There is plenty of ‘phish’ in the sea

Fraude en oplichting in de banksector

febelfin

2020: te veel ‘phishers’ in de zee

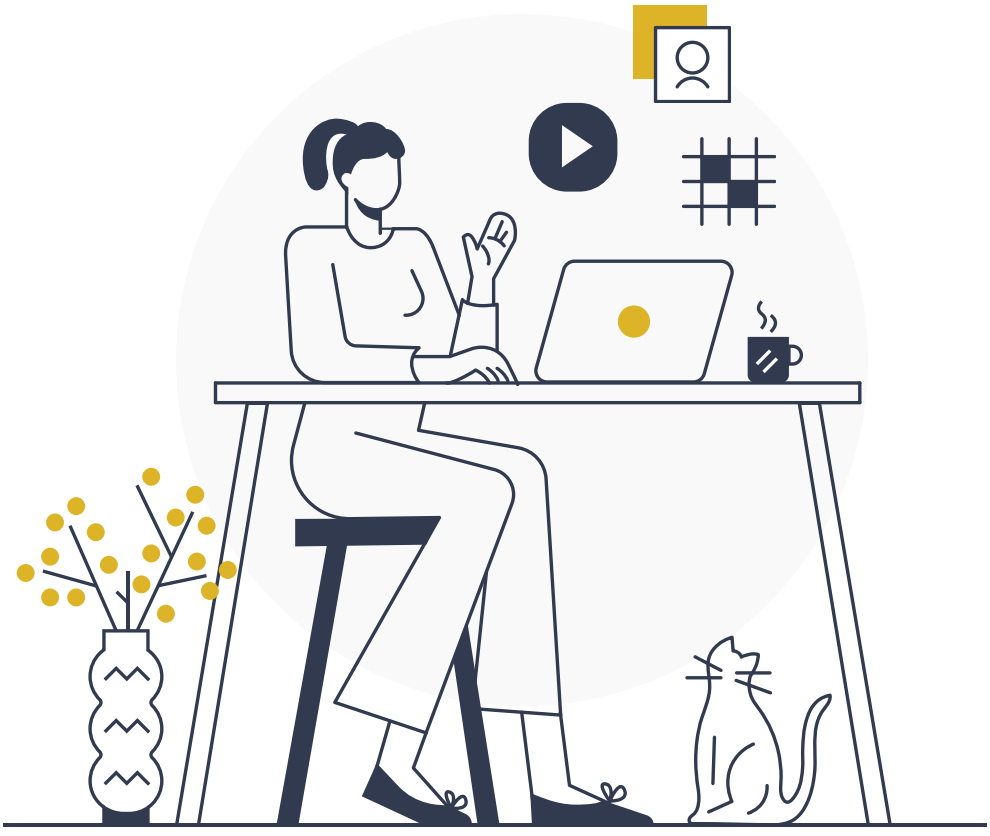
2020 was een jaar van ongekende uitdagingen: de pandemie veranderde ons dagelijks leven op een ingrijpende manier en de lockdown-maatregelen hadden een aanzienlijke impact op de economie. Terwijl gezinnen en bedrijven het moeilijk hadden, hebben de criminele bendes hieruit munt weten te slaan door hun fraudepraktijken snel aan te passen aan onze veranderende levensstijl. Het gaat onder meer om oplichting die inspeelt op de emotie en angst van de mensen voor de pandemie, waarbij fraudeurs zich voordoen als medewerkers van betrouwbare organisaties zoals gezondheids-organisaties of overheidsdiensten en banken. Coronagerelateerde berichten (bijvoorbeeld over mondmaskers, beloofde premies, ...) trokken de aandacht en hierdoor werd de ‘klikkans’ groter.

Internetgebruikers hebben in 2020 exact 3.225.234 berichten doorgestuurd naar het e-mailadres verdacht@safeonweb.be. Dagelijks waren er dat meer dan 8.800, of bijna het dubbele dan een jaar eerder (1,7 miljoen meldingen). *bron: CCB*

Criminelen spelen ook in op de toename van online winkelen en thuiswerk door zich voor te doen als pakketbezorgers, e-commerceplatformen of netwerkproviders. Daarnaast rekruteren criminelen “geldezels” om gestolen geld wit te wassen door valse advertenties op jobsites en sociale media te plaatsen, gericht op mensen die werk zoeken of tijdens de pandemie gemakkelijk geld willen verdienen.

In 2020 detecteerde Safeonweb 667.356 frauduleuze links. *bron: CCB*

De frauduleuze praktijken worden steeds gesofisticeerder en fraudeurs gebruiken technologie en het internet om hun aanpak nog overtuigender te maken. Dit heeft geleid tot een continue stijging van fraude, waarbij mensen worden overtuigd om zelf geld over te maken naar een crimineel. Denk maar aan kluisrekeningfraude of hulpvraagfraude, twee fraudetechnieken die vorig jaar zijn doorgebroken.



ENKELE INTERESSANTE WEETJES

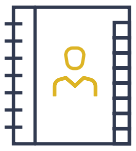
Fraudeurs richten zich liever en vaker op **mensen** dan op systemen. Kijk je naar de geslaagde fraudegevallen van de voorbije jaren, dan is dat de constante. Het is voor cybercriminelen dan ook de meest eenvoudige strategie. Waarom zouden ze complexe firewalls en antivirussystemen onder vuur nemen als er een makkelijker pad te bewandelen is? 9 op de 10 succesvolle data breaches worden veroorzaakt door menselijke fouten. 'People don't think, they click', blijft in 2020 nog altijd razend actueel.

Phishers hoeven niet te zoeken naar 'zwakke' profielen: ongeacht leeftijd, taal, geslacht, opleiding, ... iedereen kan slachtoffer worden van phishing.

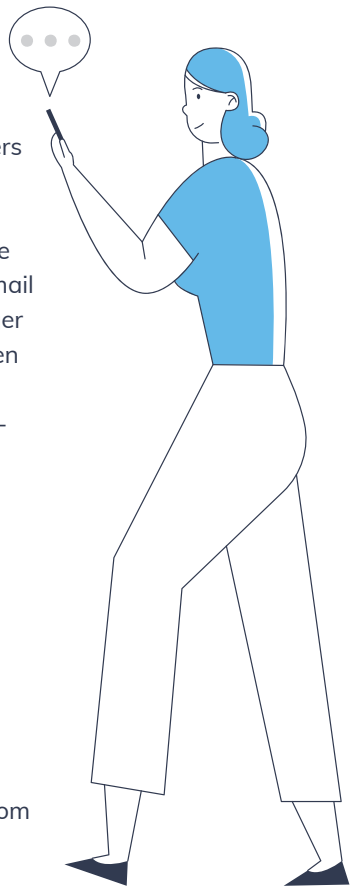
Hoe **korter** en meer to the point de inhoud van de mail is, hoe groter de kans dat de ontvanger de kwaadaardige URL of bijlage gaat openen. Zeker wanneer de ontvanger gevraagd wordt om even te helpen. Voor cybercriminelen is het met phishingmails geen kwestie van rocket science of diepgaande epistels: het is gewoon de juiste vraag op het juiste moment stellen. En hups... Mensen willen maar al te graag helpen, en vullen gegevens in.

Fraudeurs spelen bovendien graag in op de **actualiteit**: Ook al is het nieuwsfeit verzonnen of bij de haren getrokken: mensen willen het nieuws als eerste weten en reageren dan te snel. Het zijn niet enkel nieuwsberichten die scoren. Overheidsnieuws of bedrijfsnieuws scoort evenzeer.

Fraudeurs nemen helaas **geen vakantie**: terwijl de meesten vaak wat gas terug nemen tijdens de vakantiemaanden, steken fraudeurs net een tandje bij.



Wanneer een vals bericht afkomstig is van iemand die de ontvanger kent (of denkt te kennen), dan klikt maar liefst 30% op een link. Hoe meer vooronderzoek (door de fraudeur) en hoe persoonlijker de inhoud, hoe groter de kans dus dat ontvangers toehappen.



Fragiel via **mobiel**: ontvangers zijn het meest vatbaar voor phishing wanneer ze die openen op hun mobiel. Op de smartphone leest men een mail vluchtiger en klikt men vlugger op een link. Doorgaans is men ook bezig met andere zaken zoals het volgen van een TV-programma.

Donderdag is phishingdag: dan heb je het meeste kans om 'gephished' te worden.

Bron: Whitepaper Phished

2020: Een jaar uitgebeeld in fraude en oplichting

JANUARI - FEBRUARI

Bankkaart-phishing via brief (stuur je doorgeknipte bankkaart op en geef je pincode)

VANAF MAART

(Start corona compensatie via mail, sms)

- Hulpvraagfraude via WhatsApp
- Kluisrekeningfraude
- Fraude via sms CardStop, ITSME
- Phishingmail van FOD Financiën (terugbetaling belastingen, FOD Economie: vraag hier uw coronapremie aan)

SEPTEMBER

- Kluisrekeningfraude

OKTOBER

- Phishing Bpost pakje
- Smishing Card Stop sms

NOVEMBER

- WhatsApp fraude
- Phishing kaartlezer updaten
- Black Friday en Cyber Monday: jaarlijks phishingfeest loopt uit de hand

DECEMBER

- Phishing Bpost pakje
- Smishing Card Stop sms
- Bankkaart-phishing" via brief (stuur je doorgeknipte bankkaart op en geef je pincode)

Meer informatie over bovenstaande vormen van fraude is terug te vinden op: **www.febelfin.be**

FRAUDE EN OPLICHTING: TOPPRIORITEIT VAN DE BANKSECTOR IN 2021

In 2020 hebben we een enorme opmars gezien van alle vormen van online fraude, en dus ook van phishing. Bij phishing geven slachtoffers hun persoonlijke bankcodes door aan fraudeurs – meestal door te klikken op een link die leidt naar een frauduleuze website – zodat zij in naam van het slachtoffer transacties kunnen uitvoeren. Uit onze statistiek blijkt dat in 2020 ongeveer 67 000 frauduleuze transacties via phishing hebben plaatsgevonden, voor een totaal nettobedrag van ongeveer 34 miljoen euro. Helaas stopt fraude niet bij de overgang naar een nieuw jaar. Alle signalen wijzen op een verderzetting van deze stijgende trend in 2021.

Ook de bevindingen uit een recente studie van Febelfin (maart 2021) in samenwerking met het onderzoeksbureau IndiVille1 baren zorgen:

34% **van de bevolking** heeft in de **afgelopen maand een phishingbericht gekregen**. In totaal kreeg 56% het afgelopen halfjaar een dergelijk bericht. Dit toont de grote omvang van het probleem. Je moet continu alert zijn voor fraude.

'Phishing' is nog **onvoldoende bekend bij de Belg. 12%** van de bevolking heeft **nog nooit gehoord van phishing**.

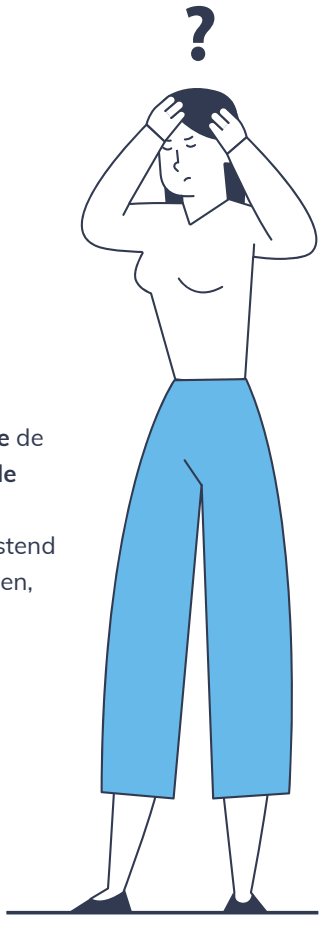
30% van de **jongeren** (16- 30 jaar) heeft **nog nooit van phishing gehoord**.

3% **van wie ooit een phishingbericht ontving, is hierop ingegaan.** Jongeren zijn kwetsbaarder, 5% ging in op het bericht.

26% **deelde ooit financiële gegevens** waarover men zich schuldig voelde. Vorig jaar was dit 23%.

7% van de Belgen **deelde** de **afgelopen 6 maanden financiële gegevens** waarover men zich ongemakkelijk voelde. Verontrustend is dat dit cijfer bij de 16-30 jarigen, 17% is.

3% **van de bevolking zou** zijn **bankcodes doorgeven als zijn bank daarom vraagt.** Dat 8% van de jongeren dit zou doen, is geen goed teken.



[1] *Enquête van Febelfin in samenwerking met IndiVille bij 2045 respondenten tussen 16 en 79 jaar, afgenomen tussen 3 – 5 maart 2021.*

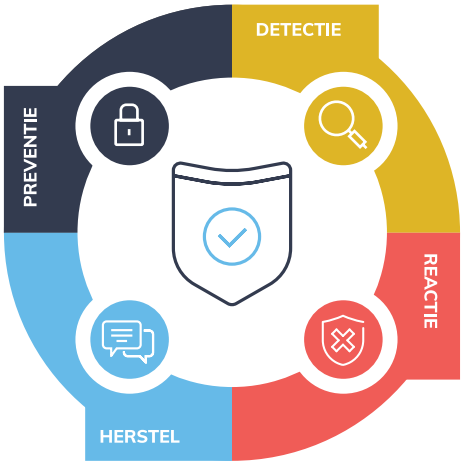
Bovendien blijkt uit cijfers van de meest recente **Unisys Security Index™** dat de bezorgdheid bij Belgen over cybercriminaliteit is afgenomen. En dat is verontrustend! Wereldwijd is de bezorgdheid over internetveiligheid met 7 punten gedaald (van 179 naar 172 punten) ten opzichte van vorig jaar. België volgt de algemene trend, maar hier daalt de bezorgdheid veel sterker (van 160 naar 141 punten). De Belgen zijn ook minder bezorgd over hacken en computervirussen, met maar 44% in vergelijking met 54% vorig jaar.

Genoeg redenen om aan te nemen dat blijvende acties en sensibilisering op dit vlak absoluut noodzakelijk zijn bij verschillende doelgroepen, zeker ook bij **jongeren**. De veronderstelling dat jongeren digitaal meer onderlegd zijn, lijkt niet op te gaan als het gaat over het kennen van de gevaren van online fraude. **Daarom beschouwt de banksector de bestrijding van fraude en oplichting als topprioriteit in 2021** en zal men verder blijven inzetten op **sensibiliseringscampagnes die zich richten op specifieke doelgroepen** en dit in **samenwerking met overheid en verschillende stakeholders**.

HOE GAAN BANKEN DE STRIJD AAN MET PHISHING?

Preventie:
- Authenticatie
- Sensibilisering van de klant

Herstel:
- Contact opnemen met betrokken banken
- En met handelaars



Detectie:
- Proactieve monitoring
- Vroegtijdige detectie via fraudelijn

Reactie:
- Websites blokkeren
- Fraudeonderzoek
- Aanpassen logica/procedures voor fraudedetectie
- Vals-positief percentage onder controle houden

Authenticatie & detectie

Banken hebben verschillende systemen ingebouwd om transacties veilig te laten verlopen en de fraude naar aanleiding van phishing zo veel mogelijk te voorkomen en/of in te dijken. Zo is er sinds een tiental jaar **tweestapsauthenticatie** vereist bij online en mobiel bankieren. De klant identificeert zichzelf aan de hand van twee elementen – een kaart of telefoon, een pincode, een vingerafdruk of een gezichtsscan – om e-betalingen te initiëren. De Belgische banksector was hierin koploper. De inzet van nieuwe biometrische technieken is iets om in de nabije toekomst naar uit te kijken.

De banken investeren daarenboven in intensieve monitoring en maken op die manier veel schade ongedaan. Deze inspanningen leveren opmerkelijke resultaten: meer dan 75% van alle frauduleuze overschrijvingen (waarvoor een gephishte responsecode werd gebruikt) wordt door de banken gedetecteerd en geblokkeerd of teruggevorderd. Ook artificiële intelligentie wordt door sommige banken al ingezet om fraude te detecteren.

Delicaat evenwicht tussen gebruiksgemak en veiligheid

Het garanderen van **vlot en snel betaalverkeer én efficiënte fraudedetectie is een moeilijk en delicaat evenwicht**. Het vergt **continue investeringen in personeel en infrastructuur** vanuit de banksector. Maar de **klant verwacht** ook **gebruiksgemak en snelle betalingen** (denk maar aan “instant payments” waarbij het geld binnen enkele seconden op de bankrekening staat). Een bank heeft tijd nodig om grondig onderzoek te doen als een anomalie wordt gedetecteerd. Elke fraudeteam heeft daarvoor zijn eigen regels en procedures. Veiligheid en gebruiksgemak op elkaar afstemmen brengt dan ook uitdagingen mee voor de sector. Het is een echte ‘balancing game’.

> **“33% van de Belgen vindt de veiligheidsstappen (bv. kaartnummer ingeven, kaartlezer bij de hand hebben) bij online aankopen overbodig. Zij ervaren dit eerder als een hindernis. Deze instelling baart zorgen want deze stappen worden net ingebouwd ter beveiliging van de consument”, aldus Karel Baert, CEO Febelfin.**

Blijven herhalen

Ook wordt volop ingezet op sensibiliseringsacties, waarbij de sector iedereen oproept om waakzaam te zijn voor phishing en online fraude. Campagnes met tips, zowel op sociale media als op tv en radio, bereikten een groot doelpubliek. Maar er is nog werk aan de winkel. Dat zien we aan het aantal fraudegevallen. Sensibiliseringsacties blijven dus noodzakelijk. Laten we samen de belangrijke boodschap om nooit je persoonlijke codes te delen (pincode en responsecode) zoveel mogelijk herhalen.

1 BOODSCHAP: GEEF NOOIT JE CODES EN KLIK NIET DOOR OP EEN LINK

De coronacrisis en de vele digitale contacten zijn voor fraudeurs een opportuniteit om mensen op te lichten. De verschillende vormen van phishing zijn talrijk en complex. Fraudeurs maken niet alleen gebruik van verschillende kanalen - zoals email, brief, telefoon, sms, sociale media en whatsapp - maar ze plegen de fraude ook in naam van verschillende organisaties en instellingen zoals banken, overheidsadministraties, telecomoperatoren, nutsbedrijven, enzovoort. De lijst is lang. Door de grote verscheidenheid aan kanalen is **iedereen potentieel slachtoffer**.

De vindingrijkheid van fraudeurs mag dan indrukwekkend zijn, phishing is nog altijd **eenvoudig te voorkomen**:

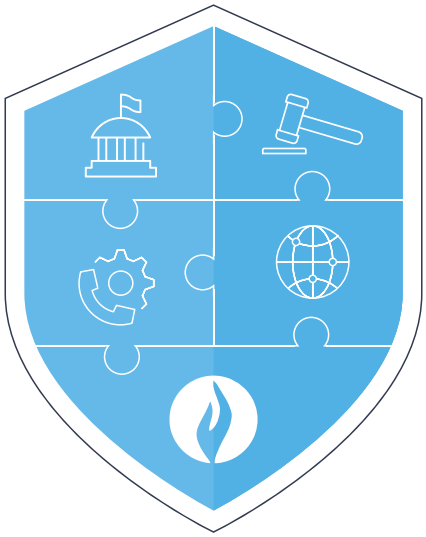
Geef nooit persoonlijke codes (pincode & response code) door naar aanleiding van een email, telefoongesprek, sms, sociale media of whatsappbericht.

Klik ook nooit op een ontvangen link, maar typ altijd zelf het adres van de gewenste bankwebsite in je browser of gebruik je eigen mobiele banking app. Alleen dan ben je zeker dat er niks aan de hand is.

Kortom: digitaal betalen en bankieren is en blijft veilig, zolang je je persoonlijke codes voor jezelf houdt en waakzaam blijft. Je geeft je portefeuille toch ook niet zomaar weg?

Nieuwe initiatieven

Het is van zeer groot belang om snel te kunnen ingrijpen, want het geld wordt vaak op korte tijd van de ene naar de andere bankrekening doorgesluisd, via geldezels. Daarom werd midden 2020 het zogenaamde "mule stop proces" ingevoerd opdat de bank van het slachtoffer efficiënt de bank van de geldezel kan vragen om het overgeschreven fraudebedrag te blokkeren.



Gezien de aard van het probleem zijn er niet alleen technische werkgroepen met financiële experten die onderling informatie uitwisselen om zoveel mogelijk fraude te detecteren, maar maakt de sector ook werk van samenwerkingsverbanden met andere stakeholders. Zo lopen er initiatieven in samenwerking met telecomoperatoren, internetproviders, parket, politie, overheidsinstanties en justitie om phishing in al zijn dimensies en verschijningsvormen aan te pakken en de sensibiliseringsboodschap zo breed mogelijk te verspreiden. Deze samenwerkingsverbanden moeten in de toekomst nog meer op een gestructureerde en geautomatiseerde manier gebeuren. Dit zal in grote mate bijdragen tot de snelheid waarmee men kan ingrijpen bij de detectie en het tegenhouden van fraude.

Vast staat dat de bereidheid vanuit de banksector heel groot is.

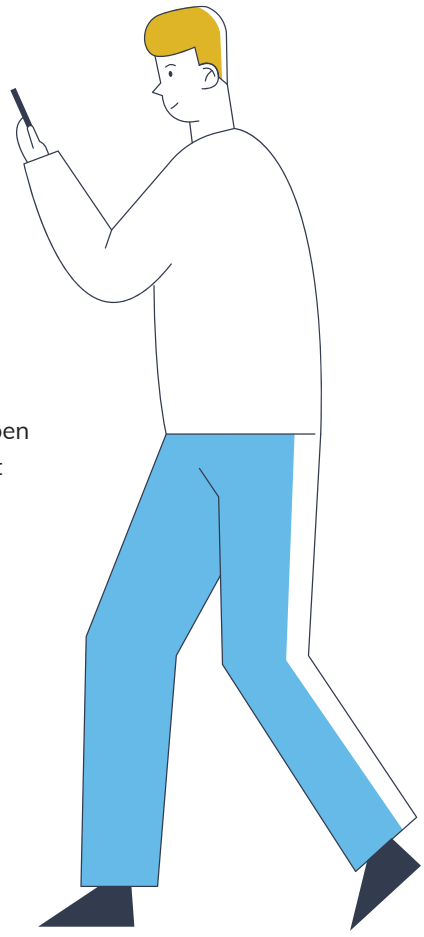
Momenteel is het nog niet mogelijk om persoonsgegevens inzake fraude uit te wisselen omwille van (privacy)wetgeving. Banken blijven op dit vlak zeer voorzichtig omdat zij door de toezichthouders en wetgeving aan zeer strikte reglementering gebonden zijn.

Febelfin onderzoekt de mogelijkheid om op wettelijke basis een systeem op te richten voor het uitwisselen van identiteitsgegevens van *money mules* tussen financiële instellingen.

Kan wetenschap een oplossing bieden?

Hoe komt het dat mensen blijven klikken op links of ingaan of andere vormen van fraude? Volgens de gedragswetenschap valt dit te verklaren doordat ons brein op dat moment overschakelt op 'fast thinking' en we niet meer rationeel gaan denken. Fraudeurs spelen handig in op enkele mechanismen die op dat moment optreden:

- **Loss aversion:** angst om te verliezen
- **Social influence:** verandering in houding of gedrag veroorzaakt door externe druk, reëel of ingebeeld
- **Unrealistic optimism:** we denken altijd dat phishing ons niet zal overkomen
- **Discounting:** mensen staan altijd zeer receptief tegenover grote kortingen of gelimiteerde oplages
- **Availability heuristic:** soort snelkoppeling met directe voorbeelden in ons geheugen



Diezelfde mechanismen kunnen echter gebruikt worden om gedragstechnieken te ontwikkelen waarbij mensen subtiel gestimuleerd worden om zich op een bepaalde wijze te gedragen, ook wel aangeduid met de term *nudging*. Op dit ogenblik zijn er nog niet veel wetenschappelijke experimenten ontwikkeld waarbij nudging wordt ingezet om phishing te beperken. In de UK en Nederland is men reeds de eerste stappen op dit vlak aan het zetten. Febelfin volgt dit nauw op en wil dit graag verder onderzoeken.

Altijd bij de les blijven

Onze 'huisacademie' Febelfin Academy heeft een breed pallet aan opleidingen uitgewerkt naar alle 'doelgroepen' toe binnen de financiële instelling – van commerciële medewerker naar product expert tot bestuurder. Dit zorgt ervoor dat iedereen binnen de sector bij de les blijft. Febelfin Academy werkt hier nauw samen met zowel de business (experten uit financiële instellingen) als internationale docenten en organisaties (vb. IMF).

Hieronder een greep uit hun aanbod:

- Algemene awareness naar alle medewerkers van financiële instellingen : e-learning vertrekkende vanuit concrete situaties met oefeningen en simulaties, zowel privé als professioneel.

  Cyber security: Do's & Don'ts (eng) - e-learning

- Opleiding tot experten in fraude/cyber : gevorderde opleidingen met certificatie

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

  Traject Certified Fraud Examiner (CFE) - in samenwerking met IMF

- Opleidingen voor product managers in kader van payments : PSD2 en SCA

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

- Risk management: cybersecurity is duidelijk één van de belangrijkste nieuwe risico's voor onze leden en komt prominent aan bod in de cursussen risk management – en zeker nu in coronatijden – met als doelgroep risk en compliance managers.

  CoVID 19: New challenges in Risk Management - Live Webinar

  Masterclass in Risk Management

- Board effectiveness: executive program voor board members met focus op de cyber risico's en hoe hiermee omgaan als bestuurder – welke vragen hierbij stellen om zich te wapenen tegen cyber risico.

  Executive program - The Board of Directors in the Financial Sector

EEN GROOT VISNET IS NODIG

De banksector loopt echter tegen de **grenzen** aan van wat zij alleen kan doen. De afgelopen jaren hebben we gezien dat de grootste katalysators van fraude zich buiten de banksector naar andere sectoren hebben verplaatst, een trend die alleen maar is toegenomen door de COVID-19-pandemie. Criminelen omzeilen steeds vaker de geavanceerde beveiligingssystemen van banken.
We moeten er echter ook voor zorgen dat deze fraude een halt wordt toegeroepen.

Phishing is geen probleem van de banksector alleen, maar is een **maatschappelijk fenomeen**. We bevinden ons op een kantelpunt. **Alle sectoren** moeten 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 doorgedreven samenwerking, niet alleen sectoraal maar ook cross border.

De linken tussen fraude, georganiseerde criminaliteit en terrorisme vormen een belangrijke en toenemende bedreiging voor de nationale veiligheid. De betrokken criminele bendes gebruiken de opbrengsten van fraude om andere schadelijke en illegale activiteiten te financieren en veroorzaken daarmee onnoemelijk leed en schade aan onze samenleving. Daarom is het ook cruciaal dat de overheid zijn verantwoordelijkheid opneemt in deze problematiek en bekijkt hoe men een aangepast wetgevend kader kan creëren. Er moeten ook voldoende middelen en capaciteit worden vrijmaakt zodat politionele diensten hun werk kunnen doen en zij de criminele bendes aan de top kunnen opdoeken.

In de strijd tegen cyberfraude is iedereen betrokken partij. Veilig betalen is een gedeelde verantwoordelijkheid: de banksector zorgt voor een veilige digitale infrastructuur, de klant is geïnformeerd en alert, 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. **Alleen samen kunnen we deze strijd winnen, want elk schadegeval is er één te veel.**

febelfin

Belgische Federatie van de financiële sector

www.febelfin.be