Stijging schade als gevolg van digitale fraude maakt gezamenlijke aanpak noodzakelijk

NIEUWS

17 november 2021

De totale schade als gevolg van phishing (6,1 miljoen euro) en bankhelpdeskfraude (16,5 miljoen euro) kwam in de eerste zes maanden van 2021 uit op ruim 22,5 miljoen euro. Ter vergelijking: de totale schade van deze fraudevormen bedroeg in heel 2020 39,5 miljoen euro. De schade door fraude en oplichting in het betalingsverkeer loopt daarmee verder op naar een zorgwekkend hoog niveau. Banken willen daarom vaart maken om samen met de overheid en andere betrokken partijen te komen tot een integrale aanpak om digitale fraude te bestrijden.

Door extra beveiligingsmaatregelen en omdat er door Corona minder fysieke betalingen plaatsvonden nam de schade van meer traditionele fraude met credit cards en gestolen bankpassen sterk af. Zo halveerde de schade van fraude met credit cards naar ruim een miljoen euro en daalde de schade door gestolen bankpassen met 68% naar 940.000 euro.

Bij phishing werd de schade voor 98% van het schadebedrag vergoed door de bank. In 2020 besloten banken om de schade door bankhelpdeskfraude uit coulance te vergoeden, omdat bij nummerspoofing misbruik wordt gemaakt van het vertrouwen van klanten in hun bank. Omdat klanten hier ook een eigen

verantwoordelijkheid houden, hebben banken **toetsingscriteria** opgesteld om te bepalen in hoeverre de schade wordt vergoed. In de eerste zes maanden van 2021 werd 92% van de schade door bankheldpdeskfraude vergoed.

Digitalisering biedt veel gemak en nieuwe mogelijkheden maar heeft ook een keerzijde. De toename van digitale criminaliteit vormt een breed maatschappelijk probleem. Hiertegen kan alleen in gezamenlijkheid, dus met medewerking van alle betrokken publieke en private partijen, een vuist worden gemaakt. Banken pleiten daarom al langer voor een integrale aanpak, waarbij zij onder andere met de verantwoordelijke ministeries, toezichthouders, politie, Openbaar Ministerie, sociale media, BigTech's, Internet Service Providers, telecompartijen en handelsplatformen de handen ineenslaan. Ook de Cyber Security Raad heeft **opgeroepen** tot actie en investeringen om de trend van toenemende digitale fraude te keren. Verder uitstel betekent meer schade voor slachtoffers en grotere winsten voor criminelen.

In afwachting van zo'n gezamenlijke aanpak blijven banken er alles aan doen om het betalingsverkeer veilig te houden. Dat is nodig want criminelen bedenken steeds slimmere oplichtingsmethoden. Voorbeelden zijn de IBAN-Naam Check (naam-nummercontrole), de mogelijkheid om betaallimieten in te stellen, de tweefactor authenticatie en de zogenoemde «gelijk oversteken»-service, die klanten van een online marktplaats kunnen inzetten om hun transacties veilig te laten verlopen. Daarnaast bestaan er vele voor de buitenwereld onzichtbare mechanismen die consumenten beschermen tegen fraude en oplichting. Banken werken met verschillende fraudedetectiesystemen om fraudeleuze transacties op te sporen en te onderzoeken. Ook waarschuwen banken hun klanten permanent in het directe contact (bijvoorbeeld via de app) en door **campagnes** op social media, radio en TV. Daarbij hebben banken speciale aandacht voor kwetsbare groepen zoals senioren en jongeren.