

Infoblad

Bestuurlijk advies Factuurfraude

Wat is factuurfraude?

Bij factuurfraude sturen (cyber)criminelen valse facturen in de hoop dat de ondernemer deze gaat betalen. Dit gebeurt op verschillende manieren. Ten eerste sturen zij massaal nefacturen naar willekeurige e-mailadressen. Het lijkt alsof dit facturen zijn van bekende en vertrouwde partijen als Ziggo, UPC, KPN en CJIB. Omdat het vaak om relatief kleine bedragen gaat en de e-mail lijkt te komen van gangbare partijen, betalen veel ontvangers deze nefacturen. Dit gebeurt ook als de onderneming helemaal geen klant van de zogenaamde afzender is. Het slachtoffer gaat ervan uit dat de factuur correct is.

De tweede vorm van factuurfraude betreft de gepersonaliseerde nefacturen. De ondernemer krijgt een vervalste factuur uit naam van een bestaande zakelijke relatie. In veel van deze gevallen onderschept de fraudeur de originele factuur (fysiek of digitaal). Vervolgens wordt enkel het rekeningnummer gewijzigd naar het rekeningnummer van de crimineel. De onderneming betaalt de rekening die hij verwachtte, maar het geld wordt overgemaakt naar het rekeningnummer van de oplichter.

Een andere vorm van factuurfraude is de zogenoemde CEO-fraude. Hoe groter een organisatie, hoe groter de kans op dat een oplichter een valse betaalopdracht verstuurt. De betaalopdracht komt veelal via e-mail binnen bij een potentieel slachtoffer. Het is ook mogelijk dat de criminelen via telefonisch contact druk uitoefenen om de betaling te verrichten. Fraudeurs doen zich voor als een belangrijke manager of bestuurder van uw bedrijf. Zij hebben zich in de onderneming verdiept, om zo werknemers te kunnen verleiden grote sommen geld over te boeken op hun rekening. Het proces van deze betaalopdracht wijkt vrijwel altijd af van de normale regels in uw bedrijf. Door de kennis van de structuur van de onderneming weten de oplichters veel slachtoffers te maken. Zij maken gebruik van het gegeven dat werknemers elkaar niet altijd persoonlijk kennen en er vaak geen contact is met het management.

Wie wordt slachtoffer van factuurfraude?

In principe kan iedereen slachtoffer worden van factuurfraude. In het mkb krijgen ondernemers voornamelijk te maken met de gerichte vervalste facturen afkomstig van bestaande zakelijke relaties. De bedragen die worden gestolen zijn geheel in overeenstemming met het type doelwit: bedrijven die grotere facturen betalen, lopen ook tegen fraude op met hogere bedragen dan kleinere bedrijven. In een enkel geval bedraagt de vervalste factuur vrijwel het hele werkkapitaal van de ondernemer en komt hierdoor de continuïteit van het bedrijf ernstig in gevaar.

Kunnen banken factuurfraude voorkomen?

De banken doen er alles aan wat ze redelijkerwijs kunnen om dit soort situaties te voorkomen voor hun klanten. Dat doen ze enerzijds door de klant veelvuldig te waarschuwen op dit soort risico's en anderzijds door gebruik te maken van diverse systemen voor monitoring en detectie. Voor de banken is het echter moeilijk om factuurfraude te herkennen en te stoppen. Het gaat hier immers om een betaling die de ondernemer zelf uitvoert en ondertekent; tenzij het rekeningnummer van de begunstigde bekend is als zijnde in gebruik door fraudeurs, zal de bank hier niet snel een afwijking in kunnen waarnemen. Dat de naam op de factuur wellicht niet de naam is van de begunstigde zal niet ontdekt worden; banken controleren wel of een rekeningnummer geldig is, maar de combinatie van rekeningnummer en naam van de begunstigde wordt niet gecontroleerd.

Hoe voorkomt u factuurfraude?

Hoewel fraudeurs zeer gehaaid zijn in hun pogingen om u geld afhandig te maken kunt u veel doen om factuurfraude te voorkomen. Het is belangrijk om te zorgen dat alle lagen van de organisatie deze vorm van fraude kennen. Vooral op afdelingen waar betaalopdrachten worden verwerkt. Maak factuurfraude daarom bespreekbaar in uw bedrijf. Als uw medewerkers twijfels durven uiten, krijgt CEO-fraude minder kans. Let ook goed op hoeveel informatie u op het internet vrijgeeft over uw organisatie, de bestuurders en medewerkers; deze informatie wordt door de fraudeur gebuikt om hun misleiding kracht bij te zetten. Geef tot slot uw medewerkers deze concrete tips:

- Controleer het e-mailadres van de afzender van de opdracht of factuur, is dit werkelijk het e-mailadres van uw eigen onderneming of van uw relatie?
- Controleer altijd het rekeningnummer van de ontvanger met uw eigen administratie
- Verifieer de betaling door de (genoemde) opdrachtgever te bellen. Gebruik hiervoor het nummer dat bij u bekend is; 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.

Wat moet u doen als u toch slachtoffer bent geworden van factuurfraude?

Bel zo snel mogelijk uw bank als u een betaling deed aan een fraudeur. Hoewel de kans klein is, is mogelijk nog te voorkomen dat een (deel) van het geld verdwijnt. Daarnaast is het zaak om - ook bij een eventuele buitenlandse begunstigde - aangifte te doen. Er is immers een misdrijf gepleegd en wellicht kunnen politie en justitie met de aangifte actie tegen de criminelen ondernemen. Bovendien kan dit bij eventuele geschillen met degene die het geld wel had moeten ontvangen een belangrijk element in de afhandeling zijn.

In veel gevallen blijkt het via de bovenstaande weg onmogelijk om geld terug te krijgen. In tegenstelling tot bij een automatische incasso, kan de bank een eenmalige, door u ondertekende betalingsopdracht niet terugdraaien. De bank zal proberen contact op te nemen met de (buitenlandse) bank van de begunstigde om daar de transactie te laten stoppen. Zodra een fraudeurs het geld contant heeft opgenomen is terugdraaien van de betalingsopdracht niet meer mogelijk. Snelheid is dus van belang.

Wat kunt u doen als u pogingen ziet van factuur en/of CEO-fraude?

Als u pogingen tot deze fraudes ontdekt kunt u een paar zaken doen om te voorkomen dat de fraudeurs binnen uw organisatie (of die van anderen) succesvol zijn:

- Laat het valse domein direct blokkeren op uw mailserver
- Monitor uw e-mailverkeer op valse domeinen
- Stuur valse e-mail door naar de fraudeafdeling van de geïmiteerde organisatie. Zie kader valse e-mailboxen.

Aangifte doen van factuurfraude

Aangifte doen van het criminele feit (of feiten) bij de politie is van groot belang. De politie maakt een proces-verbaal op. De beslissing of daarna ook daadwerkelijk vervolging wordt ingesteld ligt bij het Openbaar Ministerie (OM). Aangifte doen van deze vorm van criminaliteit kan bij elk politiebureau. Meldt de fraude ook bij uw bank, zodat de banken deze de informatie kunnen gebruiken bij de monitoring en detectie van toekomstige pogingen tot fraude.

Waarom is aangifte doen van belang?

Succesvol onderzoek doen naar daders begint met informatie van aangiftes. Daarbij is het van belang dat gegevens die herleidbaar zijn tot de criminele feiten ongewijzigd worden toegevoegd aan de aangifte (b.v. de valse factuur, al dan niet digitaal). De aangiftes geven inzicht in de wijze van handelen van de crimineel of organisatie van criminelen. Als elk benadeeld bedrijf aangifte doet wordt meer informatie verzameld en gecombineerd. Hoe meer informatie, hoe groter de kans dat op basis daarvan succesvol onderzoek kan worden gedaan naar de daders.

Valse e-mailboxen

ABN AMRO Bank:
valse-email@nl.abnamro.com
ING Bank:
valse-email@ing.nl
Rabobank:
valse-email@rabobank.nl
SNS Bank:
valse-email@sns.nl
ICS-/ABN AMRO creditcards:
valse-email@icscards.nl
Aegon:
valse-email@aegon.nl
ASN:
valse-email@asnbank.nl
KNAB:
valse-email@knab.nl
Regiobank:
valse-email@regiobank.nl
Triodos Bank:
valse-email@triodos.nl
ZwitserlevenBank:
valse-email@zwitserlevenbank.nl

En stuur valse e-mail van alle pluimage door naar:

Fraudehelpdesk:
valse-email@fraudehelpdesk.nl

Maar ook andere organisaties gebruiken dit format:

Overheidsorganisaties:
valse-email@rijksoverheid.nl
KPN:
valse-email@kpn.com
NS:
Nederlandse Spoorwegen:
valse.email@ns.nl
Marktplaats:
valse-email@marktplaats.nl
Ziggo:
phishing@ziggo.nl
valse-email@ziggo.nl
Intrum Justitia
infol@intrum.com onderwerp
Fraude vermelden

Aangifte doen is ook van belang voor het herkennen van nieuwe vormen van factuurfraude. De informatie uit de aangifte kan leiden tot aanpassingen in beveiligingssoftware, antivirusprogramma's en in updates van systemen. Dit maakt het voor alle mkb-bedrijven weer een stuk veiliger.

Tot slot: de verzekeringsmaatschappij zal een kopie vragen van de aangifte (mits verzekerd tegen cybercrime).

Voorbereid aangifte doen!

Vraag bij het maken van een afspraak om aangifte te doen altijd om de aanwezigheid van een digitaal rechercheur, dat helpt bij het formuleren van de aangifte en zorgt dat deze zo compleet mogelijk wordt opgenomen. Bij het opnemen van de aangifte zal om informatie worden gevraagd die gebaseerd is op de wettekst en dus op de elementen van het strafbare feit, zoals:

- betreft het een aangifte tegen een particulier of een bedrijf?
- zijn er beveiligingsmaatregelen genomen?
- wat is de geschatte schade (uren in geld, immateriële schade) en wat zijn de herstelkosten?
- is er al een verdachte bekend?

Ten slotte; de bank zal dit type fraude niet vergoeden en de ontstane schade wordt doorgaans ook niet door uw verzekeraar vergoed. U heeft immers zelf de betaling uitgevoerd naar het rekeningnummer van de crimineel en deze ondertekend als zijnde correct. Het is daarom ook in uw eigen belang om de in deze brief genoemde preventieve maatregelen te treffen en bij een geslaagde fraudepoging zo snel mogelijk actie te ondernemen.

Colofon

Dit infoblad is een uitgave van de Koninklijke Vereniging MKB-Nederland
Postbus 93002
2509 AA Den Haag
T. 070 – 349 09 09
www.mkb.nl

Dit infoblad is met zorg samengesteld. Er kan echter geen enkele aansprakelijkheid worden aanvaard voor eventuele onjuistheden of onvolkomenheden. Vermenigvuldiging van (delen van) deze uitgave is toegestaan, mits met bronvermelding.

© Copyright Koninklijke Vereniging MKB-Nederland oktober 2016.

Voorbeeld

Zes lange dagen verkeerde Johan Fransen in tergende onzekerheid of de € 400.000 terug zou komen. Het verhaal van één van de vele slachtoffers van CEO-fraude:

Johan Fransen is algemeen directeur van Taaltrainingen BV. Aan het einde van de werkdag komt Adrie naar hem toe met een betaalverzoek. Johan werkt al twintig jaar met hem samen en hij kent Adrie als een uiterst betrouwbare werknemer op de afdeling Finance. Alle informatie die Johan nodig had om de boeking te kunnen beoordelen, leek er te zijn. Steve Jefferson, sinds vier maanden directeur van het Amerikaanse moederbedrijf, had Adrie telefonisch dringend verzocht om snel vier ton over te maken voor de overname van een Chinees bedrijf. Drie dagen later zouden ze dat geld weer terug krijgen.

“Dat Steve nieuw was, heeft een rol gespeeld: nieuwe bezems vegen schoon, je wilt graag meewerken.”

Er speelde in die tijd ook een andere overname in Zweden, dus waarom niet ook eentje in China? Want daar had Steve het over gehad tijdens zijn bezoek aan de vestiging in Nederland. Dat was plausibel. En snelheid en geheimhouding, waar de pseudo-Steve, want dat was hij, op aandrang bij Adrie, horen niet zelden bij overnameprocessen. In perfect Amerikaans legde ‘Steve’ Adrie uit dat hij ook hun financieel directeur, Karin de Jong, al over de zaak had gesproken. Slim van hem. ‘Steve’ wist dat zij de deur uit was. Hij had haar nét daarvoor mobiel proberen te bellen. Van de receptie hoorde hij dat ze weg was. Hij had zich daarom laten doorverbinden met Adrie. In anderhalf uur hebben ze zeven keer telefonisch contact.

‘Steve’ leverde de naam en het e-mailadres van een advocaat, die per e-mail een mandaat afgaf voor de betaling, plus de betaalgegevens. Adrie had het advocatenkantoor, die de overname van het Chinese bedrijf begeleidde, op internet gevonden maar er helaas geen contact mee opgenomen.

Toen Adrie om 17.10 uur naar Johan toe kwam, was hij ervan overtuigd dat het geld zo snel mogelijk overgemaakt moest worden. Hoewel Johan al op het punt stond om naar huis te gaan heeft hij die boekingen van twee keer € 200.000 die Adrie al had klaar gezet, nog even snel opgevoerd. Als hij tien minuten gewacht had, was Johan zeker gaan twijfelen en éérst gaan verifiëren. Nu kwam dat gevoel te laat.

Direct na de boeking begint Johan te twijfelen. Hij heeft contact met Karin, de financieel directeur, en belt om 19.10 uur met de topman van de Engelse vestiging. Zij weten beiden niets over een overname van een Chinees bedrijf. Johan weet nu 100 procent zeker dat het foute boel is. Hij doet vervolgens al het mogelijke om het geld weer terug te krijgen.

Om 19.45 uur krijgt Johan de eerste medewerker van de fraudedesk van de bank aan de lijn. Er wordt speciaal iemand op de zaak gezet: Michiel. Van hem krijgt Johan het gevoel dat hij alles doet wat mogelijk is. Ook als er geen ontwikkelingen waren, nam Michiel contact op. Michiel kon zich verplaatsen in de preciaire situatie waarin Johan terecht was gekomen en handelde daar ook naar.

Johan heeft geluk gehad: op 5 april werd het geld overgeboekt, en op 11 april was het weer terug. Het had ook héél anders kunnen lopen.

Johan verwijt zichzelf dat hij onvoorzichtig is geweest. De fraudeurs zijn echter zéér geraffineerd bezig geweest. Zij hebben zich grondig voorbereid en psychologisch doortrapt gebruik gemaakt van hiërarchische verhoudingen binnen het bedrijf.

Johans belangrijkste tips voor iedereen waar CEO-fraudeurs hun pijlen op zouden kunnen richten: “Laat je niet imponeren door de status van hoge functies, blijf nuchter nadenken en check elementaire dingen: heb ik écht gesproken met de hoogste directeur? Doelwit zijn vaak internationale bedrijven, waar nét een nieuwe CEO is aangetreden. Dat checken van een identiteit kan in een korte tijdspanne: want dat is óók een vast ingrediënt van CEO-fraude, een zeer hoge tijdsdruk genereren. En hou je aan het vier-ogen-principe: laat altijd twee mensen van het management een betaling fiatteren.”

(Alleen de namen en de bedrijfsnaam in dit interview zijn gefingeerd, de feiten kloppen allemaal).

Tekst gebaseerd op een artikel van ABN AMRO: Joep Auwerda