Jij hebt de sleutel

Informatieblad

ABN·AMRO

Inleiding

In het huidige digitale tijdperk is geld overboeken een kwestie van één druk op de knop: het resultaat verschijnt direct op het scherm. Maar achter deze schijnbare eenvoud schuilt een complex systeem van beveiliging. De eerdere whitepaper ***'De bank als jouw kluis'*** (Mei 2025) gaf inzicht in hoe digitale veiligheid wordt geborgd. Daarbij werd uitgelegd hoe wet- en regelgeving, in samenhang met technologie, bijdraagt aan de bescherming van klantgegevens en financiële privacy. De nadruk lag op hoe de bank jouw geld beschermt: Hoe zorgt een bank ervoor dat alleen jij toegang hebt tot jouw eigen geld?

In dit informatieblad *'Jij hebt de sleutel'*, een uitbreiding van de whitepaper *'De bank als jouw kluis'*, belichten we wat het voor jou betekent dat alleen jij toegang hebt tot jouw eigen geld. Digitale beveiligingssystemen van banken zijn van een zeer hoog niveau, daarom komt de aandacht van criminelen in toenemende mate te liggen op de rol van de klant zelf als essentiële schakel, de feitelijke 'sleutel' voor toegang tot het geld. Het is daarom belangrijk dat deze sleutel goed beschermd wordt.

Criminelen proberen klanten op verschillende manieren te misleiden. Dit gebeurt bijvoorbeeld via valse e-mails, sms-berichten of telefoongesprekken waarbij zij zich voordoen als de bank, met als doel persoonlijke gegevens of inlogcodes te verkrijgen. Ook komt het voor dat klanten onder druk worden gezet of op slinkse wijze worden bewogen om zelf toegang tot hun rekening te verlenen. Het is daarom belangrijk om goed op de hoogte te zijn van de manieren waarop fraudeurs jouw sleutel proberen te bemachtigen, om je hier goed tegen te kunnen wapenen.

Verschuiving van bank naar individu

Fraude heeft in de loop der jaren een duidelijke verschuiving doorgemaakt. Waar criminelen zich vroeger vooral richtten op toegang tot de fysieke kluis in een bankfiliaal, richten ze zich nu op de 'digitale kluis'.

De digitale kluis van de bank is sterk beveiligd. Banken maken gebruik van geavanceerde technologieën en strikte veiligheidsprotocollen om ervoor te zorgen dat ongeautoriseerde toegang vrijwel onmogelijk is. Toch betekent dit niet dat er geen risico's zijn. Omdat de digitale systemen zelf zeer robuust zijn, verleggen fraudeurs nu vaker hun aandacht: zij proberen de sleutel te bemachtigen die toegang geeft tot de digitale kluis van het individu.

Jij hebt de sleutel!

Het kernpunt: *jij hebt de sleutel*. Als rekeninghouder ben jij de enige die toegang heeft tot jouw digitale kluis. Jij bepaalt wie de sleutel in handen krijgt en draagt daarmee ook de verantwoordelijkheid om te waarborgen dat deze uitsluitend bij jou blijft. Alleen zo blijven jouw geld en persoonlijke gegevens beschermd.

Hoe proberen fraudeurs toegang te krijgen tot jouw kluis?

Fraudeurs gebruiken uiteenlopende methoden om toegang te krijgen tot jouw digitale kluis. Daarbij gaan zij vaak stapsgewijs te werk: eerst verzamelen zij basisinformatie, waarna zij contact zoeken om extra gegevens te verkrijgen en zo de sleutel daadwerkelijk in handen te krijgen.

Informatie vergaren

De eerste stap voor fraudeurs is vaak het verzamelen van gegevens. Dit kan bijvoorbeeld via kwaadaardige software die persoonlijke informatie achterhaalt, of door het kopen van persoonlijke gegevens die via een hack of datalek beschikbaar zijn gekomen. Zo heeft in juli 2025 nog een incident plaatsgevonden waarbij de persoonlijke en medische gegevens van ruim 850.000 deelnemers aan het bevolkingsonderzoek baarmoederhalskanker zijn gestolen. Met deze gegevens kunnen fraudeurs zich overtuigend voordoen als een betrouwbare partij, waardoor de kans groter is dat jij in hun verhaal trapt.

Contact zoeken en verdere informatie vergaren

Op basis van de verzamelde gegevens, proberen fraudeurs rechtstreeks contact met jou te leggen, bijvoorbeeld via e-mail, telefoon of apps. Met technieken zoals *phishing* en *spoofing* doen zij zich voor als een vertrouwde organisatie, bijvoorbeeld als jouw bank zelf. Het doel is hier tweeledig: het eerste contact leggen om zo je vertrouwen te winnen én extra informatie verzamelen, zodat jij ongemerkt een deel van je sleutel prijsgeeft.

Om zo geloofwaardig mogelijk over te komen, gebruiken fraudeurs slimme methodes. Zo laten ze je door middel van specifieke vraagstellingen* geloven dat zij jouw bankgegevens in kunnen zien, of gebruiken ze jou onrechtmatig verkregen gegevens om zich voor te doen als een legitieme instantie.

*Voorbeeld: Een fraudeur vraagt: ‘Heb je de laatste dagen weleens geld overgemaakt?’ Als je dit bevestigt, reageert hij met: “Ja, dat zien we inderdaad in ons systeem.” In werkelijkheid heeft de fraudeur helemaal geen inzage in je gegevens, maar doordat je het bevestigt, kan hij doen alsof hij wél toegang heeft.

Wat is *phishing*?

Phishing is een manier waarop cybercriminelen 'vissen' naar toegangsinformatie op jouw computernetwerk. Bij phishing worden vaak valse e-mails gebruikt. Zo willen cybercriminelen je of jouw medewerkers laten klikken op een gevaarlijke link waardoor je op een website terechtkomt die van de bank lijkt te zijn, maar eigenlijk tot de fraudeurs toebehoort. Wanneer je inlogt, kunnen cybercriminelen toegang krijgen tot je computer en het netwerk. Vergelijkbare vormen van fraude zijn smishing (via SMS of WhatsApp) en quishing (via QR-codes). Wanneer wordt ingelogd, kunnen cybercriminelen toegang krijgen tot computers en netwerken. Vergelijkbare vormen van fraude zijn smishing (via SMS of WhatsApp) en quishing (via QR-codes). Bij smishing bevat het bericht een link naar een valse website. Bij quishing leidt de QR-code naar een andere website dan verwacht, waardoor criminelen persoonlijke gegevens kunnen buitmaken.

In het ‘Oplichtings ABC’ staat uitgelegd wat phishing, fraude met QR-codes en smishing is in makkelijke taal.

Wat is *spoofing*?

Spoofing is een fraudevorm waarbij criminelen de identiteit van een betrouwbare organisatie, zoals een bank, overheid of politie, vervalsen. Dit gebeurt vaak via telefoon of e-mail, waarbij de informatie van de afzender zoals een telefoonnummer of e-mailadres wordt gemanipuleerd. Wanneer je te maken krijgt met spoofing, krijg je een urgent bericht of telefoongesprek en wordt onder druk gezet om in te loggen op een nagemaakte website, persoonlijke gegevens te delen of een betaling te doen. De verkregen gegevens of gelden komen direct in handen van de fraudeurs. Spoofing maakt zo misbruik van vertrouwen in bekende namen en contactgegevens.

In het ‘Oplichtings ABC’ staat uitgelegd wat spoofing is in makkelijke taal.

Codes bemachtigen

Een belangrijk onderdeel van de sleutel tot jouw digitale kluis is tegenwoordig je mobiele telefoon. Fraudeurs proberen op verschillende manieren toegang te krijgen tot codes die via de telefoon worden ontvangen, zoals sms-codes of verificatiecodes uit apps.

Het risico beperkt zich niet tot digitale onderschepping: er bestaat ook een kans dat een fraudeur fysiek meekijkt wanneer jij je codes invoert, een methode die bekendstaat als ‘shouldering’. Door middel van deze codes kunnen fraudeurs makkelijker door de beveiliging van jouw digitale kluis breken.

Manipuleren en beroven

Fraudeurs zetten nu alles op alles om de volledige sleutel in handen te krijgen, en zo in te breken in jouw digitale kluis. Dit kan bijvoorbeeld gebeuren via de installatie van zogenoemde meekijksoftware, of doordat criminelen zich voordoen als bankmedewerkers bij zogeheten ‘bankhelpdeskfraude’. In beide gevallen proberen zij jou te misleiden of te manipuleren, zodat jij – vaak zonder het door te hebben – jouw sleutel toch uit handen geeft.

Vrijwel onzichtbaar

Waar fraudeurs vroeger te achterhalen waren door middel van vingerafdrukken, camerabeelden of ooggetuigen, zijn ze tegenwoordig niet zo makkelijk te traceren. Vandaag de dag zorgen fraudeurs ervoor dat ze nauwelijks sporen achterlaten, wanneer ze jouw kluis binnendringen. Dat maakt het moeilijk te achterhalen wie verantwoordelijk is en daardoor is het lastig om het verloren geld terug te krijgen. Dit maakt alertheid des te belangrijker.

Wat is shouldering?

Shouldering is een fraudevorm waarbij een fraudeur stiekem over de schouder meekijkt wanneer je een pincode of toegangscode intoetst. Oorspronkelijk kwam dit vooral voor bij betalingen met een betaalpas, maar tegenwoordig gebeurt het steeds vaker bij het invoeren van codes op smartphones, zoals bij mobiel bankieren- en betaalapps. Zodra de fraudeur je code heeft gezien en daarnaast de beschikking krijgt over jouw telefoon of betaalpas van het slachtoffer, kan hij of zij toegang krijgen tot bankrekeningen en andere persoonlijke diensten.

TIP: Een sterke toegangscode bestaat niet uit persoonlijke data of herhalende cijfers. Die code mag nooit gedeeld worden, ook niet met iemand die zich voordoet als de bank.

Digitale veiligheid begint bij eenvoudige concrete handelingen:

- Kies een unieke toegangscode voor smartphone én bankapp
- Wijzig de toegangscode regelmatig
- Zorg dat niemand kan meekijken bij het invoeren van codes
- Blokkeer de Mobiel Bankieren app onmiddellijk bij verlies of diefstal van het toestel

In het ‘Oplichtings ABC’ staat uitgelegd wat shouldering is in makkelijke taal.

Wat is meekijksoftware?

Meekijksoftware is een type kwaadaardige software dat, eenmaal geïnstalleerd op jouw computer, tablet of smartphone, een fraudeur direct toegang geeft tot alles wat je op jouw apparaat doet. Criminelen verkrijgen hiermee bijvoorbeeld inzicht in ingevoerde bankcodes, wachtwoorden of transacties. Installatie gebeurt vaak doordat je, bewust of onbewust, ingaat op een frauduleus verzoek om de software te downloaden. Vaak onder het voorwendsel dat dit nodig is voor ondersteuning of beveiliging. Zodra de meekijksoftware actief is, kan de fraudeur op afstand meekijken en zelfs handelingen overnemen, met grote risico’s voor de veiligheid van je bankgegevens en financiële transacties.

TIP: Het voorkomen van meekijksoftware vraagt om alertheid: denk altijd na voordat je iets installeert, houd je apparaten goed beveiligd en wees terughoudend bij onverwachte hulpvragen.

Wat is bankhelpdeskfraude?

Bankhelpdeskfraude is een oplichtingsvorm waarbij fraudeurs telefonisch contact met je opnemen en zich voordoen als medewerker van de bank. Hier krijg je te horen dat er een probleem is met je rekening of betalingen. Onder het mom van bescherming wordt er vervolgens gevraagd om geld over te maken naar een ‘veilige rekening’, persoonlijke codes te delen of toegang tot je computer te verlenen. In werkelijkheid worden deze instructies gebruikt om rechtstreeks geld of gegevens buit te maken. De beller is geen bankmedewerker maar een oplichter, en de zogenoemde veilige rekening is in handen van de fraudeur.

Twijfel je er aan of je wel echt met de bank praat? Vraag dan om de Gesprek Check. Dan stuurt de medewerker waar je mee belt jou een bericht in de ABN AMRO app of Internet Bankieren. Zo weet je zeker met wie je belt en kun je fraude voorkomen.

In het ‘Oplichtings ABC’ staat uitgelegd wat bankhelpdeskfraude is in makkelijke taal.

Tools om veilig te bankieren

Om je geld veilig te houden, biedt de bank verschillende tools die het fraudeurs moeilijker maken. Deze vijf veiligheidstools helpen je jezelf te beschermen tegen fraude: het Spaargeldslot aanzetten, je paslimiet en daglimiet instellen, pushberichten activeren en je betaalprofiel instellen.

Op deze pagina vind je meer uitleg over ***de 5 veiligheidstools*** en hoe je ze zelf inschakelt.

Fraudeurs richten hun pijlen steeds vaker op jou als klant. Niet omdat de systemen onveilig zijn, maar omdat zij weten dat de sleutel tot de digitale kluis bij jou als rekeninghouder ligt. Door in te spelen op emoties als angst, urgentie of vertrouwen proberen zij jou te verleiden om zelf de toegang uit handen te geven. Dit doen ze met slimme en bedachtzame methodes, waardoor je het niet altijd direct doorhebt.

De bank zorgt ervoor dat jouw geld veilig in jouw kluis wordt bewaard en je vrij kunt beschikken over jouw rekening. Uiteindelijk ben jij zelf degene die bepaalt wat er met je geld gebeurt. Omdat jij die toegang beheert, is het belangrijk bewust te zijn van hoe je deze deelt. Een fraudeur hoeft geen ingewikkelde systemen te kraken, zolang hij jou kan overtuigen om de deur zelf open te zetten. Jij hebt de sleutel.

Hoe kun jij je sleutel optimaal beschermen?
Lees er meer over in de whitepaper ***'De bank als jouw kluis' (Mei 2025)***