feiten & cijfers

25% Een kwart van de panelleden zegt niet goed op de hoogte te zijn van de uniforme veiligheidsvoorschriften.

5 Er zijn 5 uniforme veiligheidsvoorschriften voor veilig bankieren en betalen, zie **veiligbankieren.nl**

*'Ik ontving een betaalverzoek van een "vriendin" via Facebook. Ik kreeg mijn schade niet vergoed. Volgens Deutsche Bank was het een kwestie van **eigen schuld, dikke bult**.'*

975 In de eerste 4 maanden van 2019 kreeg de Fraudehelpdesk 975 meldingen over valse sms'jes. In heel 2018 waren dat er **303**.

'De bank gaat er te makkelijk van uit dat iedereen alles snapt.'

€3,81 MILJOEN

De schade door phishing bij internetbankieren is toegenomen van €1,05 miljoen in 2017 naar €3,81 miljoen in 2018.

50% De helft van de panelleden vindt het steeds lastiger om phishing-mails te herkennen.

'Ik hoefde alleen nog de mobiele betaling van de koper te accepteren door een QR-code te scannen, maar zo verkreeg de fraudeur volledige toegang tot mijn bankrekening.'

1 tot 1,5% Volgens het CBS heeft in 2018 naar schatting 1 tot 1,5% van de internetgebruikers daadwerkelijk geld verloren door phishing.

'Een fraudeur deed op één ochtend 21 aankopen bij iTunes, waardoor er ruim €2100 via mijn creditcard werd afgeschreven.'

1 OP 6 Van de ruim 11.000 panelleden hebben 1845 (een) poging(en) tot fraude of oplichting meegemaakt.

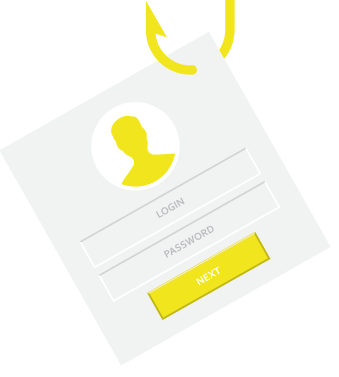
*'Toen ik de oplichters appte dat ik aangifte had gedaan, kreeg ik als antwoord: **succes ermee**'.*

De Consumentenbond vroeg ruim 11.000 panelleden naar hun ervaringen met bankfraude.

Criminelen blijven vissen

Phishing en smishing zijn een regelrechte plaag. Wie de oude en nieuwe trucs van criminelen te laat doorziet, krijgt niet altijd de schade vergoed.

TEKST INGRID ZUURMOND



Wat?

➜ Nieuwe trucs via sms, WhatsApp en sociale media om geld af te troggelen en codes te ontfutselen

EEN OP DE ZES MENSEN kreeg in 2018 of 2019 te maken met bankfraude of een poging daartoe. Dat blijkt uit een onderzoek van de Consumentenbond onder meer dan 11.000 panelleden. De grootste plagen zijn pas-opstuur-fraude en phishing via de telefoon, e-mails en sms'jes.
Bij phishing hengelen criminelen naar persoonlijke gegevens, zoals inlogcodes voor internetbankieren. Bij pas-opstuur-fraude krijg je bijvoorbeeld een bericht waarin staat dat de bank een nieuw type betaalpas invoert en je de huidige pas moet opsturen. Hiermee kan de fraudeur vervolgens pinnen. De pincode is al eerder ergens afgekeken. Of je wordt ertoe verleid je pincode op een vervalste website van de bank in te voeren.

Taxirit in Rusland

Bij 276 panelleden (ruim 2%) is daadwerkelijk geld afhandig gemaakt. Dit gebeurde relatief vaak door misbruik van internetbankier- en creditcardgegevens. 'Mijn creditcard werd gekoppeld aan een iTunes-account van een fraudeur', meldt een panellid. 'Die deed op één ochtend 21 aankopen bij iTunes, waardoor er ruim €2100 via mijn creditcard werd afgeschreven. Ik kreeg een sms'je dat mijn maximale bestedingsruimte bijna was bereikt, terwijl ik zelf helemaal geen betalingen met mijn creditcard had gedaan.'
Twee andere consumenten geven aan dat oplichters hun creditcardgegevens hadden gebruikt om een Uber-taxirit af te rekenen. Bij het ene panellid gebeurde dat in Mexico, bij de ander in Rusland. Beiden kregen hun schade volledig vergoed, net als de meeste andere panelleden die slachtoffer waren van creditcardfraude. Er waren 49 gedupeerden die niets terugkregen, ook niet na een klacht bij de bank.
CBS-cijfers laten een vergelijkbaar beeld zien. In 2018 waren bijna 700.000 internetgebruikers van 12 jaar en ouder (4,6%) slachtoffer van een vermogensdelict (fraude waarbij de dader geld opstrijkt). Oplichting bij onlinehandel – vooral betalen voor een nooit geleverd(e) product of dienst kwam het meest voor, namelijk bij 2,7% van de internetgebruikers. Ongeveer 100.000 mensen (0,7%) waren slachtoffer van oplichting via het betalingsverkeer. De dader kreeg dan in de meeste gevallen toegang tot de bankrekening, vooral door phishing en hacken. Nog eens 175.000 mensen (1,2%) verloren geld via een andere manier van online fraude, bijvoorbeeld door nepboetes en -facturen.

Minder taalfouten

Volgens Betaalvereniging Nederland is de totale schade door betaalfraude in 2018 licht gedaald ten opzichte van 2017. Maar de schade door phishing bij internetbankieren is toegenomen. De brancheverenigingwijt dat ondere andere aan de verbeterde kwaliteit van valse e-mails en websites. Ze bevatten minder taalfouten en het taalgebruik is overtuigender en persoonlijker dan voorheen. Bovendien worden berichten niet meer alleen via e-mail, maar ook via sms, WhatsApp en sociale media als Facebook verstuurd.
Volgens Betaalvereniging Nederland proberen fraudeurs nu ook via phishing beveiligingscodes te bemachtigen. Hiermee kunnen ze de mobielbankieren-app op

➜

een smartphone installeren. Die app is dan gekoppeld aan de rekening van het slachtoffer.
Een van onze panelleden kreeg met deze vorm van fraude te maken. Hij bood iets te koop aan op Marktplaats en werd via WhatsApp benaderd door een potentiële koper. 'We kwamen een bedrag overeen, waarna ik hem een betaalverzoek stuurde. De volgende dag stond het bedrag niet op mijn rekening. Volgens de koper was het bij hem al afgeschreven. Ik hoefde alleen nog de betaling te accepteren via een QR-code. Hij stuurde die naar mijn andere telefoon, zodat ik die met mijn ING-app kon scannen. Op die telefoon kwam een WhatsApp-videogesprek binnen, waarbij in een flits de QR-code in beeld kwam en onmiddellijk weer verdween. Mijn scanner had de code echter opgepikt. Dit alles ging razendsnel. Achteraf bleek dat de fraudeur zo volledig toegang had verkregen tot mijn rekening, waarna ook spaargeld werd overgeboekt naar lopende rekeningen.' De schade was bijna €4500. ING vergoedde pas na druk vanuit de media.
Ook een ander panellid liet zich 'om de tuin leiden door mooie praatjes' en koppelde de smartphone van de fraudeur aan zijn ING-rekening. De bank vergoedde geen cent van de schade van €5000, omdat het panellid 'vrijwillig' toegang tot zijn rekening had gegeven. Betaalvereniging Nederland geeft aan dat zij in de loop van 2019 meer meldingen over dit soort fraude heeft ontvangen.

Consumentenbond: het Kifid gaat te snel mee in de redenering dat klanten 'grof nalatig' zijn geweest

Appje van dochter

Een nieuwe vorm van phishing is het versturen van persoonlijke berichten van 'bekenden'. Zo kreeg een panellid zogenaamd een app-berichtje van haar dochter. 'Ze vroeg of ik voor haar een betaling van €790 wilde doen. Toen ik dat gedaan had, kwam er nog een appje met een soortgelijk verzoek voor een andere rekening. Toen ze voor de derde keer zo'n vraag stuurde, bekroop mij een gevoel van twijfel. En ja hoor, mijn dochter wist van niets. Toen ik de oplichters appte dat ik aangifte had gedaan, antwoordden die "succes ermee". Politie en bank (ING) konden er niets mee en ik ben dus €1500 kwijt.'
Iemand anders had een soortgelijke ervaring. 'Mijn zoon zat in Jordanië. Volgens het appberichtje moest hij met spoed rekeningen betalen en was er een storing bij de bank. Tot twee keer toe. Het kwam allemaal zo waarheidsgetrouw over, dat ik pas bij de derde keer argwaan kreeg. Ik herkende zijn telefoonnummer niet, maar hij had een nieuwe smartphone met een ander nummer.' Dit panellid maakte in totaal ruim €5000 over en heeft €1902 van ING teruggekregen.
Een persoonlijk betaalverzoek kan ook via sociale media komen. Een panellid kreeg zo'n verzoek van een vriendin via Facebook. Achteraf bleek dat het account gehackt was, maar dat merkte het panellid pas toen het al te laat was. Volgens Deutsche Bank was het een kwestie van 'eigen schuld, dikke bult'.

Grof nalatig

Consumenten krijgen hun schade niet vergoed als zij 'grof nalatig' zijn geweest. Tot 2014 hadden banken allemaal eigen veiligheidsregels. Nu ben je in ieder geval niet grof nalatig als je je aan vijf uniforme veiligheidsvoorschriften houdt. Heb je een regel overtreden, dan ben je niet meteen schuldig. De bank kijkt eerst naar de omstandigheden en bepaalt per geval of er sprake is van grove nalatigheid.
Een van de vijf regels luidt dat je je beveiligingscodes, zoals de pincode en toegangscodes voor bankieren, geheimhoudt. Maar bij veel trucs heeft het slachtoffer niet in de gaten dat hij zijn gegevens deelt. Toch is hij volgens de bank dan soms grof nalatig. Het verschilt per bank en situatie wanneer dat het geval is.
Bij Microsoft-fraude blijft de consument vaak met lege handen achter. Bij deze vorm van fraude belt een zogenaamde medewerker van Microsoft je op om een computerprobleem op te lossen. Je moet dan vaak een programma op je computer downloaden, zodat de medewerker kan 'meekijken' en – zonder dat je het doorhebt – het bedrag kan verhogen of bank- of creditcardgegevens kan stelen. Meerdere slachtoffers die de schade niet vergoed kregen, stapten naar klachteninstituut Kifid. In alle zaken oordeelde de geschillencommissie dat de slachtoffers grof nalatig waren geweest, omdat zij belangrijke

SLACHTOFFER GEWORDEN?

- Blokkeer je rekening en doe aangifte bij de politie.
- Vraag de bank om schadevergoeding. Laat zien dat je je aan de vijf veiligheidsvoorschriften hebt gehouden.
- Kom je er niet uit? Dien schriftelijk een klacht in bij je bank.
- Is je klacht niet naar tevredenheid afgehandeld of krijg je geen reactie? Dan kun je binnen een bepaalde termijn naar het Kifid, zie kifid.nl.
- Kijk of je beroep kunt doen op 'bijzondere omstandigheden', zoals een grote hoeveelheid afschrijvingen in een korte periode die de bank had kunnen opmerken.

inloggegevens niet hadden beschermd. Het Kifid maakte eenmaal een uitzondering: op één dag waren er 119 identieke betalingsopdrachten gedaan. Omdat de bank bekend was met de fraudevorm, had zij eerder maatregelen kunnen treffen tegen de grote hoeveelheid identieke betalingsopdrachten. Deze klant kreeg daarom 60% van de schade vergoed.
Een aantal panelleden maakte Microsoft-oplichting mee. Een Rabobankklant kreeg de schade (€4300) volledig van zijn bank vergoed.

Standpunt Consumentenbond

Het vergoedingsbeleid van de banken is duidelijk inconsistent. De Digitaalgids van de Consumentenbond merkte dat ook bij helpdeskfraude (zie consumentenbond.nl/nepklantenservice). Bij deze fraudevorm bel je zelf per ongeluk naar een nephelpdesk, die dan dezelfde truc uithaalt als de nep-Microsoft-medewerker. Bij een aantal gedupeerden vergoedde Rabobank de schade wel, ING niet.
Ook een aantal panelleden maakte helpdeskfraude mee. Opnieuw kreeg een klant van Rabobank de schade volledig vergoed, terwijl twee anderen, beiden klant van ING, hun schade van €200 en €2500 niet vergoed kregen. De Consumentenbond heeft er bij ING op aangedrongen helpdeskfraude standaard te vergoeden, maar kreeg nul op rekest.
Banken informeren consumenten via campagnes en hun websites over de nieuwste trucs. ‘Maar banken gaan er te makkelijk van uit dat iedereen alles snapt’, merkt een panellid op. ‘Ze bedenken steeds nieuwe producten waarop de consument niet zit te wachten en die fraude in de hand werken.’
Fraudeurs spelen vaak slim in op veranderingen die de bank doorvoert. Meerdere ondervraagden ontvingen bijvoorbeeld een e-mail over de afschaffing van TAN-codes door ING. Nadat een van hen op een link klikte en enkele gegevens invulde, werd er €2000 van zijn bankrekening gehaald. Gelukkig vergoedde ING in dit voorbeeld het volledige schadebedrag.

De Consumentenbond vindt dat banken niet van klanten mogen eisen dat ze constant op de hoogte zijn van de nieuwste trucs van criminelen. De uniforme veiligheidsregels van de banken houden geen rekening met de nieuwste vormen van fraude. Klanten hebben vaak niet eens in de gaten dat ze hun gegevens delen. In een uitspraak gaf het Kifid de bank gelijk dat de klant op de hoogte had kunnen zijn van het bestaan van Microsoft-fraude via de website van de bank. De Consumentenbond vindt echter dat de bank bij nieuwere vormen van fraude niet te snel naar dit argument mag grijpen. ●

MEER INFORMATIE

Kijk voor meer trucs op consumentenbond.nl/oplichtingstrucs. Ga voor tips en de vijf uniforme veiligheidsvoorschriften naar consumentenbond.nl/veiligbankieren

SMISHING

Smishing, oftewel phishing via sms, is in opkomst. Volgens Betaalvereniging Nederland is het aantal meldingen van valse bank-sms’jes in september meer dan verdubbeld ten opzichte van januari 2019. Bij smishing vraagt ‘de bank’ je om via een link in te loggen, omdat anders je rekening wordt geblokkeerd of je betaalpas vervalt. Op deze manier proberen fraudeurs je inloggegevens te bemachtigen. Overigens worden bij smishing niet alleen berichten ‘namens de bank’ verstuurd. Ook de Belastingdienst, het CJIB, zorgverzekeraars en pakketbezorgers worden gebruikt voor de truc.

Consumenten bond

Laat je niets wijsmaken

Met de onafhankelijke tips en adviezen uit de Geldgids maak je zelf de juiste financiële keuzes. Probeer nu met korting.

Bekijk de aanbieding