

Aangifte Phishing

“De nagemaakte website leek net echt!”

Phishing, wat is dat?

Helaas bent u slachtoffer geworden van phishing; U heeft in een e-mail, sms, of een WhatsAppbericht op een link geklikt die u op de inlogwebsite van uw bank of een andere inlogpagina bracht. U voerde uw inloggegevens in, maar op de één of andere manier werkt de website niet, krijgt u een foutmelding, of lijkt de internetpagina niet meer bereikbaar te zijn.

De inlogwebsite van de link waar u op heeft geklikt, is een perfect nagebouwde website die niet van uw bank of andere instantie afkomstig is; deze website is door iemand gemaakt met als doel om achter uw inloggegevens te komen en deze uiteindelijk te misbruiken. Het kan zijn dat u ziet dat er daadwerkelijk al geld van uw rekening is afgeschreven. Het kan ook zo zijn dat dit nog niet is gebeurd, maar uw inloggegevens zijn bekend bij de andere partij; u wilt hiervan aangifte doen.

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:

Het phishingbericht

V: Hoe bent u met de phishing in aanraking gekomen? Wat stond er in het bericht en hoe bent u overgehaald om op de link te klikken?

A:

V: Heeft u een phishing sms-bericht ontvangen? Vermeld dan de inhoud, het telefoonnummer en afzender in de verklaring.

A:

V: Heeft u een phishing e-mail ontvangen? Omschrijf de inhoud en vermeld de afzender in de verklaring. Vermeld ook altijd de link die u heeft aangeklikt. Het is belangrijk voor het opsporingsproces dat u deze link hier letterlijk neerzet!

A:

V: Heeft u een phishingbericht ontvangen via een andere weg, zoals een chat-app of Marktplaats? Vermeld dan zo veel mogelijk informatie zoals gebruikersnamen van zowel de crimineel als het slachtoffer.

A:

[Voeg screenshots bij van uw e-mails, sms-berichten, en WhatsAppberichten. Vergeet niet de inhoud hiervan ook te benoemen bij *Algemene vragen*.](#)

E-mailheaders

V: Is de phishing via e-mail verlopen? Stel dan de e-mailheaders veilig. De e-mailheaders bevatten aanvullende verborgen informatie over een e-mail en kunnen helpen om de afzender te traceren. De website <https://internetsporen.nl/is/emailheaders/> bevat hiervoor instructies. Deze stappen kunnen vaak alleen via een computer worden uitgevoerd.

[We vragen u om de e-mailheadertekst te kopiëren en deze te plakken in de verklaring bij *Algemene vragen*. Stuur de volledige e-mail mee in de bijlage van de aangifte.](#)

De link waarop geklikt moest worden

V: Phishing van bankgegevens vindt vaak plaats via een valse website. Vermeld de link naar deze website in de verklaring. Het is belangrijk voor het opsporingsproces dat u deze link hier letterlijk neerzet.

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:

V: Wat zag u na het klikken op de link? Hoe zag het scherm eruit?

A:

V: Welke stappen moest u op de valse website doorlopen?

A:

V: Stond er een bedrag en/of omschrijving in beeld?

A:

V: Welke gegevens heeft u ingevuld?

A:

V: Wat zag u nadat de stappen waren voltooid?

A:

De transacties

Na het afstaan van de gegevens proberen criminelen vaak toegang te verkrijgen tot uw bankrekening. Vermeld zoveel mogelijk informatie over de transacties die hebben plaatsgevonden.

V: Wat voor transacties hebben er na het verstrekken van de gegevens plaatsgevonden?

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:

- Transactieoverzichten.
- Voeg al uw relevante e-mails, sms-berichten, en WhatsAppberichten bij als bijlage in de e-mail.
- E-mailheaders

Voorkom phishing

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

- Reageer nooit op e-mails of appjes met verzoeken om persoonlijke inlogcodes of pincode. Banken, creditcardmaatschappijen en bijvoorbeeld webshops vragen hier nooit om. Ontvangt u zo'n e-mail? Verwijder deze dan meteen. Klik in geen geval op een link die in de e-mail staat.
- Krijgt u betaalverzoeken van onbekenden, klik deze dan niet aan.
- Stuur uw bankpas niet op. Uw bank zal hier nooit om vragen. Als u een nieuwe pas krijgt, vraagt de bank altijd om uw oude pas door te knippen en weg te gooien.
- Stuur ook nooit een kopie van uw identiteitsbewijs op. Criminelen kunnen uw Burgerservicenummer gebruiken om een bankpas aan te vragen.
- Geef nooit zomaar persoonlijke gegevens over de telefoon.
- Een koop via Markplaats of Facebook afwickelen? Log dan in op uw eigen bankapp of de website van uw bank en doe daar de betaling. Geef ook aan bij de koper dat u op deze manier betaalt. Vaak zal de fraudeur dan al afhaken en geen verdere actie ondernemen.
- Vertrouwt u een link niet helemaal, check hem via de website checkjelinkje.nl.
- Wijzig uw wachtwoorden naar nieuwe sterke en unieke wachtwoorden. Gebruik voor wachtwoorden bijvoorbeeld een onsamenhangende zin, die alleen u weet en/of gebruik een wachtwoordmanager.

- Wees er zeker van de uw computer de laatste software- en beveiligingsupdates heeft gehad.

Voor meer informatie verwijzen we u door naar de internetpagina van de Politie over [Phishing](#).