- **Aad svp niet direct benaderen. Dit moet lopen via Michiel (voor export) en via mij en bij mijn afwezigheid via Ruud.**

- **Wanneer er mensen verplaatst moeten worden dan svp deze stappen volgen:**
  - ❖ toestemming vragen aan de leidinggevende
  - ❖ leidinggevende vraagt toestemming aan GB van Pelt

  Bij akkoord gaat Robbert op de achtergrond de verhuizing in werking stellen ! Robbert zal dan voor de verdere afhandeling zorgen. Dus **NIET** zelf schermen en computers verplaatsen. De reden hierachter is voornamelijk verzekeringstechnisch. Robbert heeft inmiddels ook een start gemaakt met de nummering van de werkplekken. Op de monitor en pc komt een sticker waarop dit nummer komt te staan. Vanzelfsprekend mogen deze stickers NIET verwijderd worden. In plaats van dat je je GBP nummer opgeeft aan hem kan je dan volstaan met het werkpleknummer waar je op dat moment zit zodat hij je op afstand kan helpen ! Cleve Antwerpen volgt tzt ook.

- **Wachtwoorden mogen niet gedeeld worden; je bent hier zelf verantwoordelijk voor**
- **Om de drie maanden moet het wachtwoord aangepast worden; het wachtwoord mag niet eerder gebruikt zijn**
- **Nogmaals het verzoek om goed te kijken wie de afzender is van bepaalde mails.** Ken je de afzender niet dan is het de vraag uit welk land de email komt. Is het een land waar we geen of weinig zaken mee doen (bijv Rusland) dan zeker GEEN BIJLAGE(N) OPENEN en IT waarschuwen !

  In de mails worden bijvoorbeeld (te hoge) factuurbedragen, boetes, incasso's of mislukte afleverpogingen genoemd, waarvan de details in de bijlage of achter een link zouden staan. De bijlagen of links bevatten onder andere vermomde uitvoerbare bestanden (factuur.pdf.exe), javascript(.js)-bestanden of Word-bestanden met kwaadaardige macro's. Soms zijn ze verpakt in een zip-bestand. Bedrijfsnamen die hierbij als zogenaamde afzender worden misbruikt zijn onder meer KPN, Ziggo, Intrum Justitia en transportbedrijven. Hoe kan je dit dan herkennen want dit zijn wel afzenders die iedereen kent en waarvan iedereen weleens een mail krijgt.

❖ **Herken foute links**
Zo zie je waar een link echt naar leidt: zweef met het muispijltje boven een link. Linksonder op het scherm of vlak boven de muiscursor verschijnt het webadres waarnaar de link verwijst (verwijst het dan niet naar het betreffende bedrijf dan NIET KLIKKEN)

❖ **Kwaadaardige bijlagen** De volgende bestandstypen zijn extra verdacht als ze in een mailbijlage staan:
.zip: een zip-bestand wordt gebruikt om de inhoud (vaak een .exe-bestand) te maskeren.
.exe: een programmaatje, nagenoeg altijd foute boel.
.js .lnk .wsf .scr .jar: Nooit openen! Ze bevatten scripts die malware downloaden.
.**doc**: een Word-document. Standaard niet gevaarlijk, maar als het bestand na openen vraagt om het inschakelen van macro's, doe dat dan niet.
Maar ook met pdf bestanden moet je uitkijken.

Het is lastig te bepalen, soms lijkt een emailadres okee maar dat is dan niet zo. Onze mailadressen eindigen op @cleve.nl / @cleve.be / @orionco.nl / @orionco.be / @gatewayexpresslines.nl en @gatewayexpresslines.be.
Mocht je een mail krijgen van bijv invoice@cleve-rotterdam.nl dan wijst dit ook op foute boel…. Dit soort berichten kan je dus ook van je klanten krijgen, let hier dus ook extra op zeker icm bijlagen of hyperlinks in de mail !