7 tips om een phishing mail te herkennen

Whitepaper

PVO Midden-Nederland

Inleiding

In de moderne wereld zijn we steeds afhankelijker geworden van onze digitale systemen. Steeds minder mensen maken gebruik van fysieke agenda's en we mailen de hele dag door.

Maar wat als de computer uitvalt of alle gegevens niet meer vindbaar of versleuteld zijn? Volgens recente statistieken wordt 1 op de 3 ondernemers slachtoffer van cybercriminaliteit, waarbij in 90% van de gevallen cybercriminelen binnenkomen via e-mail.

PVO Midden-Nederland

Phishing

Besmette e-mails noemen we ook wel phishingmails. Cybercriminelen noemen hun slachtoffers vaak 'visjes' en proberen hen te verleiden met verleidelijke smoezen in de hoop gegevens te stelen.

Maar wat er is nou zo erg als ze jouw gegevens versleutelen?

Criminelen zijn altijd op zoek naar informatie. Betaalgegevens, persoonsgegevens, inloggegevens of bijvoorbeeld informatie over de rollen en taken van een bedrijf. Deze informatie kunnen ze gebruiken om verder in het systeem te komen en uiteindelijk gijzelsoftware te installeren. Waardoor niemand meer bij de gegevens kan. Of ze gebruiken het om een bedrijf af te persen.

Phishingmails herkennen

Deze whitepaper is opgesteld om ondernemers en medewerkers informatie te geven over het herkennen van phishingmails.

Het goed kunnen afwegen of je een e-mail veilig kunt openen is makkelijker gezegd dan gedaan. Het is vaak erg moeilijk om valse e-mails te herkennen, vooral als het gaat om gerichte aanvallen. In deze whitepaper vind je 7 tips om mogelijk valse e-mails te herkennen.

“Amateurs hack systems, professionals hack people”

Bij cybercriminaliteit is de mens de zwakste schakel. 80% van de cyberincidenten wordt veroorzaakt door een menselijke fout of menselijk handelen.

7 tips om phishing te herkennen

1. Check de afzender
2. Let op de aanhef
3. Taalgebruik en vormgeving
4. Vragen naar persoonsgegevens
5. Spoed is niet goed
6. Links of linkverkorters
7. Bijlagen

1

Check de afzender

- Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres vaag of een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie.

- Kijk goed naar de domeinnaam waarvan je de e-mail hebt ontvangen. De domeinnaam is te herkennen aan alles wat achter het @-teken in het e-mailadres staat.

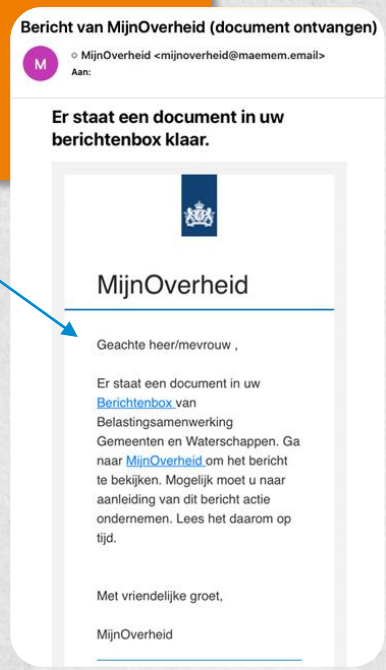
- Controleer of het e-mailadres ook echt overeenkomt met het websiteadres. Een veel gebruikte manier om valse e-mails te verspreiden is namelijk het vervangen van bepaalde letters uit de domeinnaam door cijfers.

- Het verschil tussen een legitiem en vals e-mailadres kan soms moeilijk te onderscheiden zijn. In het volgende voorbeeld is 1 (cijfer) vervangen door een I (letter). Vergelijk mail@31008mailers.nl en mail@3I008mailers.nl.

2

Let op de aanhef

Bedrijven en instanties waar je klant bent of zaken mee doet gebruiken in ieder geval je achternaam in een e-mail, of weten of je een man of een vrouw bent. Word je met heel algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op.



3

Taalgebruik en vormgeving

De huidige generatie nepmails staan allang niet meer bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Lees en bekijk de e-mail goed om te zien of je toch geen onregelmatigheden tegenkomt. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

4

Vragen naar persoonsgegevens

In veel nepmails staat het verzoek om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Je moet dan op een link klikken om dit te doen. Doe dit nooit zomaar. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit op deze manier naar persoonsgegevens.

Bel het bedrijf/instantie eerst op om te controleren of ze de e-mail hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

5

Spoed is niet goed

Veel valse mailtjes proberen je onder druk te zetten door gebruik te maken van laatste waarschuwingen of spoedmeldingen. Een voorbeeld van een dergelijk bericht is bijvoorbeeld "Uw hostingpakket verloopt, als u vandaag bedrag x niet overmaakt zal uw website worden geblokkeerd". Ga hier niet via de e-mail op in maar neem bij twijfel telefonisch contact op met de hostingpartij.

“Ik dacht echt dat het de inlogpagina van Outlook was. Ik ben er zelf keihard ingetrapt.”

- CEO na interne phishingsimulatie

PVO Midden-Nederland

6

Links en linkverkorters

Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of leiden je naar een valse website. Klik dus nooit zomaar op de links in een e-mail die je niet vertrouwt. Controleer het adres van de link door, zonder erop te klikken, de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt.

Link-verkorters: Vaak worden lange links verkort met diensten als bijvoorbeeld T.co, bit.ly en Goo.gl. Erg handig, maar voor jou als ontvanger erg belangrijk om hier waakzaam op te zijn aangezien het lastig is om te achterhalen waar je nu precies op klikt en naar toe wordt geleid.

7

Bijlagen

Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt.

Een zip of rar-bestand is altijd verdacht, omdat bijvoorbeeld facturen en aanmaningen nooit op deze manier worden verstuurd. Verwacht je toch een bestand? Neem dan contact op met de afzender om te vragen wat en hoe ze iets precies verstuurd hebben.

Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf (bijvoorbeeld via de website) op.

Meer informatie?

Voor meer informatie over cybercriminaliteit en veilig digitaal ondernemen verwijzen we je door naar het Digital Trust Center. Op deze site is onder andere de phishingbingo te vinden, een test naar jouw phishingkennis maar ook meer informatie over andere vormen van cybercriminaliteit.

Digital Trust Center (www.digitaltrustcenter.nl)

Wil je meer weten over cybercriminaliteit en wat je hieraan kan doen?

Schroom niet om contact op te nemen met een van onze adviseurs. Kijk voor de contactgegevens per adviseur op:

www.pvo-middennederland.nl of stuur een mail naar info@pvo-mn.nl

Samen Veilig Ondernemen

Daar maken we ons sterk voor.

PVO Midden-Nederland

Kroonstraat 25
3503 RH Utrecht
pvo-middennederland.nl

info@pvo-mn.nl

PVO Midden-Nederland

PVO Midden-Nederland zet zich in voor veilig ondernemen in de regio. We werken samen met overheid en bedrijfsleven om ondernemers bewust te maken van en te beschermen tegen criminaliteit, zowel fysiek als online. Ons doel is om de veiligheid in en rondom bedrijven te verbeteren en ondernemers weerbaarder te maken, zodat ze met vertrouwen kunnen blijven groeien in Midden-Nederland.