

Aangifte Telefonische helpdeskfraude

“De helpdesk medewerker kwam zo geduldig en behulpzaam over!”

Telefonische helpdeskfraude, wat is dat?

Helaas bent u slachtoffer geworden van Telefonische helpdeskfraude. Bij deze vorm van fraude doet een crimineel zich telefonisch voor als bijvoorbeeld een medewerker van de overheid of een bedrijf (bijvoorbeeld: “Dutch Supreme Court”, bank, softwarebedrijf). In de meeste gevallen wordt het slachtoffer door de crimineel benaderd, maar het kan ook voorkomen dat het slachtoffer zelf op zoek gaat naar een helpdesk van een organisatie (bijv. via Google, Bing) en per ongeluk uitkomt bij een frauduleuze helpdesk. De crimineel heeft interactie met het slachtoffer en zet het slachtoffer aan tot het doen van een overboeking, tot het afgeven van betaalmiddelen (bijv. bankpas, telefoon) of eventueel tot het installeren van Remote Access Tool (e.g. AnyDesk, Teamviewer, Quick Assist) waarna de crimineel toegang heeft tot de computer van het slachtoffer.

Voordat u aangifte doet

Heeft de crimineel toegang tot uw computer gehad? Neem dan onmiddellijk deze maatregelen:

- Informeer direct uw bank en vraag hen alert te zijn op vreemde transacties die plaatsvinden met uw rekening/account;
- Kijk na of er door de crimineel wellicht toekomstige transacties zijn ingepland. Indien dit het geval is, noteer dan alle bijzonderheden van deze transacties (kijk bij ‘De transacties’ op pagina 4 van dit document) alvorens u deze transacties uit de planning verwijdert;
- Installeer uw computer niet opnieuw (of laat dit niet door een specialist doen) totdat de aangifte is gedaan en de sporen zijn veiliggesteld. Dit i.v.m. het wissen van sporen van uw computer;
- Veiligstellen loggegevens: wij vragen u om loggegevens van het gebruikte programma veilig te stellen. Gebruik hiervoor de HowToTeamviewer of HowToAnydesk, afhankelijk van de bij u gebruikte software. Lukt u dit zelf niet? Vraag dan iemand in uw omgeving om hulp;
- Nadat u de loggegevens heeft veiliggesteld via de genoemde ‘How to’-procedure adviseren wij u om Anydesk of Teamviewer direct te (laten) verwijderen van uw computer;
- Als u er zeker van bent dat de crimineel niet meer kan “meekijken”, pas dan zo snel mogelijk al uw gebruikersnamen én wachtwoorden aan. Denk hierbij aan uw computer, internetbankieren-gegevens en uw e-mailaccounts. Maak gebruik van veilige wachtwoorden. Op internet kunt u vinden hoe u een veilig wachtwoord maakt. Doe dit voor de zekerheid en indien mogelijk op een ander apparaat.

Gegevens aangifte

U maakt een afspraak voor het doen van aangifte. Voordat u de afspraak heeft, is het belangrijk dat u alle benodigde gegevens al bij de hand heeft. Vul hieronder uw gegevens in.

U dient dit document op een *computer* in te vullen. Om het document in te vullen klikt u boven in beeld op “BEELD” en vervolgens op “Document bewerken”.

Gegevens aangever

- Voornaam
- Achternaam
- Geboortedatum
- Adres
- Postcode
- E-mailadres
- Telefoonnummer
- Burgerservicenummer
- Welk identiteitsbewijs neemt u mee naar de aangifte? Dit kan een paspoort, identiteitskaart, rijbewijs of Nederlands vreemdelingendocument zijn.
- Documentnummer identiteitsbewijs

Vragen aangifte

Wilt u ter voorbereiding van de aangifte alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling achter 'A:'.

Algemene vragen

V: Op welke dag/datum/tijd heeft het misdrijf plaatsgevonden?

A:

V: Kunt u in chronologische volgorde vertellen wat er is gebeurd? Ook alle feitelijke gegevens zoals rekeningnummers, telefoonnummers, IP-adressen en e-mailadressen etc. moet u hier noemen.

[Verwijs niet naar eventuele bijlagen die u heeft, maar benoem ze hier ook.](#)

A:

Ontstaan van het contact

V: Is er contact geweest via de telefoon? Vermeld in dat geval zowel het telefoonnummer van uzelf als dat van de (schermnaam van) crimineel.

A:

V: Bent u gebeld of heeft u zelf op internet een telefoonnummer opgezocht en gebeld?

[Vermeld de zoekcriteria van uw zoekopdracht, bijvoorbeeld "telefoonnummer helpdesk bedrijf X"](#)

A:

V: Op welke website bent u terecht gekomen?

A:

V: Welke naam gaf de persoon aan de andere kant van de lijn op?

A:

V: Met welk telefoonnummer/schermnaam belde de crimineel?

A:

V: Op welk telefoonnummer van u werd u gebeld?

A:

Beschrijf zoveel mogelijk specifieke kenmerken van de beller:

V: Welke taal/welk accent had de crimineel?

A:

V: Gebruikte de crimineel stopwoorden?

A:

V: Sprak de beller met een mannelijke of vrouwelijke stem?

A:

V: Werd u tijdens het gesprek doorverbonden of doorgegeven aan een andere "medewerker"?

A:

V: Waren er andere personen op de achtergrond te horen tijdens het gesprek?

A:

V: Wat was het tijdstip en de duur van het telefoongesprek?

A:

V: Is er chat/mail/sms-contact geweest? Wat werd hierin gezegd? Voeg indien mogelijk screenshots of een exportbestand bij van het volledige chat-gesprek.

A:

V: Via welke applicatie of programma?

A:

V: Welke naam gaf de persoon op?

A:

V: Met welk telefoonnummer maakte de crimineel gebruik van de chat?

A:

V: Zijn er tijdens het contact nog bepaalde gegevens (zoals adressen/rekeningnummers) genoemd? Dit kunnen ook opvallende gegevens zijn die de oplichter over u wist (zoals uw banksaldo).

A:

V: Heeft u in het verleden een verdachte sms of e-mail ontvangen van een externe organisatie, waar u op een link moest klikken of persoonlijke gegevens moest invullen? Zo ja, welke organisatie en link is dat geweest (Pas op! Niet op de link klikken). Voeg de e-mail toe aan de bijlage.

A:

V: Is de link nog veranderd in de tijd dat u contact had met de crimineel? Indien ja; heeft de crimineel een verklaring gegeven over waarom de site niet bereikbaar was?

A:

V: Heeft u daarna nog een nieuwe link of meerdere links ontvangen van de crimineel?

A:

Koerier

Kwam er iemand bij u aan de deur, een zogenaamde “koerier”? Beantwoord in dat geval de volgende vragen:

V: Wat was het tijdstip van de aankomst en het vertrek?

A:

V: Hoeveel personen kwamen er aan de deur?

A:

V: Waren zij te voet of met de auto?

A:

V: Indien van toepassing, wat waren de kenmerken van de auto? (Denk aan kleur, kenteken, merk en type)

A:

V: Wat heeft er binnen plaatsgevonden? (Hierbij ligt de focus op de handelingen op apparatuur van u, zoals het verhogen van limieten van de bankomgeving etc.)

A:

V: Welke spullen heeft u aan de koerier meegegeven? (Denk hierbij aan een pinpas, pincode, reader etc.)

A:

V: Welke naam gaf de koerier op?

A:

V: Welke afspraak heeft u gemaakt over de code die de koerier heeft?

A:

V: Wat is het signalement van de koerier(s)?

Uiterlijke kenmerken, denk aan lengte, postuur, huidskleur, haardracht, haarkleur (Bedrijfs)kleding

Opvallende tatoeages, moedervlekken, puisten, verwondingen etc.

A:

V: Welke taal/welk accent had(den) de koerier(s)?

A:

V: Hangen er camera's bij u in de omgeving? Zo ja, waar?

A:

V: Zijn er getuigen die de koerier(s) hebben gezien?

A:

De ondersteuning

Mogelijk heeft de crimineel u aangeboden om te helpen/ondersteunen bij een overboeking of om het probleem op uw computer op te lossen. Het is belangrijk dat duidelijk blijkt op welke manier de crimineel dit deed of wilde doen. Eén van de mogelijkheden is het op afstand digitaal 'meekijken' via een daarvoor bestemd computerprogramma. In dat geval zijn de volgende vragen van belang:

V: Moest er een programma geïnstalleerd worden? Welk programma was dat?

A:

V: Wat voor apparaat gebruikt u om in te loggen op de account? (Bijvoorbeeld computer, laptop, tablet, telefoon.) [En vermeld ook van welk merk en type dit apparaat is.](#)

A:

V: Vanaf welke website is het programma gedownload? Noteer hier de volledige URL.

A:

V: Welke stappen moest u doorlopen?

A:

V: Moest u een code voeren? Welke code was dat?

A:

V: Werd de besturing van de computer overgenomen? Welke handelingen voerde de crimineel op de computer uit?

A:

Indien u bovenstaande vragen positief heeft beantwoord, is er mogelijk een Remote Access Tool gebruikt zoals AnyDesk of TeamViewer. Voor de opsporing hebben wij logbestanden hiervan nodig. U leest [hier](#) (AnyDesk) of [hier](#) (Teamviewer) hoe u deze zelf verzamelt. Weet u niet hoe u dit moet doen? Verwijder dan NIET het programma en neem uw apparaat indien mogelijk mee naar uw aangifte-afspraak.

De transacties

Vermeld u zo veel mogelijk informatie over de transacties die hebben plaatsgevonden.

V: Hoe verliep de betaling die u van de crimineel moest verrichten?

A:

Vul in per banktransactie:

Datum en tijdstip:

Bedrag en valuta:

Van bankrekeningnummer:

Tenaamgestelde:

Naar bankrekeningnummer:

Tenaamgestelde:

Omschrijving:

Vul in per crypto transactie:

Datum en tijdstip:

Aantal en valuta:

Van wallet:

Naar wallet:

Transactie hash:

V: Zijn er pin/response/TAN/Kleur codes uitgewisseld?

A:

V: Wie maken er allemaal gebruik van de bankrekening die is misbruikt?

A:

V: Bij welk transactiepunt of vanuit welke winkel hebben de transacties plaatsgevonden?

A:

V: Op welke datum en tijdstip vonden deze transacties plaats.

A:

V: Indien er is betaald met tegoedkaarten, wat voor tegoedkaarten waren dit, en om welke bedragen gaat dit?

A:

Voeg een transactieoverzicht van uw bankrekening van het moment vlak vóór het misdrijf, en óók van vlak na het misdrijf bij de aangifte. Dit is belangrijk in het kader van het veiligstellen van eventuele camerabeelden.

LET OP: De belangrijke informatie die zich hierop bevindt moet u ook benoemen bij *Algemene vragen*.

Schade en impact

Vermeld informatie over de schade en gevolgen in de verklaring.

V: Heeft u naderhand contact gehad met uw daadwerkelijke bank?

A:

V: Is er een referentienummer of contactpersoon bij de bank?

A:

V: Wat is het totale schadebedrag?

A:

V: Bent u door uw bank schadeloosgesteld?

A:

V: Heeft u op een andere wijze schade geleden?

A:

Slachtofferhulp

V: Heeft u behoefte aan slachtofferhulp of nazorg? (zie informatie op <https://www.politie.nl/informatie/ik-ben-slachtoffer-wat-nu.html>)

Deze vraag graag met **ja** of **nee** beantwoorden. A:

Bijlagen

Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij Algemene vragen. Voeg alle relevante bijlages bij de aangifte. Denk hierbij aan:

- Loggegevens van de Remote Access Tool, zoals AnyDesk of Teamviewer.
- Transactieoverzicht van uw bankrekening van het moment vlak vóór het misdrijf, en óók van vlak na het misdrijf.
- Voeg al uw relevante e-mails, sms-berichten, en WhatsAppberichten bij als bijlage in de e-mail.
- Camerabeelden van bijvoorbeeld een videodeurbel.

Voorkom telefonische helpdeskfraude

Om in de toekomst niet nog eens slachtoffer te worden van Telefonische helpdeskfraude hebben wij de volgende tips voor u:

- Laat een helpdeskmedewerker nooit uw geld overmaken naar een andere rekening. Doe dit ook niet zelf als helpdeskmedewerker dat aan u vraagt. Uw bank zal u namelijk nooit vragen om uw geld naar een andere rekening over te maken.
- Twijfelt u of u een crimineel aan de telefoon heeft? Ook bij lichte twijfel: verbreek de verbinding direct. Zoek zelf het juiste telefoonnummer van de bank. Dan kunt u de bank terugbellen en vragen of het klopt wat u is verteld en wat u werd gevraagd te doen. U kunt ook altijd uw bankkantoor bezoeken en uw ervaring delen.
- Als u zelf een telefoonnummer op internet opzoekt, wees er dan zeker van dat dit het officiële helpdesknummer is. Het kan zo zijn dat in uw zoekresultaten op zoekmachines malafide websites verschijnen van nephelpdesks. Op <https://veiliginternetten.nl/> kunt u eenvoudig een ScamCheck doen om te checken of een website echt of nep is.
- Installeer geen software op verzoek van de beller.
- Houd uw computer up-to-date. Dat betekent dat u altijd software updates uitvoert zodra die beschikbaar zijn.
- Maak gebruik van een antivirusprogramma en een firewall.
- Informeer uw familie, vrienden en kennissen over deze oplichting en waarschuw hen.
- Als er sprake is van een gehackt account, probeer dan de toegang tot het account te herstellen, verander het wachtwoord en stel tweestapsverificatie in. Doe dit ook voor andere accounts waarvoor u hetzelfde wachtwoord gebruikte.

Voor meer informatie verwijzen we u door naar de internetpagina's van de Politie over telefonische helpdeskfraude ([bank](#) of [softwarebedrijf](#)).