Wanted: De oplichtings-praktijken die uw bedrijf bedreigen.

Hier zijn de 10 ‘Most wanted’ cyberdreigingen.

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

In dit document belichten wij de meest gebruikte scams en laten zien wat u moet doen om uzelf en uw bedrijf te beschermen.

brother
at your side

Meer dan de helft van alle cyberaanvallen wordt gepleegd tegen MKB-bedrijven.

En dat resulteert in schokkende cijfers. Van de aangevallen MKB-bedrijven gaat 60% binnen 6 maanden failliet, nadat ze slachtoffer zijn geworden van een hack*.

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

Met deze significante consequenties in gedachten, hebben we een lijst samengesteld van de meest bedreigende cyber oplichtingspraktijken. Bovendien hebben we onderzoek uitgevoerd naar de aspecten die bedrijven beter in staat stellen om cyberdreigingen het hoofd te bieden.

Een recente enquête van Brother toonde aan dat IT-managers zich onvoldoende uitgerust voelen om enkele zeer gangbare cyberdreigingen aan te pakken, waarbij malware, ransomware en phishing-aanvallen de belangrijkste gebieden zijn die problemen veroorzaken.

Het opzetten en handhaven van veilige IT-systemen is een universele uitdaging.

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

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

Het vinden van de praktische informatie over het vermijden en voorkomen van cyberaanvallen is niet eenvoudig. Wat zijn precies de risicogebieden en hoe kunt u deze herkennen en beveiligen?

Om die vraag te beantwoorden hebben we enkele van de meest ongebruikelijke en impactvolle oplichtingspraktijken blootgelegd. En we geven een overzicht van de kennis en tools die u in staat stellen om uw bedrijf of organisatie veilig te houden, zonder dat u hier een dagtaak aan heeft.

Neem een kijkje op onze lijst met de 10 ‘Most wanted’ cyberdreigingen, zodat u goed voorbereid bent op de grootste gevaren die in de digitale wereld op de loer liggen.

* TechRound maart 2023

Wist u 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, bijvoorbeeld. Het kan zelfs een bericht zijn op Microsoft Teams.

Net als veel oplichtingspraktijken zal het bericht melden 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 phishingaanvallen*.

Mogelijke gevolgen voor uw 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 uw klanten, wachtwoorden te achterhalen en uiteindelijk uw geld te stelen.

* Forbes, maart 2023

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

Waarom trappen mensen erin

Dit type oplichting vertrouwt op de bekendheid en het vertrouwen dat we hebben in de merken waarmee we elke dag werken. Dat, samen met de schijnbare urgentie die gewekt wordt, zorgt ervoor dat werknemers erin worden geluisd.

Tips om uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het 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 wellicht iets niet klopt.

Omdat LinkedIn een professioneel sociaal netwerk is, 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, ontworpen om gebruikers te 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 uw bedrijf of organisatie

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

Waarom trappen mensen erin

Dit type oplichting stent op het vertrouwen dat we hebben in een professioneel platform zoals LinkedIn. Fraudeurs zullen vaak ook recruiters nabootsen, die geweldige voordelen beloven en profiteren van de wens van mensen om vanuit huis 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 uw bedrijf en medewerkers te beschermen

- Zorg ervoor dat iedereen in het bedrijf zich bewust is van de gevaren en waakzaam blijft wanneer ze worden benaderd via social media.
- Wees op uw hoede voor ongevraagde berichten.
- Controleer alle bestanden die u wordt gevraagd te downloaden.

Waarschuw uw medewerkers voor QR-codes die worden gebruikt in multi-factor authenticatie berichten.

Oplichtingsmethode

QR-codes zijn overal te vinden. Dus als een medewerker een e-mail krijgt waarin wordt gevraagd om er een te scannen, denken ze misschien niet twee keer na. Maar niet alle QR-codes zijn veilig om te scannen.

De valse codes kunnen overal opduiken, maar de meest voorkomende plekken zijn valse e-mails voor multi-factor authenticatie of voor het vrijgeven van documenten. Maar 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 om voor parkeren te betalen. De code leidde het 71-jarige slachtoffer naar een nepwebsite waar ze haar betaalgegevens invoerde, waardoor oplichters haar betalings- en kaartinformatie konden stelen.

Mogelijke gevolgen voor uw bedrijf of organisatie

Onveilige QR-codes kunnen uw medewerkers doorverwijzen naar nepbedrijfswebsites, betalingswebsites en kwaadaardige netwerken. Ze kunnen stiekem code op hun apparaten uitvoeren, om uiteindelijk geld en gevoelige gegevens van uw bedrijf te stelen.

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, dus ze denken vaak niet twee keer na voordat ze hun gegevens invoeren.

Tips om uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het bedrijf op de hoogte van de gevaren.
- Denk na voordat u een QR-code scant. Handel niet impulsief.
- Bekijk eerst de link van de QR-code voordat u 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 contact op met uw IT-afdeling.

* Independent, november 2023

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

Oplichtingsmethode

Deze oplichting houdt in dat criminelen zich voordoen als de bank waarbij u een zakelijke rekening heeft, in een poging om het geld van uw bedrijf te stelen. En het is net zo wijdverbreid in het bedrijfsleven als in het dagelijks leven, met naar schatting de helft van de volwassenen die elke maand een phishingbericht met dergelijke inhoud ontvangt.

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

Het haarverzorgingsmerk Kent Brushes weet hier alles van, omdat ze in slechts 20 minuten ongeveer €1,8 miljoen verloren. Een van hun werknemers werd misleid om dieven toegang te geven tot de bedrijfsrekening en de rest is geschiedenis*.

Mogelijke gevolgen voor uw bedrijf of organisatie

Zodra een cybercrimineel toegang heeft tot één account, kunnen ze in meer 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, dus kunnen gemakkelijk misleid worden door het verhaal over een 'verdachte transactie' waarop actie ondernomen moet worden.

Tips om uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het bedrijf op de hoogte van de gevaren.
- Uw bank zal nooit uit zichzelf om wachtwoorden vragen, of om geld dat moet worden overgemaakt 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 uw CEO kan het doelwit zijn. En hoe drukker de persoon, des te groter de kans dat ze een fout maken.

Oplichtingsmethode

Misschien heeft u gehoord van een oplichtingsmethode genaamd ‘pretexting’. Het is waar een cybercrimineel een echte persoon nabootst (meestal een senior lid van uw bedrijf) en een geloofwaardig verhaal gebruikt om een gerichte werknemer te misleiden. Sommigen gaan zelfs zo ver om audioclips te gebruiken.

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

Mogelijke gevolgen voor uw bedrijf of organisatie

Deze criminelen doen onderzoek en gebruiken nauwkeurige informatie die ze online of elders hebben gevonden. Ze zullen deze geloofwaardigheid versterken met nep-telefoonnummers en e-mailadressen. En het kan uw 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 uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het bedrijf op de hoogte van de gevaren.
- Onthoud, uw bank zal nooit vragen om wachtwoorden of om 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 bedrijfsmatig regelmatig online spullen bestellen, zoals bijvoorbeeld kantoorbenodigdheden, kunnen baat hebben 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 phishingmails die men naar miljoenen mensen stuurt, zijn BEC-aanvallen bestemd voor specifieke individuen, waardoor ze moeilijker te detecteren zijn.

Mogelijke gevolgen voor uw 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 het 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 gingen 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 kregen handgeschreven bonnetjes voor het casino.

Waarom trappen mensen erin

Oplichters zullen zich richten op mensen in uw bedrijf die waarschijnlijk geld uitgeven. Ze zullen profiteren van de zorgen over kosten, en elke onzekerheid benutten wat betreft inkomsten. Ze zullen zich ook richten op bedrijven die wanhopig op zoek zijn naar verkopen en betalingen.

Tips om uw bedrijf en medewerkers te beschermen

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

* Security Infowatch, maart 2022

** Reuters.com, oktober 2023

Brother printers zijn standaard beveiligd en bieden 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 dit zeer verontrustend. Ze zullen de controle over uw printers overnemen en berichten beginnen te printen zoals ‘u bent gehackt’, om te bewijzen dat ze uw netwerk kunnen infiltreren. Vervolgens zullen ze dreigen om verder te gaan.

Mogelijke gevolgen voor uw bedrijf of organisatie

Meer dan alleen opscheppen over hun vaardigheden, is het voor criminelen een manier om een voet tussen de deur te krijgen in uw netwerk, zodat ze meer geavanceerde aanvallen kunnen 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. Ze verwerken gevoelige gegevens en hackers zien ze als een onbewaakte achterdeur naar uw organisatie.

Met een beveiligde printfunctie zal niemand toegang kunnen krijgen tot uw apparaten. Zorg ervoor dat uw firmware up-to-date is en dat al uw printers beveiligd zijn.

Tips om uw bedrijf en medewerkers te beschermen

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

Van het installeren van antivirussoftware tot het beveiligen van de Wi-Fi binnen het bedrijf - het handhaven van de veiligheid van bedrijfsgegevens is van het grootste belang.

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 phishingmails, gestolen identiteiten en zwakke plekken in de beveiliging van systemen om binnen te komen.

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

Mogelijke gevolgen voor uw 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, is genoeg om aan te tonen dat de beveiliging niet goed genoeg was***.

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 waardoor ze kunnen binnendringen.

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 uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het 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, wanneer data wordt verplaatst tussen verschillende databases, applicaties en services.
- Zorg voor een volledig opgeleid team dat klaarstaat om direct te reageren op een incident zodat de impact beperkt kan worden.
- Implementeer krachtige theoretische en praktijk trainingen m.bt. beveiliging van gegevens.
- Elke dag zijn er nieuwe meldingen van datalekken bij grote bedrijven en vaak leiden ze tot hoge boetes of zelfs vervolging.

* The Guardian, januari 2023

** IBM, januari 2023

Het kan verleidelijk zijn om door te klikken op onbekende gescande documenten, maar pas op voor misleiding en weersta uw 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. Maar pas op, want dit is een phishingmail.

Waarom trappen mensen erin

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

Mogelijke gevolgen voor uw bedrijf of organisatie

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

Tips om uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het bedrijf op de hoogte van de gevaren.
- Wees op uw hoede voor bijlagen en links in onverwachte e-mails.
- Download alleen bestanden van betrouwbare bronnen.
- Pas op als er urgentie wordt gevraagd.

Door AI-tools, zoals ChatGPT, herken je phishing-e-mails niet zo gemakkelijk. 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. Maar tegenwoordig is dat anders. Criminelen gebruiken AI tools, zoals ChatGPT en chatbots, om phishingberichten 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 aannemen als zijnde echt en persoonlijke info en accountgegevens delen.

Mogelijke gevolgen voor uw bedrijf of organisatie

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

Tips om uw bedrijf en medewerkers te beschermen

- Houd iedereen binnen het 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 uw bedrijf tegen de 10 ‘Most Wanted’ oplichtingsmethodes.

Nu u deze informatie heeft gelezen, kunt u het gedrag, de methodes en trucs van cybercriminelen herkennen.

Maar liefst 60% van de kleine bedrijven die getroffen worden door een cyberaanval gaan na 6 maanden failliet. Doe uw voordeel met de kennis en waarschuwingen uit dit document en deel het met collega’s.

Met Brother ‘At your side’ bent u oplichters een stap voor en kunt u uw bedrijf of organisatie behoeden voor een potentiële cyberaanval met catastrofale gevolgen.

brother
at your side