CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

Bij CEO/BEC-fraude wordt een medewerker die betalingen mag verrichten, misleid om een valse factuur te betalen of ongeoorloofd van de bedrijfsrekening over te schrijven.

HOE WERKT HET?

De fraudeur belt of mailt en doet zich voor als hooggeplaatst persoon binnen het bedrijf (bv. CEO, CFO).

Ze kennen de organisatie goed.

Ze willen een dringende betaling.

Zij gebruiken taal zoals: 'Vertrouwelijkheid', 'Het bedrijf vertrouwt je', 'Momenteel niet beschikbaar'.

Vaak wordt er gevraagd om internationale betalingen aan banken buiten Europa.

De werknemer schrijft het geld over op een rekening die de fraudeur beheert.

Instructies over de verdere stappen kunnen later worden gegeven, door een derde persoon of via e-mail.

De werknemer wordt gevraagd de gewone toelatingsprocedures niet te volgen.

Ze verwijzen naar een gevoelige situatie (bijvoorbeeld belastingcontrole, fusie, overname).

HOE HERKEN JE HET?

- Ongevraagde e-mail/telefoonoproep
- Rechtstreeks contact met een hooggeplaatst persoon met wie je normaal geen contact hebt
- Vraag om absolute geheimhouding
- Druk en gevoel van dringendheid
- Ongewone vraag in strijd met interne procedures
- Bedreigingen of ongewone vleierij/beloften

WAT KAN JE DOEN?

ALS BEDRIJF

Ken de risico's en zorg ervoor dat **medewerkers ook op de hoogte en bewust zijn.**

Moedig je personeel aan om **voorzichtig te zijn met betalingsverzoeken.**

Voer interne protocollen in voor betalingen.

Voer een controleprocedure in voor per e-mail ontvangen betalingsverzoeken.

Stel **meldingsroutines** vast om fraude te bestrijden.

Controleer informatie op je bedrijfswebsite, **beperk de informatie en wees voorzichtig** met sociale media.

Upgrade en update je technische beveiliging.

Contacteer steeds de politie bij fraudepogingen, zelfs als je niet in de val bent getrapt.

ALS MEDEWERKER

Volg strikt de bestaande beveiligingsprocedures voor betalingen en aanbestedingen. **Sla geen stappen over en geef niet toe aan druk.**

Controleer e-mailadressen altijd zorgvuldig bij gevoelige informatie/overschrijvingen.

Bij twijfel over een betalingsopdracht, **raadpleeg een bevoegde collega.**

Open nooit verdachte links of bijlagen in e-mails. Wees vooral voorzichtig wanneer je je persoonlijke e-mail nakijkt op de bedrijfscomputers.

Beperk informatie en wees voorzichtig met sociale media.

Deel geen informatie over de hiërarchie, veiligheid of procedures van het bedrijf.

Ontvang je een verdachte mail of telefoonoproep, verwittig dan altijd je IT-afdeling.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIE

#CyberScams

BELEGGINGSFRAUDE

Vaak voorkomende beleggingsfraude kan lucratieve beleggingskansen omvatten, zoals aandelen, obligaties, cryptocurrencies, zeldzame metalen, overzeese landinvesteringen of alternatieve energie.

HOE HERKEN JE HET?

- Je wordt snelle winst beloofd en ervan verzekerd dat de belegging veilig is.
- Het aanbod is slechts beperkt beschikbaar.
- Je wordt herhaaldelijk en ongevraagd opgebeld.
- Het aanbod geldt alleen voor jou en je wordt gevraagd om het niet te delen.

WAT KAN JE DOEN?

- **Vraag altijd onpartijdig financieel advies** voordat je geld geeft of belegt.
- **Wijs ongevraagde oproepen** over beleggingsmogelijkheden af.
- **Wees op je hoede voor beloftes van veilige belegging, gegarandeerd rendement en hoge winsten.**
- **Pas op voor toekomstige fraude. Eens je hebt belegd in een oplichting, zullen fraudeurs je waarschijnlijk opnieuw benaderen of je gegevens verkopen aan andere criminelen.**
- **Contacteer de politie als je argwaan hebt.**

EUROPOL EC3 European Cybercrime Centre

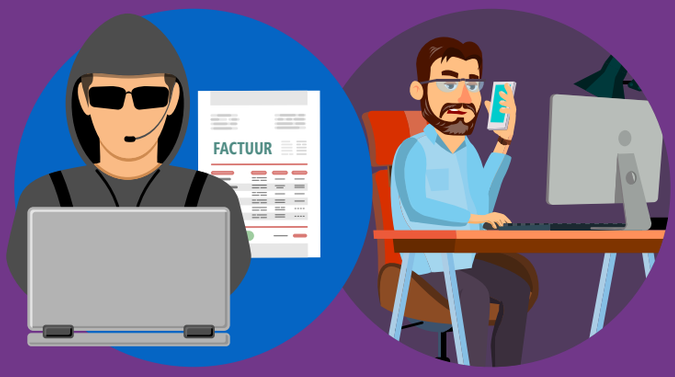
EBF European Banking Federation

POLITIE

#CyberScams

FACTUURFRAUDE

HOE WERKT HET?



- Een bedrijf wordt benaderd door iemand die zich voordoet als leverancier/dienstverlener/schuldeiser.
- Combinatie van benaderingen : telefoon, brief, e-mail, enz.
- De fraudeur vraagt om de bankgegevens voor de betaling (bankgegevens van de begunstigde) van toekomstige facturen aan te passen. Die nieuwe rekening wordt beheerd door de fraudeur.

WAT KAN JE DOEN?

ALS BEDRIJF

Zorg ervoor dat **medewerkers geïnformeerd en zich bewust zijn** van dit soort fraude en hoe ze zich ertegen kunnen wapenen.

Vraag uw medewerkers die facturen betalen om die **altijd na te kijken op onregelmatigheden.**

Werk een **controleprocedure** uit voor de echtheid van betalingsverzoeken.

Controleer de informatie die op de bedrijfswebsite staat, vooral contracten en leveranciers. Zorg ervoor dat uw medewerkers niet teveel delen over het bedrijf via hun sociale media.

ALS MEDEWERKER

Controleer alle verzoeken die van je schuldeisers lijken te komen, vooral als ze vragen om hun bankgegevens voor toekomstige facturen te wijzigen.

Werk een procedure uit om de juiste bankrekening en begunstigde te bevestigen voor betalingen boven een bepaalde limiet (bv. een vergadering met het bedrijf).

Gebruik nooit de contactgegevens op de brief/fax/e-mail dat de wijziging vraagt. Gebruik in plaats daarvan gegevens uit **eerdere correspondentie.**

Nadat een factuur is betaald, **stuur een e-mail naar de ontvanger.** Vermeld voor de veiligheid de naam van de bank van de begunstigde en de laatste 4 cijfers van het rekeningnummer.

Zorg dat je **één duidelijk contactpunt** hebt bij de bedrijven waaraan je regelmatig betaalt.

Beperk de informatie die je deelt over jouw werkgever op sociale media.

Contacteer steeds de politie bij fraudepogingen, ook al ben je niet in de val getrapt.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIE

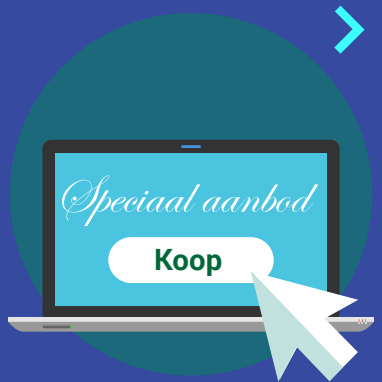
#CyberScams

ONLINE SHOPPING FRAUDE

Online deals zijn vaak interessant, maar pas op voor oplichting.

WAT KAN JE DOEN?

- **Gebruik indien mogelijk binnenlandse winkelwebsites** – zo heb je meer kans om eventuele problemen op te lossen.
- **Maak je huiswerk -** controleer de beoordelingen voor je koopt.



- **Gebruik kredietkaarten -** je hebt meer kans om je geld terug te krijgen.
- **Betaal alleen via een beveiligde betaaldienst -** Vragen ze een overschrijvingsdienst of een bankoverschrijving? Denk goed na!
- Betaal alleen wanneer je verbonden bent met een **beveiligde internetverbinding** - vermijd het gebruik van gratis of openbare wifi.
- **Betaal alleen op een veilig toestel** – Hou je besturingssysteem en beveiligingssoftware up-to-date.
- Pas op voor advertenties met ongeloofwaardige deals of wonderproducten - **Als het te mooi klinkt om waar te zijn, is het dat waarschijnlijk ook!**
- Een pop-up advertentie waarin staat dat je een prijs hebt gewonnen? **Denk er twee keer over na,** je hebt misschien gewoon malware gewonnen.
- Als het product niet aankomt, neem contact op met de verkoper. **Neem contact op met je bank** als je geen antwoord krijgt.

Doe altijd aangifte bij de politie van een vermoede fraudepoging, zelfs als je niet in de val bent getrapt.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIE

#CyberScams

BANK PHISHINGMAILS

Phishing verwijst naar frauduleuze e-mails die de ontvangers misleiden om hun persoonlijke, financiële of beveiligingsinformatie te delen.

HOE WERKT HET?

Deze e-mails:

kunnen er identiek uitzien als de correspondentie die echte banken uitsturen.

kopiëren de logo's, lay-out en toon van echte e-mails.

vragen je een bijlage te downloaden of op een link te klikken.

gebruiken dwingende taal.

WAT KAN JE DOEN?

- **Hou je software up-to-date,** inclusief je browser, antivirus en besturingssysteem.
- Wees vooral **waakzaam** als een 'bank' via mail gevoelige informatie van je vraagt (bv. je wachtwoord voor online bankieren).
- **Kijk goed naar de e-mail:** vergelijk het adres met eerdere echte berichten van je bank. Controleer op slechte spelling en grammatica.
- **Antwoord nooit op een verdachte e-mail,** maar stuur het door naar je bank door het adres zelf in te typen.
- **Klik niet op de link of download de bijlage niet,** maar typ het echte adres van je bank over in je browser.
- **Controleer** in geval van twijfel de website van je bank of bel de bank.

Cybercriminelen rekenen erop dat mensen het druk hebben; op het eerste gezicht lijken deze nepmails echt.

Kijk uit wanneer je een mobiel toestel gebruikt. Het kan moeilijker zijn om een phishingpoging op je telefoon of tablet te herkennen.

#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIE

DATINGFRAUDE

Oplichters mikken op slachtoffers via online datingwebsites, maar leggen ook contact via sociale media of e-mail.

HOE HERKEN JE HET?

Iemand die je onlangs online hebt ontmoet, toont sterke gevoelens voor je en wil privé chatten.

Hun berichten zijn vaak slecht geschreven en vaag.

HAU VAN JOU

Hun online profiel strookt niet met wat ze je vertellen.

Zij kunnen je vragen intieme foto's of video's van jezelf te sturen.

€€€

Eerst winnen ze je vertrouwen. Dan vragen ze om geld, giften of je bankrekening-/kredietkaart-gegevens.

Stuur je geen geld, dan proberen ze je te chanteren. Stuur je wel, dan zullen ze om meer vragen.

BEN JE SLACHTOFFER?

Schaam je niet!
Verbreek onmiddellijk alle contact.
Indien mogelijk, hou alle communicatie bij, zoals chatberichten.
Dien een klacht in bij de politie.
Meld het aan de site waar de oplichter jou eerst heeft benaderd.
Heb je je rekeninggegevens doorgegeven? Contacteer je bank.

WAT KAN JE DOEN?

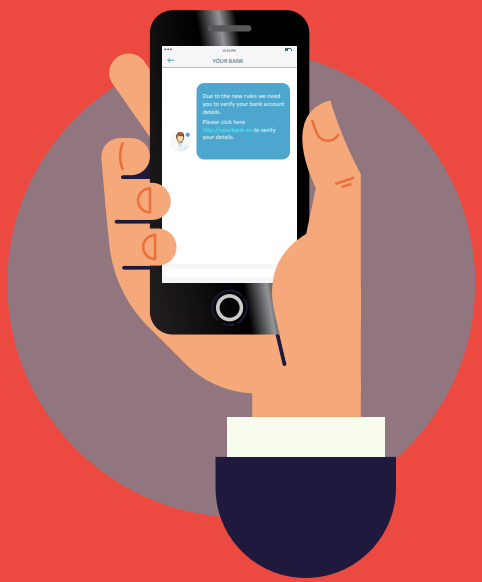
- **Wees heel voorzichtig** over de persoonlijke gegevens die je deelt op sociale netwerk- en datingsites.
- **Houd altijd rekening met de risico's.** Oplichters vind je op de meest gerenommeerde sites.
- **Ga langzaam** en stel vragen.
- **Onderzoek** de foto en het profiel van de persoon om te zien of het materiaal elders is gebruikt.
- **Let op** spelling- en grammaticafouten, tegenstrijdigheden in hun verhalen en excuses zoals dat hun camera niet werkt.
- **Deel geen** compromitterend materiaal waarmee je kan worden gechanteerd.
- Willen jullie elkaar ontmoeten, **vertel familie en vrienden** waar je naartoe gaat.
- **Pas op voor geldverzoeken. Stuur nooit geld, kredietkaart- of rekeninggegevens of kopieën van persoonlijke documenten.**
- **Schiet hen nooit geld voor.**
- **Schrijf geen geld over** voor iemand anders: geld witwassen is een misdrijf.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIE

#CyberScams

SMISHING: SMS'EN VAN EEN VALSE BANK

Smishing (combinatie van SMS en phishing) is een poging van fraudeurs om via sms persoonlijke, financiële of beveiligingsinformatie te verkrijgen.



HOE WERKT HET?

In de sms wordt er je meestal gevraagd op een link te klikken of een telefoonnummer te bellen om je account te 'verifiëren', te 'updaten' of 'opnieuw te activeren'. Maar de link leidt naar een valse website en het telefoonnummer naar een fraudeur die zich voordoet als het echte bedrijf.

WAT KAN JE DOEN?

- **Klik niet op links, bijlagen of afbeeldingen** die je ontvangt in ongevraagde sms-berichten zonder eerst de afzender te controleren.
- **Laat je niet opjagen.** Neem je tijd en voer de nodige controles uit voordat je reageert.
- **Reageer nooit op een sms-bericht** waarin je PIN of wachtwoord voor online bankieren of andere veiligheidsgegevens worden gevraagd.
- Als je denkt dat je op een smishingbericht hebt gereageerd en je bankgegevens hebt opgegeven, **contacteer onmiddellijk je bank.**

EUROPOL EC3 European Cybercrime Centre

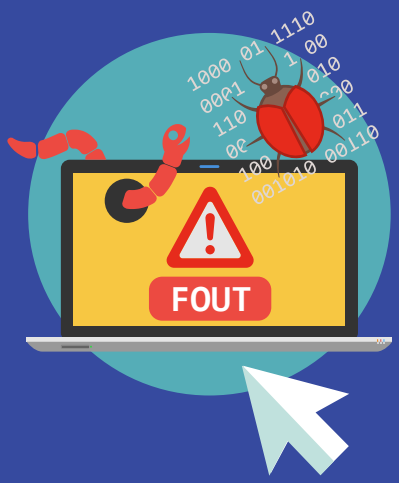
EBF European Banking Federation

POLITIE

#CyberScams

VALSE BANKWEBSITES

Phishingmails van banken bevatten meestal links naar een valse website van een bank waar je wordt gevraagd om je financiële en persoonlijke gegevens te geven.



HOE HERKEN JE HET?

Valse websites van banken zien er bijna hetzelfde uit als de echte websites. De websites tonen vaak een pop-upvenster dat vraagt om je bankgegevens in te voeren. Echte banken gebruiken zo'n vensters niet.

Kenmerken van deze websites:

Dwingende taal: zo'n berichten vind je niet op legitieme websites.

Pop-upvensters: ze worden vaak gebruikt om gevoelige informatie van jou te verzamelen. Klik er niet op en geef je persoonsgegevens niet in op deze vensters.

Slecht design: wees voorzichtig met websites die design-, spelling- of grammaticafouten hebben.

WAT KAN JE DOEN?

Klik nooit op links in e-mails die leiden naar de website van je bank.

Typ de link van je bank altijd handmatig of gebruik een bestaande link uit je 'favorieten' lijst.

Gebruik een browser om **pop-upvensters te blokkeren.**

Als iets belangrijks echt je aandacht vereist, zal je bank je waarschuwen **wanneer je je onlinerekening bezoekt.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLITIE

#CyberScams

VISHING: TELEFOONOPROEPEN VAN EEN VALSE BANK

Vishing (woordcombinatie van voice en phising) is telefoonfraude waarbij de fraudeurs het slachtoffer misleiden om persoonlijk, financiële of beveiligingsgegevens te delen of om hen geld over te schrijven.

WAT KAN JE DOEN?

- **Let op** voor ongevraagde telefoonroepen.
- **Noteer het nummer van de beller** en vertel dat je hen terugbelt.
- Om hun identiteit te valideren, **zoek het telefoonnummer van de organisatie op** en neem rechtstreeks contact op met hen.
- **Vertrouw het telefoonnummer dat de beller je opgeeft niet** (dit kan een vals nummer zijn).
- Fraudeurs kunnen je basisgegevens online vinden (bv. via sociale media). **Ga er niet van uit dat een beller** echt is alleen maar omdat ze die gegevens hebben.
- **Deel nooit** de PIN-code van je krediet- of bankkaart of je wachtwoord voor online bankieren. Jouw bank zal nooit om dergelijke gegevens vragen.
- **Schrijf geen geld over** naar een andere rekening op hun verzoek. Jouw bank zal je dit nooit vragen.
- Als je denkt dat het een valse oproep is, **meld dit dan aan je bank.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLITIE

#CyberScams