# Wanted: De oplichtings-praktijken die je bedrijf bedreigen.

## Hier zijn de 10 ‘Most wanted’ cyberdreigingen.

Cyberaanvallen zijn een enorm probleem. De aan slachtoffers toegebrachte schade bedroeg in 2023 wereldwijd €9 biljoen. Een verbijsterend bedrag. De aanvallen hebben invloed op bedrijven van alle formaten.

In dit document belichten we de meest gebruikte scams en laten we zien wat je moet doen om jezelf en je bedrijf te beschermen.


brother
at your side

## Meer dan de helft van alle cyberaanvallen wordt gepleegd tegen kleine en middelgrote bedrijven.

En dat resulteert in schokkende cijfers. 60% van de kmo’s gaat binnen de 6 maanden na een cyberaanval falliet*.

Zelfs als een bedrijf een aanval overleeft, kunnen de gevolgen verstrekkend zijn - van financiële verliezen tot de sluiting.

Met deze significante gevolgen in gedachten, stelden we een lijst met de meest bedreigende cyberoplichtingspraktijken samen. We onderzochten ook welke aspecten bedrijven beter beschermen tegen cyberdreigingen.

Een recente enquête van Brother toonde aan dat IT managers zich onvoldoende toegerust voelen om enkele veel voorkomende cyberdreigingen aan te pakken. Malware, ransomware en phishing aanvallen zijn hierbij de belangrijkste risico’s die problemen veroorzaken.

Het opzetten en handhaven van veilige IT systemen is een universeel probleem.

44% van de IT experts beschouwen het beheer van deze systemen als hun grootste uitdaging.

* TechRound maart 2023

## Brother staat ‘At your side’ om hulp te bieden.

De praktische informatie over het voorkomen van cyberaanvallen vinden is niet eenvoudig. Wat zijn precies de risicogebieden en hoe kan je ze herkennen en beveiligen?

We legden enkele van de meest ongebruikelijke en impactvolle oplichtingspraktijken bloot. Het resultaat? We geven je een duidelijk overzicht van de kennis en tools die je helpen je bedrijf of organisatie veilig te houden, zonder dat je hier een dagtaak aan hebt.

Hierna volgt onze lijst met de 10 ‘Most wanted’ cyberdreigingen. Bereid je goed voor op de grootste gevaren die in de digitale wereld op de loer liggen.


## Wist je dat?

**Het meest geïmiteerde merk is Microsoft (29%), gevolgd door Google (13%) en Amazon (13%).**

## Oplichtingsmethode

Een werknemer ontvangt een bericht, meestal een e-mail, van een ogenschijnlijk vertrouwd merk - zoals Apple of Google. Het kan zelfs een bericht zijn op Microsoft Teams.

Net als veel oplichtingspraktijken meldt het bericht dat er DRINGENDE actie nodig is, zoals het bekendmaken van account-, betaal- of wachtwoordinformatie.

Helaas gaan phishing oplichtingspraktijken meestal gepaard met het nabootsen van bekende merken zoals Microsoft, Amazon, DocuSign en Google om gebruikers te misleiden. Sterker nog, in 2022 werden meer dan 30 miljoen berichten met Microsoft branding of vermelding van Microsoft producten gebruikt in phishing aanvallen*.

## Mogelijke gevolgen voor je bedrijf of organisatie

Door zelfs kleine stukjes informatie weg te geven, krijgen hackers de gegevens die ze nodig hebben om toegang te krijgen tot de accounts van je klanten, wachtwoorden te achterhalen en uiteindelijk je geld te stelen.

* Forbes, maart 2023

**Geef alle collega’s regelmatig trainingen over cyberbeveiliging, met een sterke focus op het herkennen van verdachte links. Er is slechts één klik nodig voor een rampscenario.**

## Waarom trappen mensen erin

Dit type oplichting vertrouwt op de bekendheid van en het vertrouwen dat we hebben in de merken waarmee we elke dag werken. Samen met het wekken van de schijnbare urgentie worden werknemers erin geluisd.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Controleer het e-mailadres - is dit in het juiste formaat van de organisatie?
- Ziet het eruit als een echte e-mail van het betreffende merk?
- Let op voor Microsoft Teams berichten die er verdacht uitzien.
- Controleer op voor de hand liggende spelfouten.
- Wees alert als er nadruk wordt gelegd op urgentie - dit is altijd een waarschuwingssignaal dat er iets niet klopt.


**LinkedIn is een professioneel sociaal netwerk is. Dat betekent niet dat het ook alijd veilig is.**

## Oplichtingsmethode

LinkedIn is een belangrijk doelwit voor phishing oplichtingspraktijken. Criminelen proberen uitingen van dit platform na te bootsen, zoals valse vacatureaanbiedingen, misleidende gesprekken over persoonlijke connecties, en zelfs potentiële romantische connecties. Deze oplichtingspraktijken - gebruikers misleiden om gevoelige informatie te delen - worden steeds gebruikelijker. Zodra een imitator het vertrouwen van iemand heeft gewonnen, is het veel eenvoudiger om hen uit te buiten.

## Mogelijke gevolgen voor je bedrijf of organisatie

Imitators vragen om persoonlijke gegevens of sturen malware die vermomd is als belangrijke documenten. Dat geeft hen uiteindelijk toegang tot verdere gegevens, waardevolle bestanden of zelfs zakelijke bankrekeningen.

## Waarom trappen mensen erin

Dit type oplichting steunt op het vertrouwen dat we hebben in een professioneel platform zoals LinkedIn. Fraudeurs bootsen vaak ook recruiters na, die geweldige voordelen beloven en profiteren van de wens van mensen om thuis te werken.

**Een recent onderzoek van Check Point Research* onthulde dat LinkedIn het meest nagebootste merk is bij phishing aanvallen.**

* Infosecurity Magazine, april 2022

## Tips om je bedrijf en medewerkers te beschermen

- Zorg ervoor dat iedereen in het bedrijf zich bewust is van de gevaren en waakzaam blijft ingeval van benadering via social media.
- Wees op je hoede voor ongevraagde berichten.
- Controleer alle bestanden die men vraagt te downloaden.


**Waarschuw je medewerkers voor QR codes in multi-factor authenticatie berichten.**

## Oplichtingsmethode

QR codes vind je overal. Als medewerkers een e-mail ontvangen met de vraag om er een te scannen, moeten ze voorzichtig zijn. Maar niet alle QR codes zijn veilig.

De valse codes duiken overal op, maar meestal in valse e-mails voor multi-factor authenticatie of voor het vrijgeven van documenten. Zelfs in het openbaar komen misleidende QR codes voor.

Een recente zwendel kostte een vrouw €15.000, nadat ze een valse QR code had gebruikt voor de betaling van een parkeerplaats. De code leidde het 71 jarige slachtoffer naar een nepwebsite waar ze haar betaalgegevens invoerde. De oplichters stalen haar betalings- en kaartinformatie.

## Mogelijke gevolgen voor je bedrijf of organisatie

Onveilige QR codes verwijzen je medewerkers door naar nepbedrijfswebsites, betaalwebsites en kwaadaardige netwerken. Ze kunnen stiekem code uitvoeren op hun apparaten en uiteindelijk geld en gevoelige gegevens van je bedrijf stelen.

* Independent, november 2023

## Waarom trappen mensen erin

Bedrijven gebruiken elke dag multi-factor authenticatie, vooral bij het gebruik van merken zoals Microsoft. Mensen zijn gewend om hun gegevens te verstrekken en denken vaak niet na voordat ze hun gegevens invoeren.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Denk na voordat je een QR code scant. Handel niet impulsief.
- Bekijk eerst de link van de QR code voordat je deze scant.
- Controleer of de URL er legitiem uitziet en geen spelfouten bevat.
- Scan geen onverwachte QR codes van vreemden of onbekende bedrijven.
- Bij twijfel, neem je contact op met je IT afdeling.


**Het geven van toegang aan personeel tot bedrijfsaccounts is handig, maar het brengt ook risico's met zich mee. Dergelijke fraude heeft bedrijven de afgelopen jaren miljoenen gekost.**

## Oplichtingsmethode

Criminelen doen zich voor als de bank waarbij je een zakelijke rekening hebt om het geld van je bedrijf te stelen. Dit geberurt in het bedrijfsleven én in het dagelijks leven. Naar schatting ontvangt de helft van de volwassenen elke maand een phishing bericht met dergelijke inhoud.

Oplichters nemen contact op met je bedrijf via telefoon, sms of e-mail; ze beweren vaak dat een verdachte transactie moet worden geverifieerd. Ze vragen om te klikken op een link naar een valse aanmeldingspagina, om vervolgens inloggegevens te stelen en toegang te krijgen tot je account. Sommigen gebruiken zelfs nepbank apps.

Het haarverzorgingsmerk Kent Brushes weet hier alles van. In slechts 20 minuten verloren het ongeveer €1,8 miljoen. Een van hun werknemers werd misleid om dieven toegang te geven tot de bedrijfsrekening…*

## Mogelijke gevolgen voor je bedrijf of organisatie

Als cybercriminelen toegang hebben tot één account, kunnen ze ook in andere accounts inbreken, waaronder e-mail, bank- of andere financiële rekeningen.

* BBC.co.uk, oktober 2023

## Waarom trappen mensen erin

Bedrijven vertrouwen, net als mensen, op hun bank. Ze zijn zeer op hun hoede om slachtoffer te worden van fraude en kunnen gemakkelijk misleid worden door het verhaal over een 'verdachte transactie' waarvoor actie moet worden ondernomen.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Je bank zal nooit uit zichzelf vragen naar wachtwoorden of het overmaken van geld naar nieuwe rekeningen.
- Stuur nooit bankgegevens via sms berichten.
- Klik niet op onverwachte of verdacht uitziende links.
- Let op verdachte spelfouten op inlogpagina's van banken.


**Niemand is veilig voor pretexting. Zelfs je CEO kan het doelwit zijn. En hoe drukker de persoon het heeft, des te groter de kans om een fout te maken.**

## Oplichtingsmethode

Misschien heb je al gehoord van een oplichtingsmethode ‘pretexting’. De cybercrimineel bootst een echte persoon na (meestal een senior lid van je bedrijf) en gebruikt een geloofwaardig verhaal om een gerichte werknemer te misleiden. Sommigen gebruiken zelfs audioclips.

Ze vragen de werknemer om gevoelige informatie of zelfs geld af te staan, vaak zeggend dat hun baan ervan afhangt.

## Mogelijke gevolgen voor je bedrijf of organisatie

Deze criminelen doen onderzoek en gebruiken nauwkeurige informatie die ze online of elders vinden. Ze versterken deze geloofwaardigheid met nep telefoonnummers en e-mailadressen. Het kan je bedrijf veel geld kosten.

## Waarom trappen mensen erin

Dit type oplichting vertrouwt op onze angst voor autoriteit en het verliezen van onze baan. Ze gebruiken ook echte informatie en construeren een geloofwaardig verhaal.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Onthoud dat je bank nooit vraagt om wachtwoorden of geld over te maken naar nieuwe accounts.
- Verstuur nooit bankgegevens via sms berichten.
- Klik niet op onverwachte of verdachte links.
- Let op spelfouten op inlogpagina’s van banken.


**Medewerkers die geld uitgeven (zelfs aan kantoormateriaal) hebben baat bij extra training over het herkennen van valse e-mails of berichten.**

## Oplichtingsmethode

Bij BEC fraude (Business Email Compromise) doen criminelen zich voor als potentiële klanten en sturen dan realistische e-mails naar specifieke werknemers. Ze vragen ongebruikelijke betalingen, sturen links naar valse websites of vragen gewoon om producten te kopen die dan worden aangekocht met gestolen creditcards.

In tegenstelling tot standaard phishing e-mails die men naar miljoenen mensen stuurt, zijn BEC aanvallen bestemd voor specifieke individuen, waardoor ze moeilijker te detecteren zijn.

## Mogelijke gevolgen voor je bedrijf of organisatie

Alle bedrijven, groot en klein, lopen risico. 29% van de bedrijven is al eens een klant kwijtgeraakt door een BEC fraude*.

MGM was het slachtoffer van een BEC fraude die hun hele computersysteem uitschakelde. Dit kostte hen €100 miljoen**.

Met informatie uit een LinkedIn post deed een cybercrimineel zich voor als een MGM medewerker en belde hun IT afdeling. Ze vroegen om hun wachtwoord opnieuw in te stellen. Dit gaf de fraudeur toegang tot de account van deze werknemer. Hij nam uiteindelijk het hele systeem van MGM over.

Alles, van digitale hotelkamersleutels tot gokautomaten en de websites van veel vestigingen, ging offline. Het bedrijf ging in manuele modus om operationeel te blijven. Gasten stonden urenlang in de rij om in te checken en fysieke kamersleutels te krijgen of ontvingen handgeschreven bonnetjes voor het casino.

## Waarom trappen mensen erin

Oplichters richten zich op mensen in je bedrijf die waarschijnlijk geld uitgeven. Ze profiteren van de zorgen over kosten, maken misbruik van de onzekerheid over inkomsten en richten zich op bedrijven die wanhopig op zoek zijn naar verkopen en binnenkomende betalingen.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Hou je aan de officiële werkwijzen met betrekking tot financiële transacties.
- Wees argwanend tegenover e-mails van organisaties waarmee je geen zaken doet.
- Wees je bewust van welke informatie openbaar beschikbaar is.
- Controleer of mensen echt zijn wie ze beweren te zijn.
- Gebruik verschillende wachtwoorden voor al je accounts.
- Let op bij dringendheid.

* Security Infowatch, maart 2022

** Reuters.com, oktober 2023


**Brother printers zijn standaard beveiligd en voorzien van drielaagse beveiliging op netwerk-, apparaat- en documentniveau.**

## Oplichtingsmethode

Meer dan 1 op de 10 beveiligingsincidenten die een bedrijf treffen, hebben te maken met een printer*. Het klinkt misschien als iets uit een goedkope horrorfilm, maar wanneer hackers kwetsbare printerapparatuur aanvallen, is dat zeer verontrustend. Ze nemen controle over je printers en printen berichten, zoals ‘je bent gehackt’, om te bewijzen dat ze je netwerk kunnen infiltreren. Vervolgens dreigen ze om verder te gaan.

## Mogelijke gevolgen voor je bedrijf of organisatie

Naast het opscheppen over hun vaardigheden, is het voor criminelen een manier om in je netwerk binnen te dringen en meer geavanceerde aanvallen te lanceren. Printers zijn een toegangspoort tot belangrijkere bronnen, zoals bestandsservers en e-mailservers.

* Quocirca, oktober 2023

## Waarom trappen mensen erin

Bedrijven beschouwen printers vaak als een laag risico. Maar niets is minder waar. Printers verwerken gevoelige gegevens en hackers zien ze als een onbewaakte achterdeur naar je organisatie.

**Met een beveiligde printfunctie krijgt niemand toegang tot je apparaten. Zorg ervoor dat je firmware up-to-date is en dat al je printers beveiligd zijn.**

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Hou je printers uit de buurt van ongeautoriseerde gebruikers.
- Vraag om authenticatie voor printerinterfaces.
- Gebruik sterke wachtwoorden.
- Zorg dat printopdrachten versleuteld zijn tijdens de verzending naar de printer om onderschepping van informatie en manipulatie te voorkomen.
- Hou firmware up-to-date.


**Van het installeren van antivirussoftware tot het beveiligen van de Wi-Fi in je bedrijf - je gegevens veilig houden is heel belangrijk.**

## Oplichtingsmethode

Dit is waarschijnlijk de meest opvallende oplichting in onze 'Most wanted' lijst. Criminelen richten zich op grote organisaties, vaak in de gezondheidszorg, financiële en energiesector. Ze stelen grote hoeveelheden privacygevoelige gegevens, waarvoor ze 'losgeld' eisen.

Ze gebruiken phishing e-mails, gestolen identiteiten en zwakke plekken in de beveiliging van systemen om binnen te geraken.

Royal Mail werd getroffen door een ransomware-aanval van een criminele groepering die dreigde de gestolen informatie online te publiceren. Royal Mail kon hierdoor geen pakketten of brieven meer naar het buitenland versturen*.

## Mogelijke gevolgen voor je bedrijf of organisatie

In de meeste landen zijn organisaties wettelijk verplicht om alle persoonlijke gegevens die ze bewaren te beschermen. Datalekken kunnen tot aanzienlijke boetes leiden. Momenteel bedragen de gemiddelde kosten van een datalek circa € 5,1 miljoen**.

Een van de meest recente en ernstige datalekken vond plaats in het Verenigd Koninkrijk. Criminelen hadden het gemunt op de verkiezingscommissie en kregen toegang tot de persoonlijke gegevens van ongeveer 40 miljoen mensen. Er is geen bewijs dat de gegevens misbruikt werden, maar het feit dat men toegang kreeg, toont aan dat de beveiliging niet voldoende was***.

* The Guardian, januari 2023 ** IBM, januari 2023 ***bbc.co.uk, augustus 2023

## Waarom trappen mensen erin

Criminelen azen op de zwakke plekken in organisaties. Gecompromitteerde e-mails, cloud misconfiguratie, ongepatchte kwetsbaarheden en een gebrek aan goede training zijn allemaal potentiële redenen om binnen te dringen.

**Elke dag zijn er nieuwe meldingen van datalekken bij een aantal van de grootste bedrijven ter wereld. Niemand is immuun. En ze leiden vaak tot forse boetes of zelfs vervolging.**

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Zorg voor beveiliging in elke fase, van softwareontwikkeling tot implementatie, en test deze regelmatig.
- Gebruik technologieën voor gegevensbeveiliging wannneer data worden verplaatst tussen verschillende databases, applicaties en services.
- Zorg voor een volledig opgeleid team dat klaarstaat om direct te reageren op een incident en de impact te beperken.
- Implementeer krachtige theoretische en praktijktrainingen m.b.t. gegevensbeveiliging.


**Het kan verleidelijk zijn om door te klikken op onbekende gescande documenten, maar pas op voor misleiding en weersta je nieuwschierigheid.**

## Oplichtingsmethode

Een willekeurige e-mail van een kantoorprinter meldt dat een collega een nieuw document heeft gescand. Alle details lijken echt. Er is zelfs een bericht dat het document veilig gescand is en een copyrightmelding. Vervolgens geven twee links de optie om het document te bekijken of te downloaden. Pas op! Dit is een phishing e-mail.

## Waarom trappen mensen erin

Deze oplichting is gevaarlijk omdat het afkomstig is van een vertrouwd kantoorapparaat. Het is zeer ongebruikelijk dat een dergelijk apparaat je een mail stuurt, maar nieuwsgierigheid kan je toch verleiden tot het klikken op een onbekende link en delen van gegevens.

## Mogelijke gevolgen voor je bedrijf of organisatie

De links brengen je naar een nepwebsite waar scammers proberen e-mail wachtwoorden te achterhalen om spam e-mails te versturen, malware te verspreiden en mogelijk toegang te krijgen tot financiële gegevens.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Wees op je hoede voor bijlagen en links in onverwachte e-mails.
- Download alleen bestanden van betrouwbare bronnen.
- Pas op wanneer er urgentie wordt gevraagd.


**Door AI tools, zoals ChatGPT, herken je phishing e-mails moeilijker. Dit verhoogt het risico voor bedrijven aanzienlijk.**

## Oplichtingsmethode

We weten allemaal hoe we een phishing e-mail herkennen. Ze zitten vol spelfouten en erbarmelijke grammatica. Nu niet meer! Criminelen gebruiken AI tools, zoals ChatGPT en chatbots, om phishing berichten te sturen met perfecte spelling en grammatica.

## Waarom trappen mensen erin

Door geloofwaardige phishing e-mails te sturen, is de kans groter dat slachtoffers ze vertrouwen en persoonlijke info en accountgegevens delen.

## Mogelijke gevolgen voor je bedrijf of organisatie

Frauduleuze communicatie lijkt authentieker en betrouwbaarder. Als het vertrouwen is gewonnen, verzamelen criminelen aanvullende persoonlijke gegevens om zich vervolgens voor te doen als bekende personen of hun accounts. Phishing e-mails zijn met maar liefst 1265% toegenomen en AI speelt daar een grote rol in*.

## Tips om je bedrijf en medewerkers te beschermen

- Hou iedereen in je bedrijf op de hoogte van de gevaren.
- Wees voorzichtig met de informatie die medewerkers delen.
- Geef geen inloggegevens en wachtwoorden door.
- Wees voorzichtig met openbaar beschikbare gegevens. Cybercriminelen kunnen deze tegen je gebruiken.
- Controleer of mensen zijn wie ze beweren te zijn.

* CNBC, november 2023

# Bescherm je bedrijf tegen de 10 ‘Most Wanted’ oplichtingsmethodes

Nu je deze informatie hebt gelezen, herken je het gedrag, de methodes en trucs van cybercriminelen.

Maar liefst 60% van de kleine en middelgrote bedrijven die getroffen worden door een cyberaanval gaan na 6 maanden failliet. Hou deze gids binnen handbereik en deel hem met je collega’s.

Met Brother ‘At your side’ ben je oplichters een stap voor en behoed je je bedrijf of organisatie voor een potentiële cyberaanval met catastrofale gevolgen.

brother
at your side