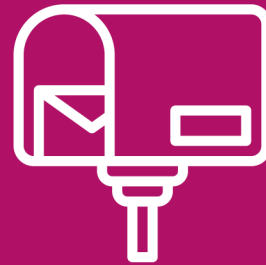


# PHISHING CHECKLIST

## 1. AFZENDER

Vergeet niet om regelmatig te controleren of de afzender, het e-mailadres en de inhoud van een e-mail daadwerkelijk overeenkomen met de verwachte communicatie. Maak medewerkers bewust van de risico's van phishing en het belang van het kritisch beoordelen van elke ontvangen e-mail.



## 2. URGENTIE

In het MKB, waar de werklust soms hoog is en tijd een kostbaar goed, is het van belang om extra waakzaam te zijn bij e-mails die dringende actie vereisen. Herinner personeel aan het belang van het nemen van de nodige tijd om verdachte e-mails zorgvuldig te beoordelen voordat er actie wordt ondernomen.



## 3. LINKS EN BIJLAGEN

In de zakelijke omgeving is het belangrijk om extra voorzichtig te zijn met links en bijlagen in e-mails, gezien de gevoeligheid van bedrijfsgegevens. Tip: zweef (niet klikken!) met je cursor over een link of bijlage om de bestemming te zien.



## 4. TAALGEBRUIK

Mede door A.I. is dit een steeds minder relevante rode vlag, maar phishing e-mails bevatten soms nog steeds spelfouten, onlogische zinnen of vreemde vertalingen.



## 5. VERIFICATIE

Als je twijfelt over de authenticiteit van een e-mail, neem dan contact op met de vermeende afzender via een ander communicatiekanaal, zoals telefoon of officiële website.

