Veilig Bankieren
Alle tips

Over het herkennen van verschillende vormen van fraude en weet hoe je moet handelen als het jou overkomt.

Inhoud:

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank

Bankhelpdeskfraude

Bij bankhelpdeskfraude wordt iemand meestal uit het niets gebeld uit naam van de bank. Vervolgens wordt verteld dat de reken-ing niet meer veilig is. Om deze rekening weer veilig te krijgen moet er actie ondernomen worden. De oplichter probeert dit op verschillende manieren

1. Geld overmaken naar een zogenaamde ‘kluisrekening’.

Dit is vaak een rekening bij een andere bank of een rekening in het buitenland en hierbij gaat het meestal om een rekening op naam van een vreemde persoon/naam. De bank vraagt je nooit om een overboeking te doen en al helemaal niet naar een rekening op naam van een persoon.

2. Meekijken op de tablet, mobiele telefoon of computer.

De zogenaamde bankhelpdeskmedewerker zal je vragen om op afstand met je mee te kijken om zo jouw apparaat over te kunnen nemen. Dit is een vreemd verzoek, een echte medewerker van ASN Bank zal hier nooit om vragen. Daarna wordt er gevraagd om in te loggen in jouw bankomgeving. Hierdoor worden er uiteindelijk betalingen klaargezet of worden jouw bankgegevens onderschept.

3. Afgeven van bankproducten.

De oplichter komt bij je thuis langs om jouw bankproducten inclusief pincodes op te halen. Soms vragen ze daarbij ook om jouw mobiele telefoon, computer of sieraden mee te geven. De bank vraagt je nooit om jouw bankproducten en/of pincodes of andere goederen af te geven en komt ook niet bij je thuis om deze op te halen.of andere goederen af te geven en komt ook niet bij u thuis om deze op te halen.

Spoofing

Oplichters kunnen jou bellen met een vreemd telefoonnummer. Maar let op: Oplichters kunnen ook een nummer vervalsen, waardoor het lijkt alsof je wordt gebeld door het telefoonnummer van jouw bank. Dat is telefoonspoofi ng. Het kan dus zijn dat er “ASN Bank” staat, terwijl dit geen medewerker van ASN Bank is, doordat het nummer overgenomen (gespooft) is.

Hoe voorkom je dat je slachtoffer wordt van bankhelpdeskfraude?

Noteer de naam van degene die je spreekt en neem contact op met de ASN Klantenservice via 070 – 35 69 335 (24/7).
Het is ook verstandig om dit nummer op te slaan in je contacten. Twijfel je of er mogelijk sprake is van deze manier van oplichting? Neem dan direct contact op met de ASN Klantenservice via 070 – 35 69 335.

Banken vragen je nooit om:

1. Overboekingen te doen (ook niet naar een zogenaamde kluisrekening).
2. Jouw pincodes of beveiligingscodes te verstrekken.
3. Directe toegang tot jouw computer te krijgen.
4. Bankproducten en andere spullen mee te geven. Ook niet aan iemand die bij je aan de deur komt en zegt een bankmedewerker te zijn.

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank

Hulpvraagfraude

Dit gebeurt vaak via WhatsApp. Zij doen zich voor als een bekende van jou die in nood is. Vervolgens ontvang je een betaalverzoek of een bankrekeningnummer waar het bedrag naar overgemaakt kan worden. Met deze tips weet je hoe je hulpvraagfraude herkent en wat je het beste kunt doen als je ermee te maken krijgt.

Hoe herken je hulpvraagfraude?

- Een familielid of andere bekende heeft plotseling een nieuw nummer.
- Deze bekende vraagt je om vaak met spoed, geld over te maken.
- Het rekeningnummer dat ze doorgeven, ken je niet.
- De bekende zet je onder druk door te vertellen over de negatieve gevolgen wanneer het geld niet snel wordt overgemaakt.

Hoe voorkom je dat je wordt opgelicht?

- De belangrijkste tip: neem contact op met de bekende of het familielid op het oude, vertrouwde telefoonnummer dat je van diegene hebt.
- Niemand gesproken? Niets overmaken! Hoe meer druk diegene ondertussen uitoefent om toch snel geld over te maken, hoe groter de kans dat je inderdaad met een oplichtzer te maken hebt

Toch geld overgemaakt?

- Heb je geld overgemaakt en twijfel je achteraf of je misschien bent opgelicht? Bel ons dan meteen op 070 - 35 69 335 (24/7).
- Verzamel zoveel mogelijk bewijsmateriaal. Noteer het nummer waar het bericht vandaan komt, maak screenshots van het gesprek en noteer het bankrekeningnummer dat genoemd wordt.
- Doe aangifte bij de politie.
- Rapporteer het account bij de gebruikte berichtendienst (bijvoorbeeld WhatsApp).

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank

Verkoopplatformfraude

Wanneer je spullen koopt of verkoopt via verkoopplatformen zoals Marktplaats of Facebook Marketplace, bestaat het risico dat internetoplichters geld of het product van je proberen te stelen. Hierbij gebruiken ze verschillende tactieken. Met deze tips weet je hoe je deze fraudevorm herkent en wat je het beste kunt doen als je ermee te maken krijgt.

Hoe herken je verkoopplatformfraude?

- Je ontvangt een bod dat te mooi lijkt om waar te zijn of het bod is snel geplaatst nadat je het te koop hebt gezet.
- De (ver)koper vraagt om jouw identiteitsbewijs ter verificatie. Die kunnen ze later misbruiken voor identiteitsfraude.
- De (ver)koper wil jouw betaling en/of jouw identiteit controleren door 1 cent over te laten maken via een nep betaalverzoek.
- Hierna kom je op een nagemaakte betaalpagina uit. Als je alles hebt ingevuld, heeft de oplichter toegang gekregen tot jouw bankrekening.

Hoe voorkom je dat je wordt opgelicht?

- Maak gebruik van de chatfunctie en de betaalmogelijkheden van het verkoopplatform zelf. Dit is handiger en veiliger dan bijvoorbeeld via WhatsApp.
- Ga nooit in op verzoeken van particulieren om 1 cent over te maken. De oplichter zal je vragen om een klein bedrag over te boeken, zogenaamd ter controle. Maar onthoud: je hoeft nooit te betalen om geld te ontvangen.
- Haal een artikel dat je koopt zelf op en laat een artikel dat je wilt verkopen ophalen. Is dit niet mogelijk? Zorg er dan altijd voor dat je de betaling doet via het platform zelf.
- Controleer de betrouwbaarheid van de verkoper. Kijk bijvoorbeeld hoe lang de verkoper actief is op het platform, naar ervaringen en kijk bij zijn/haar andere advertenties.
- Stuur nooit een foto van jouw identiteitsbewijs, bankafschrift of betaalpas naar een (ver)koper als hij/zij daarom vraagt.

Toch geld overgemaakt?

- Heb je geld overgemaakt en twijfel je achteraf of je misschien bent opgelicht? Bel ons dan meteen op 070 - 35 69 335 (24/7).
- Verzamel zo veel mogelijk bewijsmateriaal, zoals screenshots van het gesprek, telefoonnummers en bankrekeningnummerslvan een betaalverzoek.
- Doe aangifte bij de politie en rapporteer de oplichter bij het verkoopplatform.

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank

Phishing

Bij phishing proberen oplichters, via het sturen van nepberichten, jouw bankgegevens, jouw bankrekening of betaalpas in handen te krijgen om bijvoorbeeld geld van je te stelen. Met deze tips weet je hoe je phishingberichten kunt herkennen en wat je moet doen als je hiermee te maken krijgt.

Hoe herken je een phishingbericht?

- Het e-mailadres van de afzender eindigt niet op @asnbank.nl of @mail.asnbank.nl.
- Je krijgt een e-mail op een e-mailadres dat je niet aan ons gegeven hebt.
- De e-mail is niet persoonlijk aan jou gericht.
- Jouw e-mailprovider of spamfilter geeft aan dat de e-mail ‘spam’ is.
- De e-mail heeft een bijlage.
- In de e-mail wordt gevraagd naar jouw beveiligingscodes of persoonlijke gegevens.
- In de e-mail wordt gedreigd met negatieve gevolgen als je niet meteen reageert.
- De e-mail is in een andere taal.
- Wanneer er een link naar een inlogpagina in de e-mail staat, is dit verdacht. ASN Bank stuurt je geen link naar de inlogpagina. Staat er een link in de e-mail, klik niet op de tekst of het plaatje van de link, maar beweeg er met je muis overheen. Je ziet dan naar welke website de link verwijst. Een link van ASN Bank begint altijd met https://www.asnbank.nl/.

Verdachte e-mail ontvangen?

- Stuur het bericht `1-op-1` door naar valse-email@asnbank.nl, anders gaat er belangrijke informatie verloren en kan de e-mail niet verwerkt worden. Verander het onderwerp of de inhoud dus niet.
- Verdachte SMS ontvangen? Stuur een schermafbeelding van het SMS-bericht naar valse-email@asnbank.nl, waarop ook het telefoonnummer zichtbaar is.
- Stuur geen persoonlijke gegevens mee, zoals jouw adres of je e-mailhandtekening.
- Heb je een verdachte e-mail, telefoontje of sms gehad en heb je wél gegevens gedeeld? Bel ons dan meteen op 070 - 35 69 335.
- Belangrijk: Heb je geen gegevens gedeeld met de verstuurder van het phishingbericht? Bel dan niet, maar stuur een e-mail. Zo voorkomen we een lange wachttijd aan de telefoon en kunnen we mensen die wél gegevens hebben gedeeld zo snel mogelijk helpen.

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank

Geldezels

Oplichters proberen via onder andere social media jou te overtuigen om snel en makkelijk geld te verdienen. Dit kan doordat je toegang verleent tot jouw online bankieren omgeving of op verzoek geld ontvangt en doorboekt naar een andere rekening. Maar meestal gebeurt dit door je pinpas uit te lenen en jouw pincode af te geven. De oplichters beloven soms dat je hier een vergoeding voor krijgt.

In eerste instantie lijkt dit onschuldig, maar als je hieraan meewerkt, dan ben je strafbaar en vaak krijg je ook de beloofde beloning niet. De bedragen die op jouw rekening binnenkomen zijn namelijk afkomstig uit fraude. Doordat dit geld op jouw rekening binnenkomt, blijft de oplichter buiten beeld.

Wat zijn de gevolgen als geldezel?

- De oplichter gebruikt jouw rekening om gestolen geld op te laten storten. Als het slachtoffer hiervan aangifte doet, onderzoekt de politie samen met de bank waar het gestolen geld terechtkomt. Als ze bij de rekening van jou of bijvoorbeeld jouw kind uitkomen, kunnen de gevolgen groot zijn. In plaats van snel geld verdienen, staat een geldezel vooral problemen te wachten.
- Veel geldezels zijn zich er niet van bewust dat ze hebben meegewerkt aan criminele activiteiten. Als de politie onderzoek doet naar deze criminele activiteiten, zullen ze het spoor van het geld volgen en uiteindelijk altijd bij de geldezel uitkomen. De kans dat zij gepakt worden is daarom bijna 100 procent. Een geldezel kan vervolgens een celstraf van maximaal 8 jaar krijgen voor witwassen.
- Geldezels kunnen door de slachtoffers aansprakelijk worden gesteld om het schadebedrag terug te betalen. Daarnaast krijgt een geldezel mogelijk extra boetes en vergoedingen die betaald moeten worden. Een geldezel wordt geregistreerd als fraudeur bij de bank. Hierdoor is het openen van een rekening lastiger. Ook het afsluiten van leningen zoals hypotheken en (telefoon)abonnementen gaat niet meer zo makkelijk door deze registratie.
- Een Verklaring Omtrent Gedrag (VOG) is nodig voor sommige beroepen, maar deze kan een geldezel niet altijd meer krijgen.

Hoe kunt u voorkomen dat u een geldezel wordt?

- Als een verhaal te mooi lijkt om waar te zijn, dan is dat het vaak ook. Ga er niet op in en geef nooit je pincode, bankrekening of bankpas uit handen. Werk ook nooit mee aan het ontvangen en doorboeken van gelden voor anderen.
- Maak het bespreekbaar met familieleden, vrienden of kennissen om te voorkomen dat in jouw kring slachtoffers komen. Heb je kinderen, bespreek dit dan met hen. Dit heeft veel impact op de toekomst van je kind.
- Het is belangrijk dat je het meldt aan de politie of jouw bank als je benaderd bent voor het uitlenen van je pas of pincode. Zo wordt de kans kleiner dat oplichters geldezels kunnen vinden. En je helpt de politie om de oplichters op te pakken.
- Denk je dat je slachtoffer bent van fraude of zie je iets verdachts? Meld fraude en incidenten zo snel mogelijk bij de ASN Klantenservice via 070 - 35 69 335 (24/7).

Ga voor meer informatie over alle fraudevormen naar onze veilig bankieren pagina: asnbank.nl/veiligbankieren.

asn bank