Do not feed the phish

Fraude en oplichting uitgelicht

febelfin

Vandaag de dag zijn we met zijn allen meer dan ooit online: de coronapandemie in 2020 heeft het digitale leven verder versneld. De pandemie heeft wel meerdere veranderingen teweeg gebracht, maar heeft ook gezorgd voor een opstoot in het aantal frauduleuze berichten die constant circuleren.

Internetfraude is vandaag alomtegenwoordig. De meeste Belgen kwamen intussen al eens in aanraking met een poging tot online fraude. Er is zeker ook goed nieuws: ondanks de vele fraudepogingen, blijkt uit de cijfers van 2021[1] dat geslaagde fraude met phishing met een kwart gedaald is. We zien echter een verschuiving naar andere vormen van fraude.

Hoe staan we er nu voor? Hoe evolueert online fraude en wat zijn de actuele fraudevormen? Hier lees je de resultaten van het jaarlijkse onderzoek[2] dat Febelfin in samenwerking met onderzoeksbureau IndiVille uitvoerde.

PHISHING: HENGELEN NAAR GEHEIME CODES

Fraudeurs vissen naar persoonlijke bankcodes van hun potentiële slachtoffers, door zich voor te doen als een gekende of vertrouwde organisatie. Hun modus operandi: ze sturen hun slachtoffer een e-mail, sms, WhatsApp'je, berichtje via Facebook Messenger of andere sociale media, ...). Dat bericht bevat een link naar een – vaak nagenoeg perfect - nagemaakte website, waarop het slachtoffer persoonlijke bankcodes invoert. Wanneer ze die persoonlijke bankcodes kunnen bemachtigen, voeren fraudeurs in naam van het slachtoffer transacties uit en plunderen ze de rekening.

WIST JE DAT?

De term 'phishing' werd voor het eerst gebruikt in 1996, toen hackers wachtwoorden probeerden stelen van America Online-gebruikers (nu AOL). Ze maakten de vergelijking met 'fishing', sportvissen, omdat ze met hun valse e-mails lijntjes uitsmeten in de 'zee' van internetgebruikers. Net zoals bij het hengelen naar vissen, moeten er maar een paar mensen bijten om van succesvolle phishing te spreken.

Het aantal fraudepogingen via phishing blijft vandaag de dag hoog en geen enkele sector wordt gespaard. Gelukkig is er ook goed nieuws: het aantal geslaagde gevallen van phishing neemt af. Zo werd er in 2020 via deze fraudevorm 34 miljoen euro buitgemaakt. In 2021 was dit 9 miljoen euro minder: een mooie daling van meer dan 26%. De samenwerking tussen verschillende stakeholders, de inspanningen van de banken en de verscheidene sensibiliseringsacties zorgen ervoor dat minder phishers hun slag konden slaan. Daarnaast kon ook via intensieve monitoring door de banken, veel schade vermeden worden: in 2021 werd maar liefst 75% van alle frauduleuze overschrijvingen via phishing geblokkeerd of teruggevorderd.

Helaas zagen we in 2021 ook een belangrijke verschuiving richting andere fraudevormen zoals beleggings-, factuur-, hulpvraag- of kluisrekeningfraude, waarbij het slachtoffer wordt overgehaald om zelf geld over te maken. Fraudeurs maken gebruik van verschillende kanalen - zoals email, brief, telefoon, sms, sociale media en whatsapp - en plegen de fraude in naam van verschillende organisaties en instellingen zoals banken, overheidsadministraties, telecomoperatoren, nutsbedrijven, enzovoort. In de strijd tegen online fraudeurs is samenwerking dus essentieel, ook in 2022 en de volgende jaren.

[1] Phishingfraude in 2021: de cijfers | Febelfin

[2] *IndiVille onderzoek februari-maart 2022, op een representatief staal van de Belgische bevolking n: 2164 NL/FR enquêtes, leeftijd 16-79.*

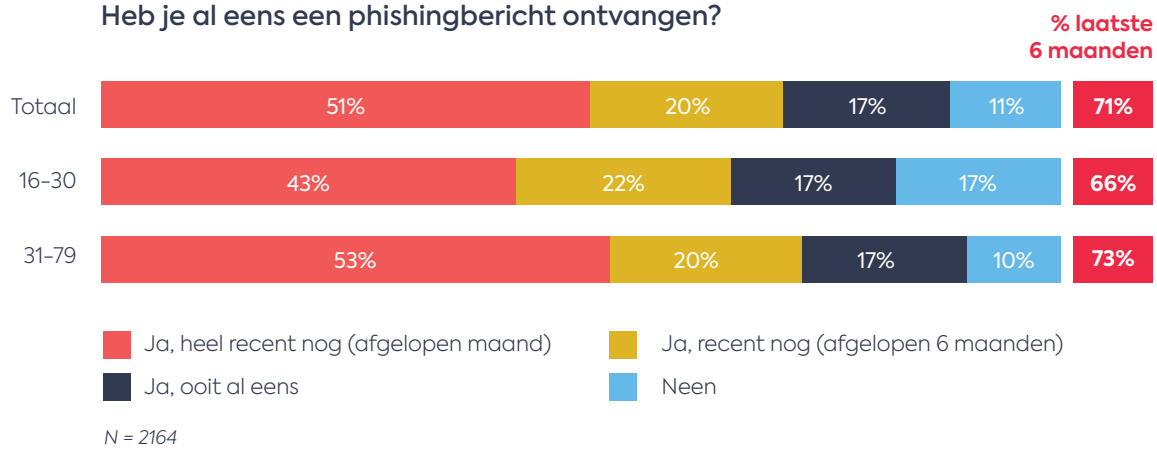
DE PHISHINGPOGINGEN BLIJVEN TOENEMEN

71%

van de ondervraagden ontving in de voorbije 6 maanden een phishingbericht

Hoewel er in 2021 minder geslaagde pogingen waren, blijft het phishingprobleem groter worden. Het **aantal phishingpogingen** neemt namelijk **wél nog steeds toe in 2022**. 71% van de ondervraagden ontving in de voorbije 6 maanden een phishingbericht. Dit cijfer kent een stijging in vergelijking met 2021 toen 34% een phishingbericht had ontvangen.

Heb je al eens een phishingbericht ontvangen?



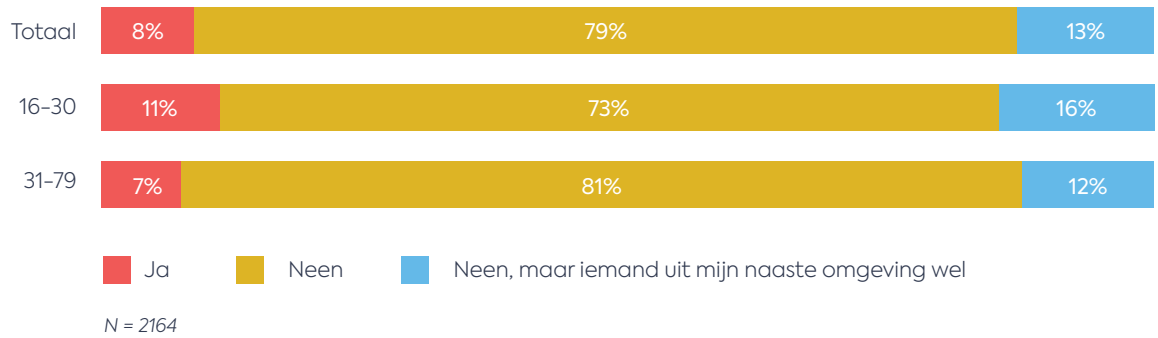
N = 2164

8%

van de ondervraagden is al ingegaan op een frauduleus bericht

Van de mensen die zo'n frauduleus bericht ontvingen, geeft 8% aan hierop te zijn ingegaan. Dit toont aan dat het belangrijk is om blijvend te sensibiliseren tegen online fraude en mensen te helpen bij het herkennen van frauduleuze berichten.

Ben je al slachtoffer geworden van phishing?



N = 2164

WELKE STAPPEN NEEM JE ALS JE SLACHTOFFER WORDT VAN PHISHING?

- **Contacteer onmiddellijk je bank.**
- **Bel Card Stop op het nummer 078 170 170 om je bankkaarten te blokkeren.**
- **Dien een klacht in bij de politie.**

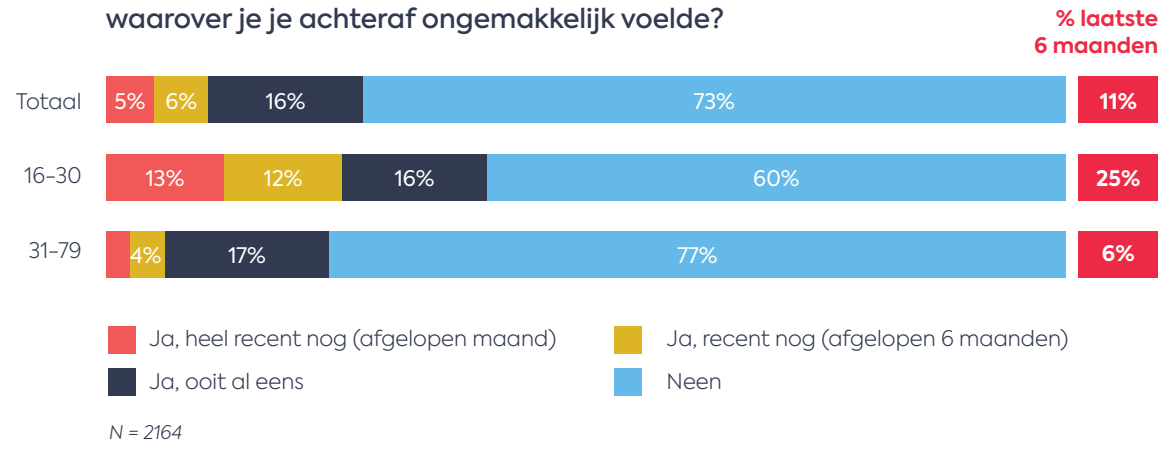
Deel jij zomaar financiële gegevens met onbekenden?

11%

van de ondervraagden deelden de afgelopen 6 maanden financiële gegevens waar ze zich ongemakkelijk bij voelden.

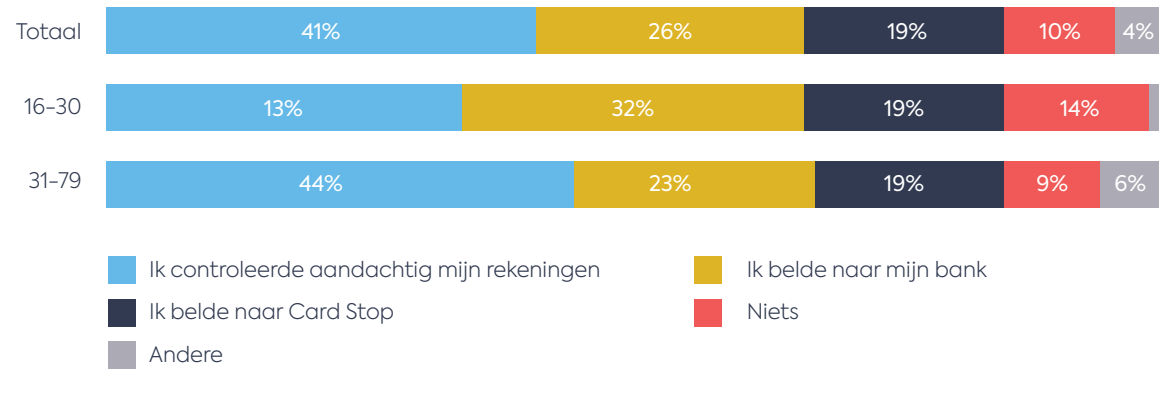
In het algemeen deelde 11% van de ondervraagde Belgen in de afgelopen 6 maanden financiële gegevens waar ze zich ongemakkelijk bij voelden. Dat is een **stijging tegenover 7% in 2021**. Een positieve noot hierbij: **90%** van deze mensen ondernam actie en **controleerde** hun rekening, of **nam contact op met de bank of Card Stop** nadat ze financiële gegevens hadden gedeeld.

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



N = 2164

Wat deed je met dit gevoel?



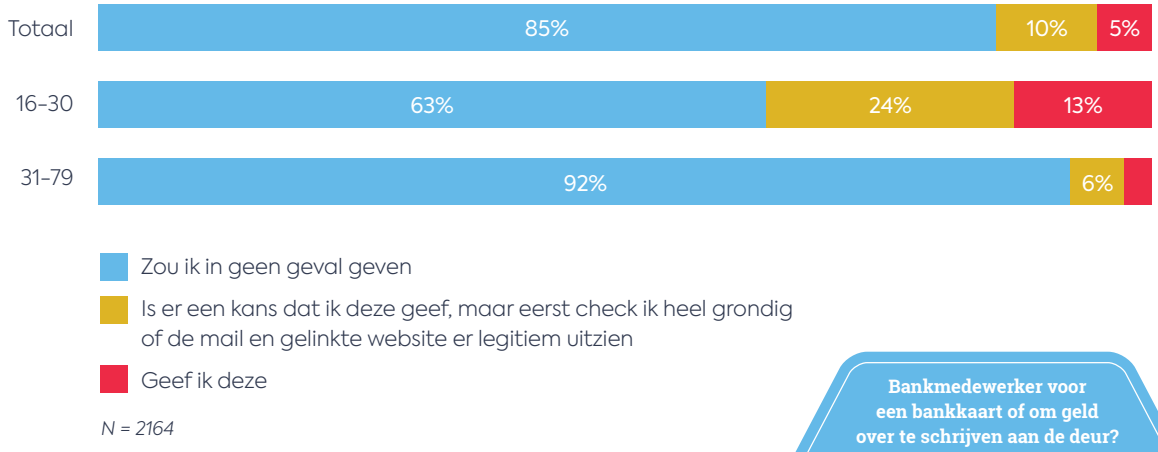
N = 607

Je bankcodes alsjeblieft

5%
van de bevolking geeft zonder aarzelen zijn bankcodes door.

En toch zijn er ook mensen die zonder aarzelen hun bankcodes zouden doorgeven als hun bank erom zou vragen. Dat gaat om 5% van de bevolking. Bij jongeren tussen de 16 en 30 jaar stijgt dit zelf naar 13%, wat bijzonder verontrustend is. **Jouw bank zal nooit naar jouw geheime codes vragen**. Let op: wanneer een zogenaamde 'bankmedewerker' dit wel doet, want dan heb je een fraudeur aan de lijn!

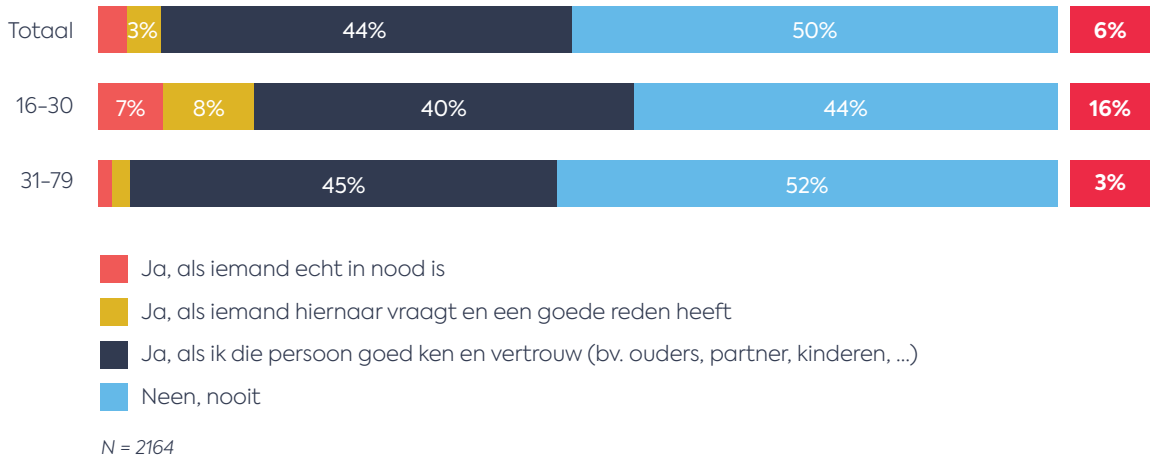
Als je bank via e-mail, sms, whatsapp, telefoon ... naar mijn bankcodes vraagt ...



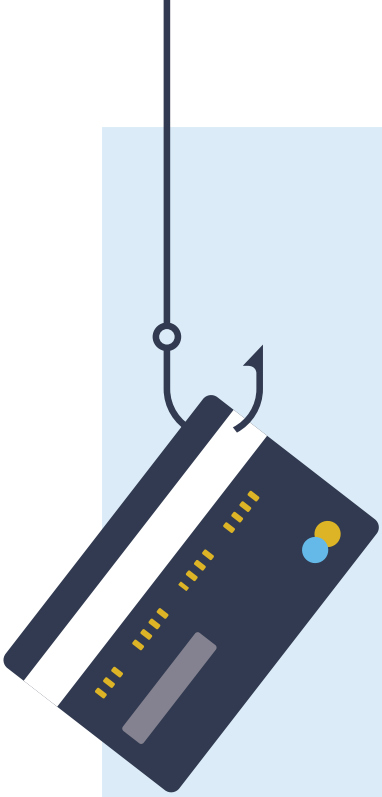
N = 2164

Ook bij bankkaart-phishing en bankkaart-phishing aan huis merken we een toename. **6%** van de Belgische bevolking (tegenover 3% in 2021) zou hun **bankkaart mét pincode afgeven aan iemand die ze niet kennen. Ook hier stijgt het percentage bij jongeren naar 16%**.

Zou jij je bankkaart en pincode afgeven aan iemand anders?



N = 2164



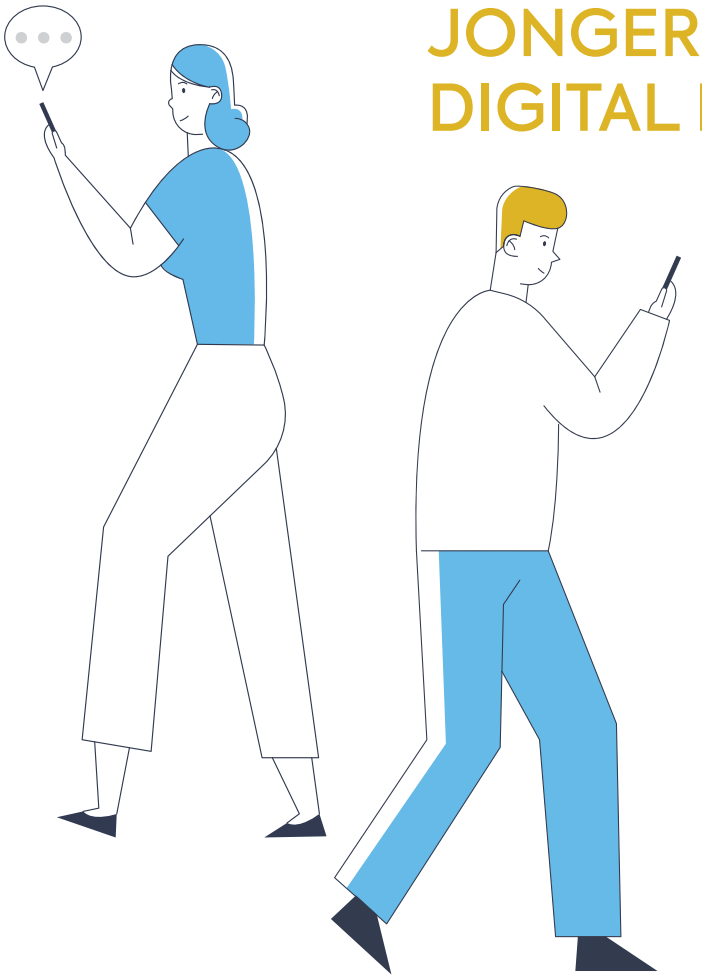
WAT IS BANKKAART-PHISHING?

Fraudeurs proberen rechtstreeks je **bankkaart en bijhorende codes** te pakken te krijgen. Hun modus operandi?

- Je ontvangt een e-mail of sms van je 'bank' waarin staat dat je debetkaart vervangen moet worden. Je moet je oude debetkaart zogezegd terugsturen om ze te recycleren en de nieuwe kaart krijg je daarna toegestuurd.
- Via de link in de e-mail of de sms kom je terecht op de valse website. Daarna vragen de fraudeurs je om:
  - Je persoonlijke gegevens en je kaartnummer in te vullen;
  - Je huidige pincode in te geven en een nieuwe pincode te kiezen;
  - Je huidige debetkaart op te sturen met de post.

Bij bankkaart-phishing aan huis komen oplichters bij je thuis als 'bankier' en helpen jou om in te loggen in je online bankomgeving. Op die manier kunnen ze natuurlijk meekijken en je codes zien. De fraudeurs vragen ook naar je bankkaart en nemen deze mee.

ONTHOUD!
Je bank zal nooit tot bij thuis komen om je kaart op te halen. Je bank zal ook nooit vragen om je bankkaart op te sturen of om je pincode te delen. Ga hier niet op in!



JONGEREN: MULTITASKENDE DIGITAL NATIVES?

Helaas behalen jongeren de slechtste scores in dit onderzoek: al te vaak leeft er de veronderstelling dat jongeren die opgegroeid zijn in dit digitale tijdperk, ook goed op de hoogte zijn van online bankieren en veiligheid. Ze mogen dan wel handig overweg kunnen met allerhande digitale snufjes en mee zijn met de nieuwste online trends, het onderzoek stelt vast dat ze van online veiligheid veel minder kaas hebben gegeten.

Uit de Digitale Inclusiebarometer van de Koning Boudewijn Stichting (KBS)[3] blijkt dat bijna één op de drie jongeren tussen 16 en 24 jaar (33%) zwakke algemene digitale vaardigheden heeft. De idee van de multitaskende digital natives? Die klopt dus niet helemaal.
Uit de KBS-studie blijkt ook dat 97% van de jongeren een smartphone ter beschikking heeft. Dit maakt hen extra kwetsbaar, want vaak trappen we gemakkelijker in de val wanneer we 'druk' bezig zijn op onze mobiel.

[3] Barometer Digitale Inclusie 2022

Te los met online veiligheid van bankgegevens

25%

van de ondervraagde jongeren deelden de afgelopen 6 maanden financiële gegevens waar ze zich ongemakkelijk bij voelden.

Een groot deel van de jongeren gaat namelijk te los om met online veiligheid. Zo kwamen er uit het onderzoek enkele verontrustende cijfers naar voren: van de ondervraagde jongeren tussen 16-30 jaar, deelde maar liefst 25% in de laatste 6 maanden financiële gegevens waar bij ze zich eigenlijk ongemakkelijk voelden. Dat is niet alleen een serieuze stijging tegenover 2021, toen het over 17% ging, het ligt ook een **stuk hoger dan bij volwassenen** (11%).

Ook zou 16% van de ondervraagde jongeren zonder twijfelen **zomaar hun bankcodes doorgeven als hun 'bank' hierachter vraagt**. Dit is een heel negatieve evolutie: in 2021 was dit 8% van de ondervraagde jongeren.

Zou jij je bankkaart en pincode afgeven aan iemand anders?

Ja, als iemand echt in nood is
Ja, als iemand hiernaar vraagt en een goede reden heeft
Ja, als ik die persoon goed ken en vertrouw (bv. ouders, partner, kinderen, ...)
Neen, nooit

N = 2164

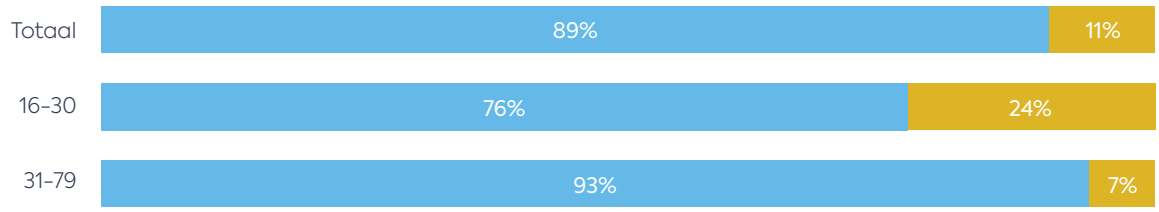
1 op 4 jongeren kent de term 'phishing' niet

24%

van de jongeren heeft nog nooit gehoord van phishing.

En dat is een groot probleem. Want door die algemeen zwakke digitale vaardigheden, zijn jongeren ook kwetsbaarder wanneer zij in contact komen met phishing. Onder jongeren heeft 24% nog nooit gehoord van phishing. Dit is wel een lichte verbetering, want in 2021 had 30% nog nooit van phishing gehoord.

Heb jij al gehoord van phishing?



Ja
Neen

N = 2164

JONGEREN ALS GELDEZELS

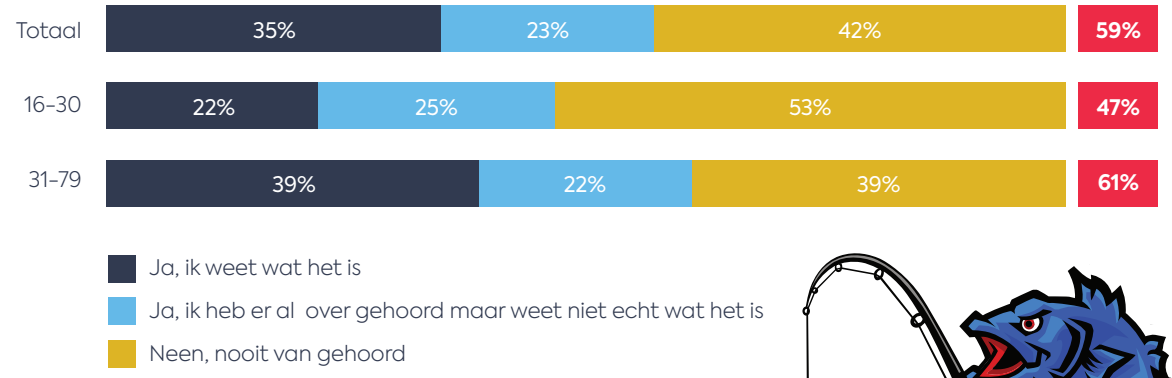
78%

van de jongeren weet niet wat een geldezel is.

Dit gebrek aan bewustzijn bij jongeren en het belang van online veiligheid, maakt jongeren ook vatbaarder om **geldezel t**e worden. **16%** van de jongeren zou hun **bankkaart uitlenen** aan iemand die ze niet kennen in ruil voor geld. Een slechtere score dan vorig jaar, toen dit om 9% ging. Iemand die dit doet, wordt een geldezel en dat is strafbaar.

Het probleem is dat heel weinig jongeren weten wat een geldezel is. Bijna **8 op 10** jongeren heeft geen idee. Amper **22%** wist wat een geldezel is, en zelfs dan zijn ze zich weinig bewust van de gevaren die hiermee gepaard gaan.

Weet jij wat een geldezel is?



Toch is het fenomeen geen ver-van-mijn-bed-show meer: de criminelen ronselen jongeren aan de schoolpoort, in het uitgaansleven of de stations-buurt maar ook online. En het is iets wat zich allang niet enkel meer afspeelt in een grootstad: **10%** van de ondervraagde jongeren is **zelf ooit benaderd** geweest om geldezel te worden. In 2021 was dit nog 6%. Van de jongeren kende 13% iemand die ooit werd benaderd om geldezel te worden.

Oplichters worden bovendien steeds creatiever in geld witwassen en de manieren waarop ze geldezels gebruiken. Het blijft niet enkel meer bij vragen naar de bankkaart en pincode: er wordt ook steeds meer naar (een kopie van) identiteitskaarten, gsm-nummers en adresgegevens gevraagd. Want ook deze info kan het voor criminelen makkelijker maken om fraude te plegen.

WAT IS EEN GELDEZEL?

Een geldezel stelt zijn/haar bankrekening en/of bankkaart en codes ter beschikking van criminelen. Criminelen gebruiken geldezels om **illegaal verkregen geld** (bv. van phishing) **door te sluizen** en **zelf in handen** te krijgen. De criminelen beloven geldezels dat ze snel en makkelijk geld kunnen verdienen, in ruil voor het uitlenen van hun bankrekening en/of bankkaart en pincode.

Is een geldezel worden strafbaar?

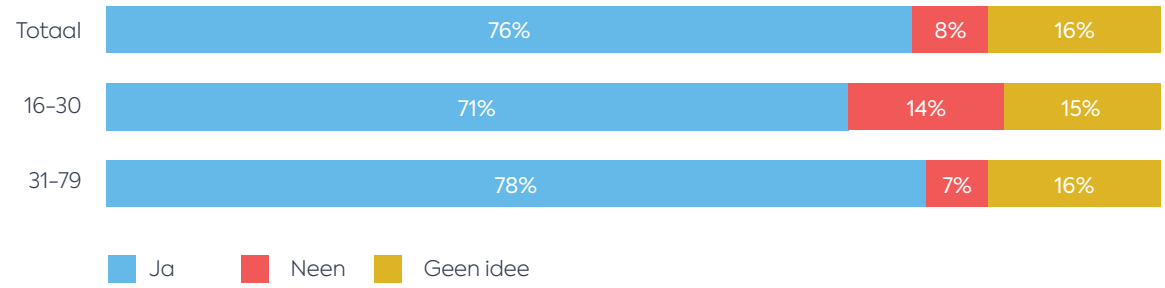
14%

van de ondervraagde jongeren denkt dat geldezel worden geen strafbaar feit is.

14% van de ondervraagde jongeren denkt dat geldezel worden, geen strafbaar feit is. Fout gedacht: door je bankkaart en codes uit te lenen, werk je mee aan het witwassen van geld en dat is wel degelijk een strafbaar feit. De gevolgen zijn vaak niet mals:

- Een geldezel kan aansprakelijk gesteld en vervolgd worden en riskeert zo grote gerechtelijke en fiscale boetes, of zelfs een celstraf.
- een veroordeling zal ook een impact hebben op de toekomstige bankrelatie.
- Bovendien riskeert de geldezel dat de phisher ook zijn/haar rekening plundert.

Denk je dat de geldezel zelf risico loopt?



BANKEN EN DE STRIJD TEGEN FRAUDE

ENKELE FRAUDEFACTS

- Vorig jaar kwamen er **47,917** meldingen over fraude of oplichting binnen bij het meldpunt van de FOD economie.
- Dat is gemiddeld **131** meldingen per dag.
- Meer dan de helft hiervan hield verband met **phishing** of **valse websites**.
- Het gaat om het op één na grootste aantal ooit, na het uitzonderlijke coronajaar 2020 met meer dan 55.000 meldingen. Sinds de start van het meldpunt in 2016 gaat het om een verdubbeling.

Online bankieren is enorm populair: het merendeel van de mensen (**91%**) verkiest om **online betalingen** uit te voeren, en dat aantal zal blijven toenemen. Online veiligheid is dan ook een topprioriteit voor de Belgische banken.

De banken doen heel wat om veilige banksystemen te garanderen en de klant in staat te stellen om hun transacties veilig uit te voeren:

- Online bankieren gebeurt altijd via een **beveiligde verbinding**.
- Om toegang te krijgen tot de online bankdiensten, moet je je altijd **identificeren** en je identiteit steeds dubbel bevestigen.
- Betalingsopdrachten moeten altijd **digitaal** worden **ondertekend**. Met deze digitale handtekening stem je in met de uitvoering van de betalingsopdracht.
- Je wordt **automatisch uitgelogd** van online bankieren als er geen activiteit heeft plaatsgevonden binnen een bepaald tijdsbestek.
- Bij de banken zijn er **beveiligingsexperts** die de door cybercriminelen gebruikte technieken voortdurend monitoren en analyseren om de beveiligingsmaatregelen aan te passen.

- Banken monitoren de transacties om verdachte patronen op te sporen. Als de bank een **verdachte betalingsopdracht** opmerkt, verwerkt zij die niet onmiddellijk. Zij voert eerst een aantal aanvullende controles uit. In het kader daarvan kan zij rechtstreeks contact opnemen met de klant om de betalingsopdracht te bevestigen. Zo wordt 75% van alle frauduleuze overschrijvingen via phishing opgespoord of teruggevorderd.

Er zijn dus verschillende veiligheidsmechanismen in werking. Maar we weten ook dat een kwart (26%) van de Belgen deze maatregelen en stappen, zoals de tweestapsauthentificatie, eerder overbodig vindt. Bij jongeren is dit nog hoger (38%). Een groot deel van de mensen vindt die maatregelen dus eerder een belemmering. En dat is zowel een interessant als een verontrustend gegeven, omdat die maatregelen er in de eerste plaats zijn om de veiligheid van de consument te garanderen. De banken moeten in dit opzicht een constante evenwichtsoefening maken:

- De banken willen vlotte betalingen garanderen en het gebruiksgemak voor de consument zo groot mogelijk houden
- Tegelijkertijd willen ze natuurlijk voldoende veiligheid garanderen, en willen ze frauduleuze transacties proberen te blokkeren en terug te vorderen, die vaak toch correct zijn ondertekend omdat er codes werden doorgegeven. Dit vergt van de banksector voortdurende investeringen en inzet van personeel en infrastructuur.

WAT IS 'TWEESTAPSAUTHENTIFICATIE'?

Om toegang te krijgen tot je rekening moet je bewijzen dat je bent wie je beweert te zijn. Dat kan op 3 manieren of met 3 factoren:

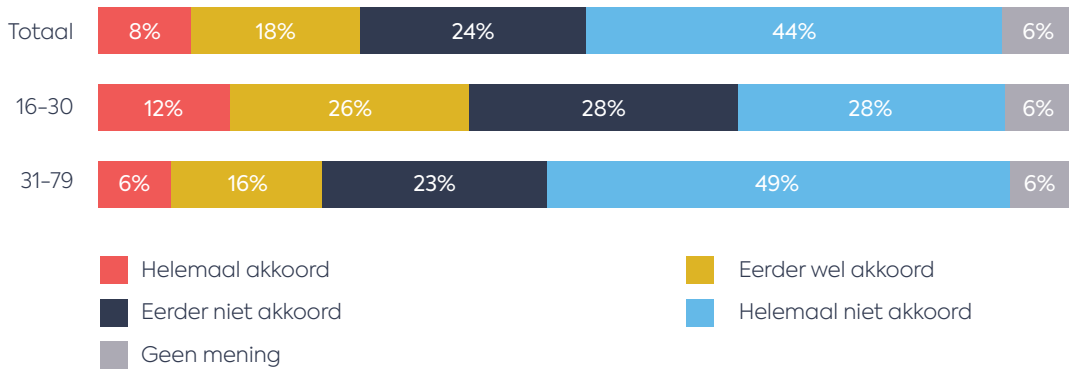
met iets dat jij alleen ***weet*** *(jouw wachtwoord of pincode)*

met iets dat jij alleen ***hebt*** *(jouw telefoon of token)*

met iets dat jij alleen ***bent*** *(jouw vingerafdruk, gelaat, iris ...)*

Meestal gebruik je één van deze factoren, vaak een wachtwoord, om te bewijzen wie je bent, maar het is beter om 2 of meer factoren te gebruiken: dit is twee- of meerstapsauthentificatie (2FA of MFA). Je gebruikt dan bv. een wachtwoord en je laat daar bovenop ook een code naar je GSM sturen, of je gebruikt je vingerafdruk en een app om toegang te krijgen.

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



N = 2164

SENSIBILISERING BLIJFT EEN MUST

Uit de Digitale Inclusiebarometer van de KBS blijkt dat het niveau van de algemene digitale vaardigheden bij de Belgen nauwelijks stijgt. **Sensibilisering rond online veiligheid en digitale vaardigheden is en blijft dus meer dan nodig**. Veel mensen geven ook aan dat ze graag meer willen weten over hoe men veilig kan online bankieren. 50% van de ondervraagden in de IndiVille studie geven aan interesse te hebben in een dergelijke opleiding.

Digitale vaardigheden onderhouden

Digitale vaardigheden zijn natuurlijk geen vaardigheden die je voor eens en altijd verwerft, en moet je goed onderhouden. De aard van digitale vaardigheden beweegt mee met de veranderingen en vernieuwingen in de samenleving en de introductie van nieuwe online toepassingen. Het is dus belangrijk om steeds goed bij te blijven en waakzaam te zijn.

Wanneer heb je goede digitale vaardigheden op vlak van cybersecurity?

- Kan je nagaan of een website beveiligd is (via URL, veiligheidscertificaten enz.)?
- Kan jij documenten lezen en begrijpen, en acties uitvoeren op een webpagina die het verzamelen van jouw persoonsgegevens kan beperken? Dit gaat dan over privacybeleid, beperkt prijsgeven van de locatie, beperkte toegang tot de inhoud van een persoonlijk profiel, weigeren van het laten inzamelen van data voor reclamedoeleinden), etc.
- Kan jij de instellingen van een browser aanpassen om zo de cookies te beperken die aangemaakt worden?
- Kan je fraudevormen herkennen en rinkelt er een belletje als men vraagt om persoonlijke codes door te geven?

Deze digitale skills zijn een belangrijk onderdeel om je blijvend te kunnen wapenen tegen phishing en andere fraudevormen.

Bescherm jezelf tegen online fraude

Je kan jezelf op heel wat manieren beschermen tegen phishing. De vuistregel is: klik nooit zomaar op een link. We zijn vaak druk en haastig bezig op onze smartphone, en dan even snel klikken op een link in een bericht of bij het installeren van een app, is niet altijd verstandig!

Een campagne die de banksector mee ondersteunt, is die van het CCB: ontdek 'OK is niet altijd Ok' hier. Blijf je graag geïnformeerd over de meest recente cyberdreigingen? Installeer dan zeker ook de Safeonweb app. Die werd al meer dan 180.000 gedownload en houdt je succesvol op de hoogte van frauduleuze berichten die in de omloop zijn.

TIP! Krijg jij een melding van je pc of smartphone dat er een update klaarstaat? **Installeer die dan**. Een update bevat vaak verbeteringen aan de kwetsbaarheden in jouw toestel. **Hoe update je nu juist jouw toestel?** Je leest er meer over op SafeOnWeb: **Doe regelmatig updates** (safeonweb.be)

Download alleen van erkende app stores

Meer tips op safeonweb.be

Febelfin sensibiliseert

De banksector heeft zeker een belangrijke rol te spelen in de sensibilisering rond online veiligheid. Febelfin zet dan ook enorm in op sensibilisering: naast jaarlijkse campagnes en samenwerkingen met een groot netwerk van partners, gaven enthousiaste Febelfin collega's dit jaar doorheen heel Vlaanderen en Wallonië **meer dan 50 infosessies en webinars over veilig digitaal bankieren en betalen**.

Omdat de vraag naar infosessies rond dit thema groot is, werkt Febelfin momenteel aan een gratis e-learning die uitgaat van het "train the trainer" principe, en die kan dienen als **referentiewerk** voor professionelen en vrijwilligers die werken rond online veiligheid. Voltooi je de e-learning, dan behaal je ook het bijhorende certificaat. De e-learning focust op:

- De meest relevante en actuele fraudevormen
- Overzicht van alle bestaande tools en sensibiliseringsmateriaal
- Guidelines voor het omgaan met digistarters
- Tips en tricks om veilig te bankieren
- Mogelijkheid om vragen te stellen aan Febelfin experten.

Voor meer info hierrond kan je altijd terecht bij info@febelfin.be. Naast de infosessies, stelt Febelfin ook heel wat **gratis campagne- en sensibiliseringsmateriaal** ter beschikking rond de verschillende fraudevormen: van **posters en stickers tot infobrochures**, voor elk wat wils. Febelfin kan hiervoor de bronbestanden aanleveren zodat het logo van jouw organisatie er ook bij kan vermeld worden.

Fraude is overal, ook daar waar je kind zit

Phishing, online fraude en de zoektocht naar geld-ezels gebeurt vaak achter de schermen. Letterlijk dan. Op TikTok of Instagram bijvoorbeeld. Kanalen waar enkel jongeren te vinden zijn en ze net het kwetsbaarst zijn. Want ouders zitten meestal niet op deze apps en zien dus niet altijd wat jongeren te zien krijgen. Op sociale mediakanalen worden kinderen constant verleid door aanlokkelijke voorstellen en worden vaardigheden op vlak van e-veiligheid constant op de proef gesteld . Daar moeten we ons van bewust zijn. Wat als we een online probleem, offline brengen? En zichtbaar maken wat voor ouders vaak onzichtbaar is. Febelfin ontwikkelde in deze context een nieuwe campagne gericht op jongeren maar vooral ook voor ouders. Zodat zij online fraude mee kennen, herkennen en zoon of dochter kunnen inlichten.

Met een outdoor-campagne die start met een gigantisch billboard aan de Brusselse beurs met louche reclame op. We mikken op PR en gezonde verontwaardiging van iedereen die het ziet. Ga je naar de link, dan krijg je deze boodschap te zien: “Dit is wat je kind online te zien krijgt. Help ze online fraude herkennen op beschermjezelfonline.be”. Daarbij wordt een social media campagne gelanceerd met testimonials.

Wil je meer hierrond weten of het campagne-materiaal gebruiken, neem dan contact met info@febelfin.be

SAMENWERKING IS KEY

Toch is deze sensibilisering niet enkel een taak voor de banksector alleen. De strijd tegen fraude is een gedeelde verantwoordelijkheid die pas echt ten volle voor verandering kan zorgen als verschillende sectoren samenwerken. Want de grootste katalysators van fraude bevinden zich allang niet meer enkel in de banksector, maar hebben zich ook naar andere sectoren uitgebreid.

Fraude is een maatschappelijk fenomeen. Alle sectoren in de samenleving moeten dus samen hun verantwoordelijkheid opnemen in deze strijd, denk maar aan de telecom en de online handelsplatformen. En alleen samen kunnen we de fraude zoveel mogelijk een halt proberen toe te roepen. Er is nog veel ruimte voor meer samenwerking op verschillende niveaus.

Veilige betalingen zijn een gedeelde verantwoordelijkheid: de banksector zorgt voor een veilige digitale infrastructuur, de klant is geïnformeerd en waakzaam, de politie en het parket vervolgen de misdaad en de overheid voorziet het juiste wettelijke kader. Als we deze balans in evenwicht kunnen houden, valt de schade te beperken. Samen maken we het verschil in de strijd tegen fraude, want elk schadegeval is er één te veel.

febelfin

Belgische Federatie van de financiële sector

www.febelfin.be