Voorkom misbruik van uw bedrijfsgegevens

FRAUDEHELPDESK.nl

Inleiding

Als ondernemer kunt u te maken krijgen met uiteenlopende vormen van fraude. Vaak gaat het om acties van criminelen die bestaande bedrijven of personen binnen een organisatie imiteren.

Oplichters maken er soms flink werk van u om de tuin te leiden. Ze verdiepen zich in de structuur van een bedrijf en gebruiken deze informatie om geld afhandig te maken van u of van derden.

Het is goed te weten waar de dreiging precies uit bestaat en hoe u het beste kunt reageren als oplichters op uw pad komen.

In deze brochure beschrijven we daarom de meest voorkomende fraudevormen in het bedrijfsleven. Mét adviezen, zodat u beter bent voorbereid op mogelijke pogingen tot oplichting.

Fraude gemeld door het bedrijfsleven

Cijfers 2018

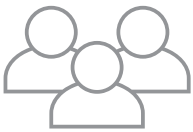
Bijna € 6 miljoen

is de schade die in 2018 door bedrijven is gemeld bij de Fraudehelpdesk.

6.734

meldingen heeft de Fraudehelpdesk in 2018 ontvangen van bedrijven.*

426



slachtoffers die daadwerkelijk geld verloren, hebben zich vorig jaar gemeld.

*) Meldingen zijn alle signalen over fraude die de Fraudehelpdesk ontvangt. Slachtoffers zijn ook daadwerkelijk geld kwijtgeraakt.

CEO-fraude

Bij CEO-fraude ontvangt een medewerker op de financiële administratie een e-mail van de baas. Bij grote, internationale bedrijven is dat de CEO of CFO. Maar met deze fraudevorm worden ook verenigingen en kleine ondernemingen benaderd. In werkelijkheid is de e-mail afkomstig van criminelen die het mailadres van de echte baas goed hebben nagebootst.

De 'baas' draagt de medewerker op een fors bedrag over te maken, bijvoorbeeld voor een overname. Er wordt gevraagd de transactie nog even stil te houden voor andere medewerkers. Meestal is er veel haast geboden bij de overboeking. Ter verificatie van gegevens kan de medewerker in sommige gevallen een advocatenkantoor bellen. Dit 'advocatenkantoor' zit in het complot.

Een dergelijke e-mail mail sturen de fraudeurs heel gericht. Ze achterhalen vooraf wie de CEO is, wie verantwoordelijk is voor het doen van (internationale) betalingen, en wat hun e-mailadressen zijn. Bedrijven waar in het Nederlands wordt gecommuniceerd krijgen Nederlandstalige e-mails en anderen krijgen Engelse mailtjes. En als het taalgebruik informeel of juist heel zakelijk is, dan passen de fraudeurs hun taalgebruik erop aan.

Advies

Als u rekening houdt met de volgende tips, verkleint u de kans dat uw bedrijf getroffen wordt door CEO-fraude:

- Maak uw medewerkers of collega's attent op deze fraudevorm;
- Wees extra alert op verzoeken om grote sommen geld over te maken, zeker als het geld naar een buitenlandse rekening gaat;
- Maak duidelijke afspraken over de werkwijze bij betalingen. Spreek bijvoorbeeld af nooit op basis van alleen een telefoontje of e-mail grote bedragen over te boeken;
- Betrek bij twijfel of bij grote bedragen de direct leidinggevende. Dat zou immers ook de meest voor de hand liggende persoon zijn van wie een dergelijke opdracht zou komen;
- Worden er vaker grote overboekingen gedaan, leg dan procedures vast over hoe een opdracht gecontroleerd kan worden;
- Benadruk dat het van groot belang is dat iedereen zich te allen tijde aan de bestaande werkafspraken houdt;
- Wees u ervan bewust dat alle openbaar geplaatste informatie, bijvoorbeeld op LinkedIn of uw website, kan worden misbruikt.

Misbruik van e-mailgegevens

Het is voor oplichters heel interessant om e-mails te kunnen versturen namens een bestaande organisatie. Ze kunnen zo informatie inwinnen bij andere bedrijven, valse facturen sturen of valse e-mails betrouwbaarder laten lijken.

Zo kunnen cybercriminelen bijvoorbeeld een e-mail versturen namens een bank, waarbij de mail door de bank verstuurd lijkt te zijn. Als afzender is namelijk echt het maildomein van de bank te zien.

Deze truc is voor oplichters vrij eenvoudig. Tenminste, als dat bedrijf én de mailprovider hun beveiliging niet goed op orde hebben. En dat zien we helaas maar al te vaak.

Advies

Gelukkig zijn er technieken ontwikkeld waarmee organisaties misbruik kunnen helpen tegengaan. Voorbeelden van zulke technieken zijn Sender Policy Framework (SPF), DomainKeys Indentified Mail (DKIM) en Domain-based Message Authentication, Reporting & Conformance (DMARC).

U kunt bij de Fraudehelpdesk een (gratis) handleiding opvragen om SPF in te stellen via **communicatie@fraudehelpdesk.nl**

SPF, DKIM en DMARC zijn voor personen met beperkte technische kennis niet eenvoudig om in te stellen. Vraag daarom eventueel uw ICT-leverancier om met deze veiligheidsmaatregelen te helpen.

Misbruik van uw bedrijfsnaam

Het blijkt al jarenlang een lucratieve business voor oplichters: via een online handelsplaats bestellingen binnenhalen, een aanbetaling vragen en vervolgens niet leveren. Bij deze praktijken worden ook vaak namen van bestaande Nederlandse bedrijven misbruikt.

In augustus 2015 deed de Fraudehelpdesk een steekproef op Alibaba.com, een grote Chinese online marktplaats. Maar liefst dertig procent van de 'Nederlandse aanbieders' bleek vals. Het waren malafide partijen die zich verscholen achter de gegevens van bestaande Nederlandse bedrijven.

Advies

Voorkomen dat oplichters op een website een handeltje starten onder uw naam is lastig. Het is verstandig een automatische zoekopdracht op uw bedrijfsnaam in te stellen via Google Alerts. Daarmee wordt internet voortdurend doorzocht op het gebruik van uw naam. Dat kan helpen misbruik in een vroeg stadium te ontdekken.

FRAUDEHELPDESK.nl

Bel met de Fraudehelpdesk

088 786 7372

Domeinnaam-fraude

Bij domeinnaamfraude wordt een ondernemer benaderd door een hostingpartij. Dat gebeurt via e-mail of telefonisch. Het 'hostingbedrijf' zegt dat iemand anders een domeinnaam wil registreren die sterk lijkt op die van uw bedrijf. Het kan ook gaan om exact dezelfde naam maar dan met een andere extensie, zoals .eu, .info of .com.
De beller zegt dat hij verplicht is om u hiervan op de hoogte te stellen. En dat u snel moet handelen om die domeinnaam zelf in handen te krijgen.

De registratie van de domeinnaam vindt vervolgens echt plaats, maar wel tegen veel hogere kosten dan een registratie bij de eigen hostingaanbieder. Bovendien blijkt het verhaal dat een ander deze domeinnaam zou willen registreren over het algemeen niet te kloppen.

Advies

- **Laat u niet verleiden door zo'n telefoontje. De kans is groot dat u te veel betaalt;**
- **Neem contact op met uw eigen hostingbedrijf en vraag bij hen de prijs voor de domeinnaam op;**
- **Is het een risico als uw domeinnaam met andere extensies verschijnt? Laat dan bij voorbaat relevante domeinnamen of extensies vastleggen.**

Spookfacturen

We zien twee soorten spookfacturen:

1. Een factuur blijkt een offerte te zijn

Dit is een aanbieding die eruitziet als een factuur. Allen uit de kleine lettertjes blijkt dat het gaat om een aanbieding. Dit is een vorm van acquisitiefraude. Wanneer u betaalt, gaat u een overeenkomst aan met de afzender. Het sturen van zulke spookfacturen is strafbaar: de afzender mag niet op een verkapte wijze vermelden dat het een offerte betreft.

Advies

Let goed op waarvoor u tekent. Controleer de tekst goed en lees vooral de kleine letters aandachtig.

2. Een factuur zonder tegenprestatie

U ontvangt een factuur zonder dat u opdracht heeft gegeven tot levering van goederen of diensten. Het kan zijn dat er sprake is van een administratieve vergissing of van kwade opzet.

Advies

Van belang is dat u bij de afzender de reden van de factuur opvraagt. De afzender moet kunnen aantonen dat er een overeenkomst met u is, en dat u vooraf bent geïnformeerd over de inhoud van de overeenkomst. Zonder dat bewijs heeft u geen betaalverplichting. Ook het sturen van dergelijke spookfacturen is strafbaar.

Factuurfraude

Factuurfraude draait om het vervalsen van bestaande facturen. Het gaat zowel om geprinte als om digitale facturen: de oplichter onderschept een factuur door poststukken te stelen of door een e-mailaccount te hacken.

Hij wijzigt daarop alleen het rekeningnummer en stuurt de factuur vervolgens weer door naar de persoon die deze ook moest ontvangen. Degene die de rekening betaalt, maakt zonder het te weten geld over naar de fraudeur in plaats van naar het bedrijf dat de nota heeft verstuurd.

Als u de oplichter heeft betaald, blijft de verplichting om de factuur te voldoen aan de echte leverancier bestaan.

Advies

Met de volgende maatregelen maakt u de kans kleiner dat u slachtoffer wordt van factuurfraude:

- Controleer waar mogelijk of het rekeningnummer op een factuur hetzelfde is als op de offerte die eraan voorafging;
- Wijkt een rekeningnummer op een factuur af, neem dan altijd contact op met uw eigen contactpersoon bij de leverancier. Doe dat via het bij u bekende telefoonnummer en niet via het nummer dat op de factuur wordt genoemd;

- Controleer ook of nieuwe contactpersonen inderdaad voor het betreffende bedrijf werken. Ook hier weer via het bij u bekende telefoonnummer van deze leverancier;

- Maak één medewerker binnen uw organisatie verantwoordelijk voor het aanpassen van bankrekeningnummers en zorg dat deze persoon de risico's kent;

- Klik voor het beantwoorden van mail met uw klanten of leveranciers nooit op 'reply', maar selecteer het adres van de ontvanger altijd uit uw eigen adressenbestand;

- Beveilig uw mailserver goed en maak gebruik van een antivirussysteem. Laat uw personeel regelmatig hun inloggegevens aanpassen en zorg ervoor dat ze gebruikmaken van sterke wachtwoorden en tweefactor-authenticatie;

- Beperk het aantal medewerkers dat toegang heeft tot de locatie op uw server waar de facturatiesoftware staat. Wijs hen vervolgens op de gevaren van virusaanvallen;

- Krijgt u een papieren factuur? Vraag voor de zekerheid een digitale versie zodat u die kunt vergelijken met de papieren factuur;

- Controleer elk document voordat u de factuur betaalt. Kijk goed naar het rekeningnummer. Is hier gewerkt met correctievloeistof, ziet u een stempel of een sticker? Neem dan contact op met de afzender. Zo kunt u checken of de factuur en het rekeningnummer kloppen.

Acquisitiefraude

Bij acquisitiefraude benaderen advertentiebureaus ondernemers voor het plaatsen van een advertentie. Het kan gaan om vermeldingen op websites of om advertenties in bladen of magazines. U krijgt een telefoontje of een offerte die sterk lijkt op een factuur.

De verhouding tussen de prijs en wat geboden wordt is niet reëel, blijkt achteraf. Bovendien wordt u met een smoes verleid een overeenkomst aan te gaan. Want de fraudeurs gaan zo te werk dat u ongemerkt akkoord gaat met een contract.

De acquisitiefraudeurs zeggen bijvoorbeeld dat er al sprake is van een zakelijke relatie. U hoeft alleen uw bedrijfsgegevens te controleren op de brief, fax of e-mail die zij sturen. Of er wordt gevraagd of u tegen betaling belangstelling heeft voor verlenging van de ‘gratis’ vermelding op de website van het advertentiebureau. Zo niet, onderteken dan snel het overzicht dat zij sturen.

Maar een handtekening onder het overzicht van te controleren gegevens blijkt de ondertekening van een overeenkomst te zijn. Ook gebeurt het dat gedupeerden er door te knippen en plakken in de opname van een telefoongesprek worden ingeluisd.

De acquisitiefraudeurs bellen bij voorkeur op het drukste moment van de dag. Ze hopen dat u dan eerder toehapt. Vaak is er haast bij: u moet snel beslissen. De verkoopmethode is agressief, zeker als u 'nee' probeert te zeggen.

Advies

Er zijn vele strategieën die advertentiebureaus gebruiken om iemand een overeenkomst aan te smeren. Om ervoor te zorgen dat u niet de dupe wordt van deze advertentiefraude, houdt u de volgende hoofdregels in gedachten:

- Pas altijd op met mondelinge toezeggingen;
- Onderteken en retourneer nooit 'zomaar' een fax, e-mail of poststuk. Let goed op waarvoor u tekent. Controleer de tekst goed en lees vooral de kleine letters aandachtig.

Wat kan de Fraudehelpdesk voor u doen?

Heeft u te maken met (een poging tot) oplichting? Doe dan melding bij de Fraudehelpdesk. Wij kunnen u adviseren en eventueel doorverwijzen.

Om uw mailverkeer te beveiligen kunt u bij ons een (gratis) handleiding opvragen om SPF in te stellen. Hiervoor heeft u wel enige technische kennis nodig.
Mail naar communicatie@fraudehelpdesk.nl

Heeft u een conflict over een (digitale) advertentieplaatsing of de registratie van een domeinnaam? Als er sprake is van onrechtmatig handelen, kan de Fraudehelpdesk tegen aantrekkelijke tarieven juridische bijstand verlenen.

U bent (nog) niet gedagvaard
U bent in conflict en bent nog niet tot betaling overgegaan. Meldt u zich dan hieronder aan als deelnemer. U kunt per jaar gebruikmaken van de volgende diensten:
1 of 2 meldingen: begeleiding bij het maken van in totaal 4 verweerbrieven, verdeeld over de meldingen.
Meer meldingen: eerste 2 brieven € 70,- per stuk. Volgende brieven € 30,- per stuk.

U bent gedagvaard
Als u bent gedagvaard en er is geen samenwerking met een advocaat nodig, kan de Fraudehelpdesk een 'conclusie van antwoord' opstellen. Dit is een reactie op de dagvaarding.

Het tarief voor een eerste conclusie van antwoord inclusief verklaring bedraagt € 295,- per zaak. Een tweede conclusie kost € 125,- per zaak.

FRAUDEHELPDESK.nl

Bel met de Fraudehelpdesk

088 786 7372

Kosten lidmaatschap

De kosten van uw lidmaatschap bedragen, afhankelijk van de grootte van uw bedrijf, per jaar:

1-10 werknemers:	€ 98,-
11-50 werknemers:	€ 170,-
Meer dan 50 werknemers:	€ 285,-
BOVAG-lid?	Dan is deelname voor u gratis!

Genoemde tarieven zijn exclusief btw, de kosten van deelname zijn voor ondernemers van de belasting aftrekbaar.

Het lidmaatschap geldt uitsluitend voor het aangemelde bedrijf en niet voor nevenvestigingen of organisaties die u vertegenwoordigt. Deze dienen zich afzonderlijk aan te melden.

Behandeling van uw zaak

Wilt u dat wij uw zaak in behandeling nemen? Maak dan een melding via onze website.

FRAUDEHELPDESK.nl

Postadres	Postbus 963 7301 BE Apeldoorn
Tel.	088 - 786 7372
E-mail	communicatie@fraudehelpdesk.nl
Web	www.fraudehelpdesk.nl
KvK Arnhem	09138148