HERKEN EN VOORKOM FRAUDE

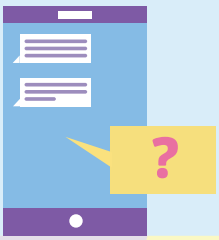
DE BELANGRIJKSTE TIPS OP EEN RIJ

- HULPVRAAGFRAUDE
- GELDEZELS
- VERKOOPPLATFORMFRAUDE
- PHISHING
- BANKHELPDESKFRAUDE

SNS

EERST DE MENS.
DAN HET GELD.

GEBRUIK ONZE TIPS EN VOORKOM HULPVRAAGFRAUDE.



Bij hulpvraagfraude proberen oplichters je te overtuigen om geld over te maken. 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 met spoed geld over te maken en stuurt je een betaalverzoek.
- 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?

- Deel niet zomaar persoonlijke informatie via WhatsApp en social media, zoals je telefoonnummer.
- Neem voordat je iets betaalt rechtstreeks contact op met je vriend, familielid of bekende via een ander communicatiekanaal of het oude telefoonnummer. Zo check je of je met een oplichter te maken hebt. Krijg je diegene niet te pakken? Maak geen geld over.
- Stel een controlevraag, al voelt dat misschien een beetje vreemd: ‘Ik wil dit voor de zekerheid even vragen... hoe heette onze eerste hond?’

TOCH GELD OVERGEMAAKT?

- Heb je geld overgemaakt en twijfel je achteraf of je misschien bent opgelicht? Bel ons dan meteen op **030 - 633 30 00**. Onze medewerkers staan 24 uur per dag, 7 dagen in de week voor je klaar om je te helpen.
- 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: **sns.nl/veiligbankieren**.

GEBRUIK ONZE TIPS EN VOORKOM MISBRUIK ALS GELDEZEL.

Oplichters proberen via onder andere social media je over te halen om snel en makkelijk geld te verdienen. Bijvoorbeeld door ze toegang te geven tot je online bankieren omgeving of door dat ze je geld geven of geld op je rekening storten en je vragen dat over te boeken naar een andere rekening. Maar meestal gebeurt dit door je pinpas uit te lenen en je pincode af te geven. De oplichters beloven soms dat je hier een beloning voor krijgt. Het lijkt misschien onschuldig, maar als je hieraan meewerkt, dan ben je strafbaar en vaak krijg je ook de beloofde beloning niet. De bedragen die ze op je rekening (laten) storten hebben ze niet op een eerlijke manier gekregen.

HOE HERKEN JE HET EN 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 je 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 hier onderzoek naar doet, 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.
- Geldezels kunnen door de slachtoffers aansprakelijk worden gesteld. Dan moeten ze het schadebedrag terugbetalen. 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 KUN JE VOORKOMEN DAT JE 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 doorboeken van geld voor anderen.
- Bespreek het met familieleden, vrienden of kennissen. Zo voorkom je dat zij erin trappen. 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 je 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 dat dan zo snel mogelijk aan ons via **030 – 633 30 00**.

Ga voor meer informatie over alle fraudevormen naar onze Veilig Bankieren pagina: **sns.nl/veiligbankieren**.

SNS

GEBRUIK ONZE TIPS EN VOORKOM 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 krijgt een bod dat te mooi lijkt om waar te zijn of het bod is snel geplaats nadat je het te koop hebt gezet.
- De (ver)koper vraagt om je identiteitsbewijs. Die kunnen ze later misbruiken voor identiteitsfraude.
- De (ver)koper wil je betaling en/of identiteit controleren door 1 cent over te laten maken via een nep betaalverzoek.
- Ga niet in zee met een koper die een koerier wil sturen of je zelf een verzendlabel toestuurt.

Hierna kom je op een nagemaakte betaalpagina uit. Als je alles hebt ingevuld, heeft de oplichter toegang gekregen tot je 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 je identiteitsbewijs, bankafschrift of betaalpas naar een (ver)koper als hij/zij daarom vraagt.

HOE CONTROLEER JE HET BETAALVERZOEK?

- Het betaalverzoek is van een klant van SNS, maar de link begint niet met **https://diensten.sns.nl/**;
- De pagina waarop je de transactie uitvoert, is niet van SNS. Onze pagina's beginnen altijd met **https://www.sns.nl/ of diensten.sns.nl/**;
- Je hebt een Mobiel Bankieren app geïnstalleerd op je telefoon, maar deze opent niet automatisch wanneer je op het betaalverzoek hebt geklikt.

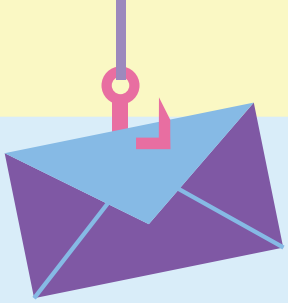
TOCH GELD OVERGEMAAKT?

- Heb je geld overgemaakt en twijfel je achteraf of je misschien bent opgelicht? Bel ons dan meteen op **030 - 633 30 00**. Onze medewerkers staan 24 uur per dag, 7 dagen in de week voor je klaar om jou te helpen.
- Verzamel zo veel mogelijk bewijsmateriaal, zoals screenshots van het gesprek, telefoonnummers en bankrekeningnummers van 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: **sns.nl/veiligbankieren**.

SNS

GEBRUIK ONZE TIPS EN VOORKOM PHISHING.



Bij phishing proberen oplichters je bankgegevens, bankrekening of betaalpas in handen te krijgen om bijvoorbeeld geld van je te stelen. Dit doen ze met het sturen van nepberichten. Dat noemen we phishing. 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 **@sns.nl** of **@e-mail.sns.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.
- In de e-mail wordt gevraagd naar je beveiligingscodes of persoonlijke gegevens.
- In de e-mail wordt gedreigd met negatieve gevolgen als je niet meteen actie onderneemt.
- De e-mail is in een andere taal, bijvoorbeeld in het Engels.
- Wanneer er een link naar een inlogpagina in de e-mail staat, is dit verdacht. SNS 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 SNS begint altijd met **https://www.snsbank.nl/**, **https://sns.nl/** of **https://t.e-mail.sns.nl/**

VERDACHTE E-MAIL ONTVANGEN?

- Stuur het bericht `1-op-1` door naar valse-email@sns.nl. Verander het onderwerp of de inhoud dus niet, anders gaat er belangrijke informatie verloren en kan de e-mail niet verwerkt worden.
- Verdachte SMS ontvangen? Maak een schermafbeelding van het SMS-bericht waarop ook het telefoonnummer zichtbaar is en stuur die naar valse-email@sns.nl.
- Stuur geen persoonlijke gegevens mee, zoals je 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 **030 – 63 33 000**.
- Belangrijk: Heb je nergens op geklikt en geen gegevens gedeeld? Dan heb je veilig gehandeld, stuur het bericht dan door naar **valse-email@sns.nl**. 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: **sns.nl/veiligbankieren**.

GEBRUIK ONZE TIPS EN VOORKOM BANKHELPDESKFRAUDE.

Bij bankhelpdeskfraude benadert de oplichter je onverwacht uit naam van de bank. De zogenaamde bankmedewerker vertelt je dat de rekening niet meer veilig is of dat er een probleem is met je bankrekening. Om dit op te lossen moet je actie ondernemen.

GELD OVERMAKEN NAAR EEN ZOGENAAMDE 'KLUISREKENING'

Dit is vaak een rekening bij een andere bank of een rekening in het buitenland. Meestal gaat het om een rekening op naam van een onbekende persoon. Wij vragen je nooit om geld over te boeken en al helemaal niet naar een rekening op naam van een persoon.

HET OP AFSTAND OVERNEMEN VAN JOUW COMPUTER, TABLET OF SMARTPHONE

De zogenaamde bankhelpdeskmedewerker vraagt je om software zoals Anydesk, Teamviewer en LogMein te installeren waarmee zij op afstand jouw computer, tablet of smartphone kunnen bedienen. Dit is een vreemd verzoek, een echte medewerker van SNS vraagt dit nooit. De oplichter vraagt je om in te loggen in je bankomgeving. En zo kan deze persoon betalingen via jouw rekening klaarzetten of je bankgegevens onderscheppen.

AFGEVEN VAN BANKPRODUCTEN

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

SPOOFING

Oplichters kunnen je benaderen met een onbekend telefoonnummer. Maar pas op; oplichters kunnen ook nummers vervalsen waardoor het lijkt of je dan benaderd wordt door het échte nummer van de bank. Zij zorgen ervoor dat het telefoonnummer of de naam van je bank op je telefoonscherm verschijnt, maar bellen eigenlijk vanuit een ander telefoonnummer of naam die je niet kunt zien.

HOE VOORKOM JE DAT JE SLACHTOFFER WORDT VAN BANKHELPDESKFRAUDE?

Noteer de naam van degene die je spreekt en bel ons op: **030 – 633 30 00**. Tip: Sla ons telefoonnummer op in je contacten. Twijfel je of er sprake is van oplichting? Bel ons dan voor alle zekerheid.

GOED OM TE WETEN, BANKEN VRAGEN JE NOOIT OM:

- geld over te boeken, ook niet naar een zogenaamde kluisrekening;
- je pincodes of beveiligingscodes te geven;
- de besturing van je apparaat over te nemen;
- programma's zoals Anydesk, Teamviewer en LogMeIn op je apparaat te installeren;
- 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: **sns.nl/veiligbankieren**.

SNS