Aangifte Boilerroomfraude

Hulpmiddel bij aangifte

Versie oktober 2024

« waakzaam en dienstbaar »

Boilerroomfraude, wat is dat?

U bent slachtoffer geworden van boilerroomfraude. Boilerroomfraude is een vorm van fraude waarbij mensen, meestal telefonisch, benaderd worden om te beleggen in bijvoorbeeld crypto. Nadat slachtoffers geld hebben ingezet worden ze onder druk gezet om steeds meer geld te storten. In werkelijkheid hebben ze geld in fictieve aandelen gestort of in waardeloze producten. In de meeste gevallen krijgen slachtoffers het geld niet meer terug.

Belangrijk preventief advies:

> *Ga niet in zee met zogenaamde 'recoverybedrijven' of advocatenkantoren die na een tijdje contact opnemen met u. Zij beweren het geld van slachtoffers te kunnen terughalen, vaak voorafgegaan door een verzoek om 'borg' te betalen. Maar deze 'recoverybedrijven' of advocatenkantoren zijn vermoedelijk onderdeel van frauduleuze beleggingsmaatschappijen, die proberen slachtoffers nog meer geld afhandig te maken.*

Voordat u aangifte doet

Heeft de oplichter 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;
- **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 bewijs van uw computer.**
- Als u er zeker van bent dat de oplichter 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 en gebruik nooit hetzelfde wachtwoord voor meerdere websites. Op https://veiliginternetten.nl/ kunt u informatie vinden over hoe u een veilig wachtwoord maakt. Voor de zekerheid kunt u gebruik maken van een ander apparaat om uw wachtwoorden aan te passen.
- Stel tweestapsverificatie in voor accounts waar dit mogelijk is, door bijvoorbeeld bij het inloggen op uw account een bevestiging met de mobiele telefoon te moeten geven.
- Op de website https://haveibeenpwned.com kunt u uw e-mailadres invullen om te kijken of uw inloggegevens in het verleden gelekt zijn. Op https://scatteredsecrets.com/ kunt u zien welke van uw wachtwoorden gelekt zijn.

Vragen 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. Wilt u ter voorbereiding alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling.

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

1) Voornaam

2) Achternaam

3) Geboortedatum

4) Adres

5) Postcode

6) E-mailadres

7) Telefoonnummer

8) Burgerservicenummer

Algemene vragen

1. Op welke dag/datum/tijd heeft het misdrijf plaatsgevonden? Binnen welke periode heeft dit plaats gevonden?

2. Kunt u in chronologische volgorde vertellen wat er is gebeurd? Ook alle feitelijke gegevens zoals rekeningnummers, telefoonnummers, IP-adressen en emailadressen etc. moet u hier noemen.
   Verwijs niet naar eventuele bijlagen die u heeft, maar benoem ze hier ook.

Ontstaan van het contact

1. Hoe bent u op de hoogte gekomen van de organisatie?
   In geval van een website of advertentie, noem ook de link en de datum en tijd waarop deze link is bezocht.
   TIP: raadpleeg eventueel de internetgeschiedenis van uw browser en maak hier een screenshot van.

2. Heeft u zich geregistreerd op een website om te beleggen? Zo ja:
   - Vermeld de exacte URL van de website waar u zich geregistreerd heeft en de datum en tijd waarop deze URL is bezocht.
     TIP: raadpleeg eventueel de internetgeschiedenis van uw browser en maak hier een screenshot van.
   - Welke gegevens heeft u ingevuld?
   - Heeft u betaald hiervoor, en zo ja naar welke rekening is dit gegaan?

Indien van toepassing, volgen hier vragen over het gebruik van een crypto platform:

1. Heeft u een crypto wallet aangemaakt op uw naam? Wat is het adres van deze wallet?

2. Wat is de exacte URL van de website van het cryptoplatform waar u gebruik van heeft gemaakt?

Vragen over het contact met de oplichter:

1. Is er contact geweest via de mail? Vermeld in dat geval zowel het e-mailadres van uzelf als dat van de oplichter.

2. Is er contact geweest via de telefoon? Vermeld in dat geval zowel het telefoonnummer van uzelf als van de oplichter.
   - Welke naam gaf de persoon aan de andere kant van de lijn op?
   - Heeft u zelf ook gebeld naar het nummer van de oplichter?

3. Welke taal gebruikte/welk accent had de oplichter?

4. Heeft u gesprekken opgenomen? Voeg de audiobestanden toe aan de bijlage.

5. Werd u tijdens het gesprek doorverbonden of doorgegeven aan een andere “medewerker”?

6. Waren er andere personen op de achtergrond te horen tijdens het gesprek?

7. Wat was het tijdstip en de duur van het telefoongesprek?

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

- Van welke chatdienst werd gebruikgemaakt?
- Welke naam gaf de persoon op?

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

De ondersteuning

Mogelijk heeft de oplichter u aangeboden om te helpen/ondersteunen bij de overboeking. Het is belangrijk dat duidelijk blijkt op welke manier de oplichter 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:

1. Moest er een programma geïnstalleerd worden? Welk programma was dat?

2. Vanaf welke website is het programma gedownload?

3. Welke stappen moest u doorlopen?

4. Werd de besturing van de computer overgenomen? Zo ja, welke handelingen voerde de oplichter op de computer uit?

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.

De transacties

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

1. Hoe verliep de betaling die u van de oplichter moest verrichten?

2. Zijn er pin/response/TAN/Kleur codes uitgewisseld of Bitcoin adressen?

3. Heeft u zelf transacties moeten verifiëren met een randomreader of via verificatie sms'jes?

4. Wat is uw eigen rekeningnummer en de tenaamstelling daarvan?

5. Wie maken er allemaal gebruik van uw bankrekening?

6. Indien er geld is overgemaakt naar een bankrekening, vul in per banktransactie:

   Datum en tijdstip:
   Bedrag en valuta:
   Van bankrekeningnummer:
   Tenaamgestelde:
   Naar bankrekeningnummer:
   Tenaamgestelde:
   Omschrijving:

7. Indien er crypto is overgemaakt. Vul in per cryptotransactie:

   Datum en tijdstip:
   Aantal en valuta:
   Van wallet:
   Naar wallet:
   Transactie hash:

8. Op welk site hebben de transacties plaatsgevonden?

❖ 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", vraag #2.*

Schade en impact

Vermeld informatie over de schade en gevolgen in de verklaring.

1. Hebt u naderhand contact gehad met uw bank?

2. Wat is het totale schadebedrag?

3. Is er een referentienummer of contactpersoon bij de bank?

4. Bent u door uw bank schadeloosgesteld?

Slachtofferhulp

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. Antwoord:

Bijlagen

Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij Algemene vragen, vraag 2. Voeg alle relevante bijlages bij de aangifte. Denk hierbij aan:

- □ E-mails, inclusief e-mailheaders
- □ Logbestanden bij waaruit blijkt vanaf welke IP-adressen de betrokken mailboxen benaderd zijn
- □ Transactieoverzichten
- □ Voeg al uw relevante e-mails, sms-berichten, en WhatsAppberichten toe in de bijlage van de e-mail
- □ Audiobestand opgenomen gesprek
- □ Screenshot van de advertentie

Voorkom Boilerroomfraude

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

- Vul niet zomaar uw gegevens in op een website, maar zoek eerst op internet naar beoordelingen over de website of de organisatie.
- Twijfelt u of u een oplichter aan de telefoon heeft? Ook bij lichte twijfel: verbreek de verbinding direct. Zoek op internet naar gegevens van de organisatie waar u contact mee had.
- Installeer geen software op verzoek van de beller.
- Houd uw computer up-to-date.
- Maak gebruik van een antivirusprogramma en een firewall
- Informeer uw familie, vrienden en kennissen over deze oplichting en waarschuw hen.
- Wees voorzichtig met waar u persoonlijke informatie achterlaat, denk aan:
    - Zet uw telefoonnummer niet openbaar op websites als Marktplaats
    - Zorg ervoor dat foto’s en (familie) relaties niet voor iedereen te zien zijn op Facebook
    - Laat geen informatie achter op niet beveiligde websites