

# Aangifte BEC-fraude

*“Ik had niet door dat ik met iemand anders aan het e-mailen was!”*

## BEC-fraude, wat is dat?

Helaas bent u, of uw bedrijf, slachtoffer geworden van BEC-fraude: Business E-mail Compromise (BEC) fraude is een verzamelnaam voor verschillende vormen van digitale fraude en cybercrime waarbij de crimineel het e-mailverkeer misbruikt om uw bedrijf of organisatie op te lichten. Het komt erop neer dat u of uw medewerkers worden misleid om een valse factuur te betalen of ongeoorloofd een fors geldbedrag van de bedrijfsrekening over te schrijven.

De meest voorkomende vormen van BEC-fraude zijn digitale factuurfraude en CEO-fraude.

## 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

## Gegevens benadeelde

- Naam bedrijf
- Adres
- Vestigingsplaats
- KVK-nummer
- E-mailadres
- Telefoonnummer

## 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? Binnen welke periode heeft dit plaats gevonden?

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:

V: Is er door de IT-afdeling van uw bedrijf onderzoek gedaan en is er een onderzoeksrapport beschikbaar? Voeg dit toe aan de bijlage.

A:

### De ontvangen e-mail(s)

V: Van wie is de e-mail met de factuur of het betaalverzoek afkomstig? Neemt u hier letterlijk de naam, bedrijfsnaam en het e-mailadres over.

A:

V: Is dit een bestaande medewerker van uw bedrijf/een bestaande zakenrelatie van u?

A:

V: Heeft de u vaker met deze persoon en/of dit bedrijf contact?

A:

V: Is de e-mail daadwerkelijk door deze persoon verzonden?

A:

V: Wat is het bankrekeningnummer in de valse e-mail die ontvangen is?

A:

V: Naar welk e-mailadres is de valse e-mail verzonden?

A:

V: Is er een vermoeden waarom de e-mail naar dit adres is verzonden?

A:

V: Wat is de functie van de persoon achter dit e-mailadres?

A:

V: Is er naast de e-mail nog op andere wijze contact opgenomen (bijvoorbeeld telefonisch of via WhatsApp)?

A:

Voeg indien mogelijk een kopie van alle e-mails, inclusief e-mailheaders, bij de aangifte. Op de website [internetssporen.nl](https://www.internetssporen.nl) kunt u lezen hoe u de e-mailheaders, belangrijk voor het opsporingsonderzoek, kunt veiligstellen.

## De ontvangen factuur

V: Welk afzender staat er op de factuur?

A:

V: Doet u normaal gesproken ook zaken met deze relatie?

A:

V: Voor welke goederen of diensten is de factuur en wat is het factuurbedrag?

A:

V: Zijn deze goederen of diensten daadwerkelijk geleverd?

A:

V: Betreft het een daadwerkelijk verstuurd factuur die is onderschept en waarvan het rekeningnummer is aangepast?

A:

V: Welk rekeningnummer staat op de factuur? En wat is het werkelijke rekeningnummer van de leverancier?

A:

## Ongeoorloofde toegang tot een mailbox

Is er sprake van ongeoorloofde toegang tot een mailbox van de leverancier/klant of van uzelf? Dan zijn de volgende vragen ook van belang:

V: Vanuit welke mailbox is de oorspronkelijke (legitieme) factuur verzonden?

A:

V: Aan wie (welke mailboxen) was de e-mail met de oorspronkelijke (legitieme) factuur gericht? Hebben deze personen de e-mail daadwerkelijk ontvangen?

A:

V: Bestaat er een vermoeden dat de criminelen toegang hebben gehad tot één of meer van de betrokken mailboxen? Zo ja, welke mailbox(en)?

A:

V: Hebben medewerkers van uw organisatie een e-mail met een link ontvangen die hen leidden naar een website waar zij hun inloggegevens moesten invoeren?

A:

V: Welke technologie/software wordt er binnen uw organisatie gebruikt voor de e-mail en/of webmail (bijvoorbeeld Office 365)?

A:

V: Zijn deze mailboxen via webmail toegankelijk? En is de toegang hiertoe alleen beveiligd met een wachtwoord of is er sprake van tweestapsverificatie (bijvoorbeeld via SMS)?

A:

V: Zijn op de betreffende mailbox(en) zogenaamde 'forward-regels' ingesteld waardoor mail wordt doorgestuurd naar externen?

A:

V: Is er vanaf opvallende IP-adressen of op afwijkende tijdstippen ingelogd op de betreffende mailbox(en)?

A:

Voeg indien beschikbaar logbestanden bij waaruit blijkt vanaf welke IP-adressen de betrokken mailboxen benaderd zijn (via webmail of met een mailprogramma of app).

## De transactie(s)

V: Is de factuur betaald?

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: Is er na de betaling nog contact geweest met de criminelen?

A:

Wanneer u aangifte bij ons doet, voeg dan graag kopieën toe van de betreffende transacties.

## Schade en impact

Vermeld informatie over de schade en gevolgen in de verklaring.

V: Heeft u contact opgenomen met de bank om te proberen de transactie(s) tegen te houden?

A:

V: Zo ja, is er een fraudeonderzoek door de bank uitgevoerd?

A:

V: Eventueel; welke rekeningnummers heeft de bank voor u bevroren?

A:

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

A:

V: Wat is het totale schadebedrag?

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:

- Het onderzoeksrapport van de IT-specialist
- 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

## Voorkom BEC-fraude

Om in de toekomst niet nog eens slachtoffer te worden van BEC-fraude hebben wij de volgende adviezen voor u:

- Controleer het e-mailadres van de afzender van de opdracht of factuur, is dit werkelijk het e-mailadres van jouw eigen onderneming of zakelijke relatie?
- Controleer altijd het rekeningnummer van de ontvanger met jouw eigen administratie.
- Verifieer de betaling door de (genoemde) opdrachtgever te bellen. Gebruik hiervoor het nummer dat bij jou bekend is en niet het nummer dat bij het betaalverzoek staat. Dat nummer kan immers van de oplichter zijn.
- Wees alert op smoesjes waarom een betaling urgent is en moet afwijken van normale procedures.
- Wees alert op telefoontjes met een dwingend karakter.
- Stel duidelijk richtlijnen op voor facturatie, met daarin beschreven wie een betaalopdracht mag uitvoeren als er geen goedgekeurde factuur is. Probeer uitzonderingen te vermijden en zorg dat er altijd meerdere handtekeningen moeten worden gezet bij een betaalopdracht (functiescheiding of dubbele autorisatie). Twee mensen zien namelijk altijd meer dan één.
- Overleg bij twijfel altijd met een collega of leidinggevende.

Voor meer informatie verwijzen we u door naar de internetpagina van de politie over [BEC-fraude](#).