaf maar liefst 39% aan niet te weten wat te doen na een geslaagde phishingpoging. Ter vergelijking: bij de 31- tot 79-jarigen ligt dat cijfer op 27%. Het toont aan dat kennis over wat te doen na een geval van phishing minstens even belangrijk is als het voorkomen ervan.

Want wie weet wat te doen, kan snel handelen. En snel handelen maakt vaak het verschil tussen beperkt verlies en grote schade.

Welke van de volgende stappen heb je gezet?





Om mensen nog beter te wapenen tegen online fraude, heeft Febelfin samen met de lokale politie en partners zoals SAAMO, CAW en andere stakeholders een nieuwe flyer ontwikkeld. Deze handige gids bundelt alle essentiële informatie op één plek: wat je moet doen bij online oplichting, waar je terecht kunt voor hulp, en hoe je jezelf beter kunt beschermen. Een praktisch hulpmiddel dat mensen op een toegankelijke manier wegwijs maakt in een vaak verwarrende situatie.

[DOWNLOAD DE FLYER →](#)

Het belang van continue sensibilisering

De cijfers spreken voor zich: steeds meer mensen herkennen de signalen van phishing.

Er is duidelijk vooruitgang geboekt in de bewustwording rond online fraude. Maar tegelijk blijft het cruciaal om verder te bouwen aan kennis en digitale weerbaarheid – vooral bij jongeren, die zich vaak in een online wereld bevinden waar risico's niet altijd zichtbaar zijn.

Daarom zet de financiële sector volop in op gerichte acties. Niet alleen door jongeren te leren hoe ze phishing kunnen herkennen en vermijden, maar ook door slachtoffers te ondersteunen met heldere stappen en toegankelijke hulp. Want hoe sneller iemand weet wat te doen, hoe kleiner de schade.

In dat kader lanceerde Febelfin een opvallende **campagne** rond fraude in online games – een thema dat jongeren rechtstreeks aanspreekt. Daarnaast werd het educatieve platform **Klassebank** gelanceerd, waar leerkrachten gastlessen en lesmateriaal vinden over financiële thema's, waaronder online fraude. Het doel? Jongeren sterker maken in hun digitale keuzes, en hen de kennis meegeven die nodig is om veilig te navigeren in een steeds complexere online wereld.



Als je een hele mooie aanbieding krijgt, is het waarschijnlijk te mooi om waar te zijn.

[BEKIJK DE VIDEO →](#)

PHISHING IS MISSCHIEN DE BEKENDSTE VORM VAN ONLINE FRAUDE, MAAR HET IS LANG NIET DE ENIGE

Andere online fraudevormen nog te weinig gekend

Online oplichters zitten niet stil.

Naast phishing gebruiken ze steeds vaker andere vormen van online fraude om slachtoffers te misleiden. Denk aan hulpvraagfraude, waarbij iemand zich voordoeft als een vriend in nood, of beleggingsfraude met beloften van snelle winst. Ook bank- en computerhelpdeskfraude winnen terrein, net als recente pogingen waarbij fraudeurs vragen om acties goed te keuren via de identificatie-app itsme®.

Voorbeelden van fraude met itsme®:

- Slachtoffers krijgen te horen dat er verdachte betalingen zijn gedetecteerd en dat ze die via itsme® kunnen annuleren. In werkelijkheid keuren ze zo de betalingen van de oplichter goed.
- Een nep-bankmedewerker vraagt om de identiteit te bevestigen via itsme®, maar in werkelijkheid geeft het slachtoffer toegang tot zijn online bankomgeving.

[ONTDEK ENKELE TIPS](#)

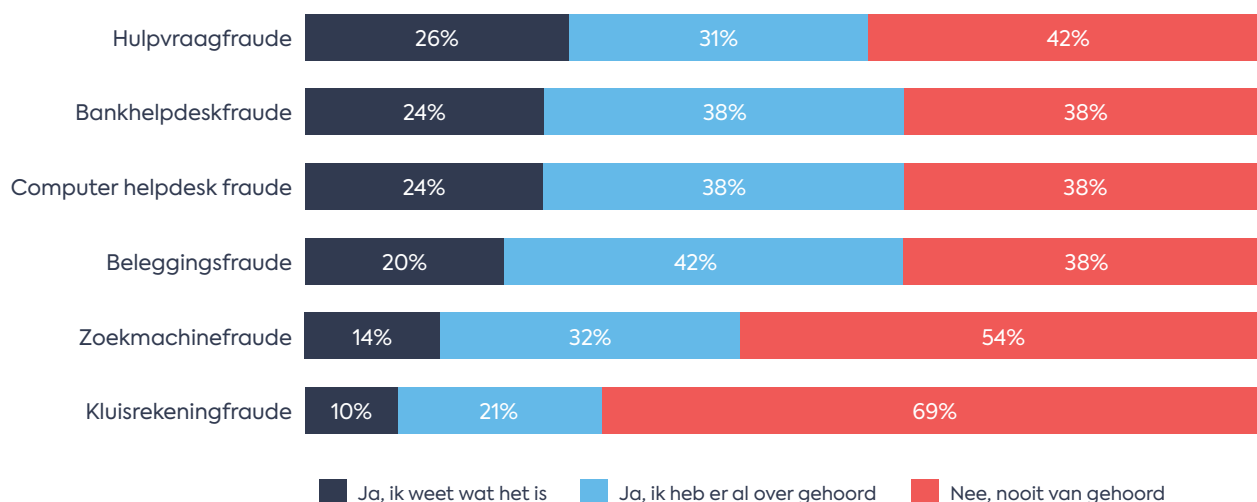
[DEZE FRAUDE TE VOORKOMEN](#) →



Uit onderzoek blijkt dat deze vormen van fraude nog te weinig gekend zijn bij het grote publiek. Slechts 1 op de 5 Belgen weet wat deze fraudevormen precies inhouden. Een derde heeft er al eens van gehoord, maar weet niet goed wat het betekent. En bijna de helft tast volledig in het duister. Opvallend: dit gebrek aan kennis is niet leeftijdsgebonden – jong of oud, de meeste mensen zijn er onvoldoende mee vertrouwd.

Sommige vormen van fraude zijn zelfs bijna volledig onbekend. Zo heeft 69% van de respondenten nog nooit gehoord van kluisrekeningfraude, en 54% kent zoekmachinefraude niet. Zelfs bij beleggingsfraude – een vorm die vaak in de actualiteit komt – weet slechts 20% van de respondenten exact wat het inhoudt.

Weet je wat deze vormen van fraude zijn?



Bron: Indiville

Het toont aan dat er nog veel werk aan de winkel is. Want hoe kun je jezelf beschermen tegen iets waarvan je niet weet dat het bestaat?

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

TIP

In het online dossier van Febelfin worden de verschillende types van online fraude makkelijk uitgelegd en krijg je waardevolle tips over hoe je jezelf kunt beschermen.

[LEES MEER →](#)

GELDEZELS

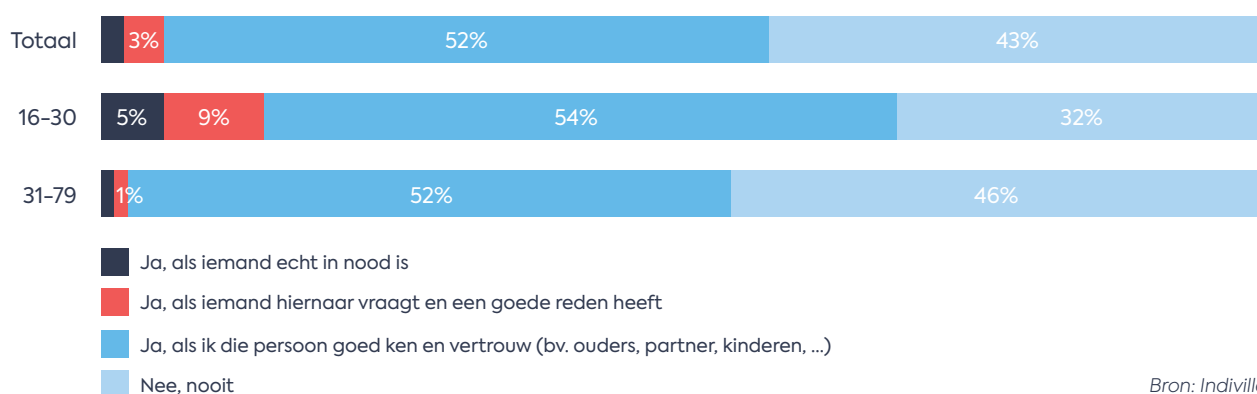
Snel geld verdienen? Klinkt goed, toch? Een onbekende vraagt je om even je bankkaart of rekening uit te lenen. Makkelijk verdiend, lijkt het. Maar achter dat onschuldige voorstel schuilt vaak iets veel ernstigers: je wordt een geldezels – en dus medeplechtig aan fraude.

Nog altijd lopen mensen in de val. Uit onderzoek

blijkt dat 14% van de jongeren bereid is hun bankkaart en pincode te delen voor geld, een lichte stijging ten opzichte van 2024. Bij de hele bevolking ligt dat percentage op 5%.

Wat begint als een snelle deal, kan eindigen in een strafblad. Daarom blijft Febelfin waarschuwen: laat je niet misleiden.

Zou jij je bankkaart en pincode afgeven aan iemand anders?



Bron: Indiville

WAT IS EEN GELDEZEL?

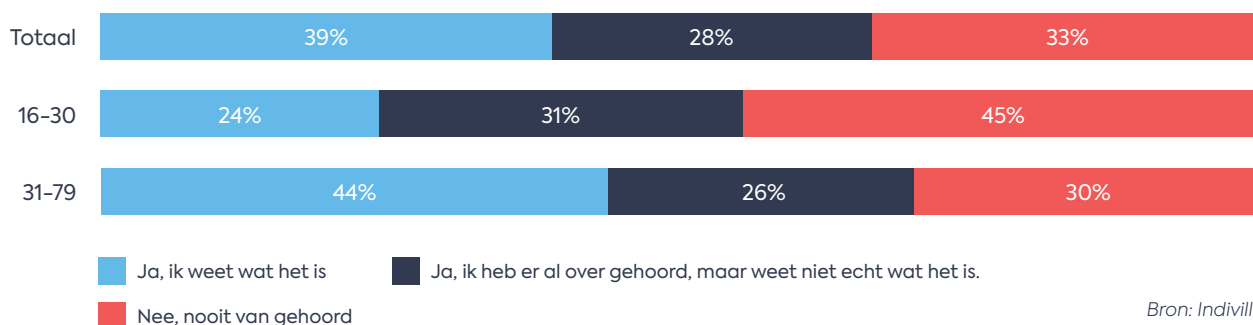
Een geldezel is iemand die zijn bankrekening en/of bankkaart en pincode laat gebruiken door criminelen om crimineel geld wit te wassen. Daardoor kan de crimineel misdaadgeld op de bankrekening van de geldezel storten om het vervolgens af te halen (met de bankkaart en de pincode van de geldezel) of door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



Wat is een geldezel? Veel jongeren hebben geen idee

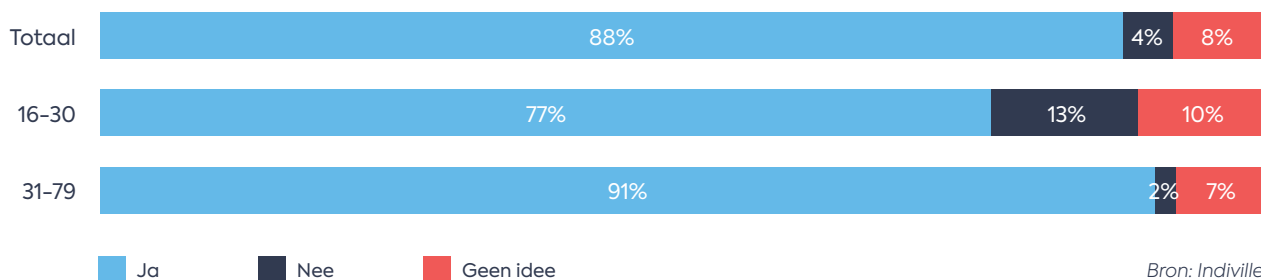
Hoewel bijna 40% van de Belgen weet wat het begrip inhoudt, zakt dat cijfer bij jongeren naar slechts 24%. Maar liefst 45% van hen heeft er zelfs nog nooit van gehoord.

Weet jij wat een geldezel is?



En wat velen niet beseffen: wie zijn bankrekening of bankkaart uitleent voor criminele doeleinden, pleegt een strafbaar feit – met zware gevolgen zoals geldboetes, celstraffen en het terugbetalen van slachtoffers.

Denk je dat je als geldezel strafbaar bent?



Toch blijft het fenomeen onder de radar. Uit het onderzoek blijkt dat 4% van de Belgen al benaderd werd met de vraag om geldezel te worden, en dat nog eens 4% iemand kent die dit meemaakte. Bij jongeren liggen die cijfers nog hoger: 7% werd zelf al aangesproken, en 12% kent iemand in hun omgeving die zo'n voorstel kreeg.

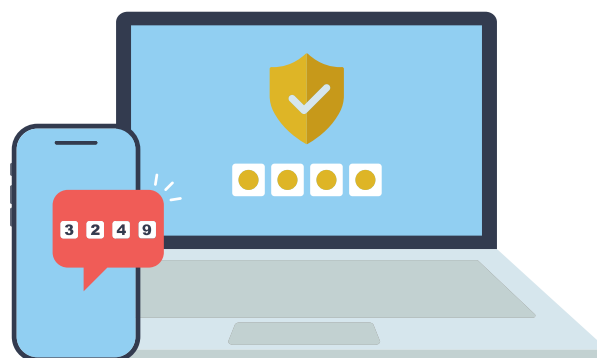
Ben je ooit zelf al benaderd geweest om geldezel te worden?



De cijfers blijven al jaren stabiel, en dat is zorgwekkend. Jongeren blijven een belangrijk doelwit voor deze vorm van fraude. Daarom is het essentieel om hen te blijven informeren over wat een geldezel is, en vooral: wat de risico's zijn.

ONLINE SHOPPEN: SNEL, MAKKELIJK... EN VEILIG?

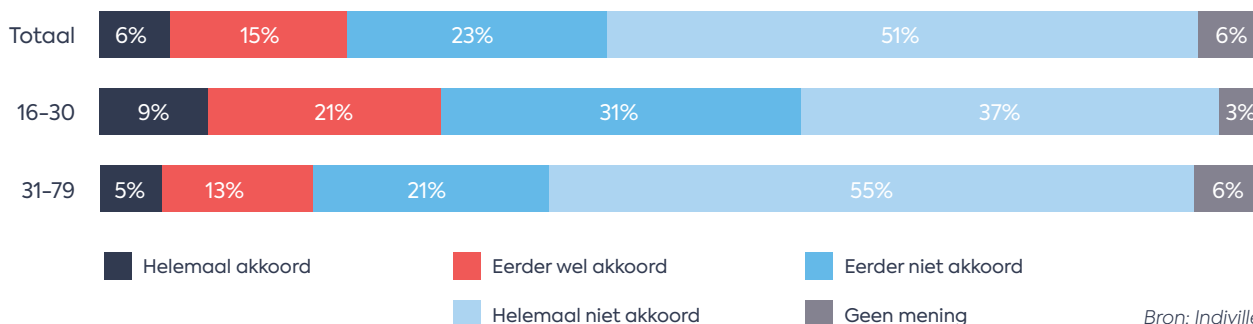
Voor veel Belgen zijn de extra veiligheidsstappen bij online aankopen – zoals het ingeven van een extra code, vingerafdruk of het gebruik van een kaartlezer – intussen vanzelfsprekend. Ze weten dat die paar seconden hen extra beschermen tegen fraude.



Toch denkt niet iedereen er zo over. Uit het onderzoek blijkt dat 1 op de 5 Belgen deze stappen eerder als een last dan als een bescherming ziet. Vooral jongeren ervaren ze vaker als een hindernis: 30% van hen vindt het omslachtig, tegenover 18% bij oudere generaties.

En dat is niet zonder risico. Want wie de beveiliging als overbodig beschouwt, is vaak ook minder alert voor online oplichting. Daarom blijft het belangrijk om te blijven uitleggen waarom die extra klik of code nodig is. Zeker bij jongeren, van wie drie op de tien nog onvoldoende beseffen hoe belangrijk die digitale sloten zijn.

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

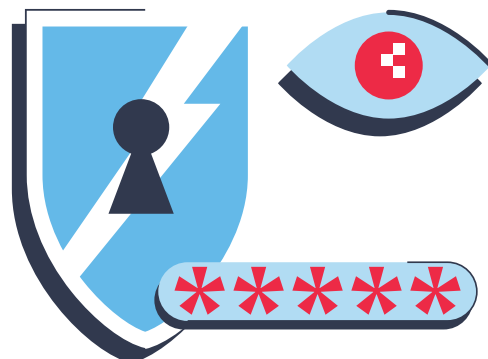


Bron: Indiville

DE STRIJD TEGEN ONLINE FRAUDE IS GEEN SOLO-OPDRACHT, MAAR EEN GEDEELDE VERANTWOORDELIJKHEID.

Online fraudeurs worden steeds slimmer – en dus moeten wij dat ook zijn. Om online fraude te beperken is het belangrijk om met alle actoren op het terrein zoveel als mogelijk de bevolking te blijven sensibiliseren. Een waakzame en geïnformeerde consument zal minder snel slachtoffer worden. De strijd tegen financiële criminaliteit, is bovendien een **gedeelde verantwoordelijkheid**, die ook door verschillende partijen gedragen moet worden, zoals de consumenten, telecomsector en de sociale mediaplatformen. Enkel met een **doorgedreven samenwerking** met alle spelers op het terrein, ondersteund door een (Europese) wetgeving kunnen wij het tij doen keren.

Het stopt echter niet daar. Ook het naleven door alle spelers in de ketting (e-commerce handelaars, online (sociale)mediaplatformen, telecom,...) van wetgeving inzake data protection en cybersecurity is van uiterst belang om online fraude te bestrijden en consumenten te beschermen. **Ook deze actoren hebben een verantwoordelijkheid ten aanzien van de maatschappij.** De Europese Commissie (EC), Europese Raad en het Europees Parlement erkennen dit ook. In het kader van de herziening van de PSD2, heeft de Europese Commissie een voorstel van Payment Services Regulation (PSR) ingediend om het aansprakelijkheidsregime te waarborgen en bovenstaande uitdagingen aan te pakken. Zo voorzien ze bijkomende handvaten om fraude



tegen te gaan en kijken ze in de richting van alle spelers in de ketting (e-commerce handelaars, sociale mediaplatformen, telecom,...) om hun steentje bij te dragen in de strijd tegen fraude.

Kortom, fraudebestrijding is niet enkel de taak van de banken. **Banken hebben versterking nodig van alle spelers in het ecosysteem om de strijd aan te gaan tegen fraudeurs.** Consumenten, de telecomsector, e-commerce handelaars, sociale mediaplatformen,... en banken moeten samenwerken teneinde burgers te beschermen tegen de steeds sluwere methodes van online oplichters.

Febelfin deed enkele aanbevelingen in zijn politiek memorandum op vlak van cybersecurity.

[LEES HET MEMORANDUM →](#)

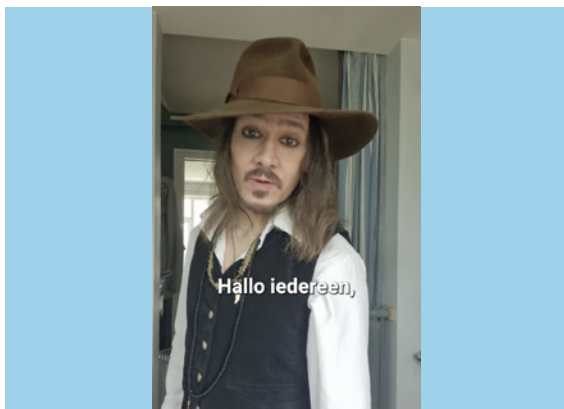
Febelfin zat het voorbije jaar dan ook niet stil

We lanceerden **opnieuw tal van initiatieven**, telkens in samenwerking met sterke partners – want daar ligt onze kracht. Zo ontwikkelden we samen met onder andere de lokale politie, SAAMO en CAW een toegankelijke **flyer** met alle essentiële info voor wie slachtoffer is van online fraude. Dankzij een testpanel samengesteld door SAAMO zijn we zeker dat ook kwetsbare doelgroepen de informatie begrijpen en kunnen gebruiken.

Daarnaast gaven we het hele jaar door **infosessies over veilig online bankieren**. Onze e-learning werd gevolgd door meer dan 450 digihelpers, die nu gewapend zijn met kennis over de nieuwste fraudevormen en het beschikbare educatief materiaal.

We speelden ook in op de actualiteit

In oktober werkten we samen met Safeonweb rond 2-factorauthenticatie. We sensibiliseerden rond **social engineering via itsme®** en lanceerden de opvallende **Johnny Depni-campagne** over datingfraude, die heel wat getuigenissen losmaakte. Onze **actie voor jongeren** met Andy Peelman was een schot in de roos: meer dan 2 miljoen jongeren zagen de video waarin hij waarschuwt voor het delen van persoonlijke gegevens in ruil voor gratis gamecoins.



Ook op technisch vlak zetten we stappen vooruit

We startten met de gefaseerde invoering van de verificatie van de naam van de begunstigde, of **IBAN-naamcontrole** – een slimme tool die klanten waarschuwt als de naam en het rekeningnummer van een begunstigde niet overeenstemmen. Deze gratis dienst verhoogt het vertrouwen bij overschrijvingen en helpt fraude voorkomen.

En we gaan door!

De financiële sector blijft zich inzetten om nieuwe, doelgerichte initiatieven te ontwikkelen. Want alleen samen maken we het verschil in de strijd tegen online fraude.



Belgische Federatie van de financiële sector

Koning Albert II-laan 19, 1210 Brussel

www.febelfin.be