

PD Recherche

Het is van vitaal belang dat u zich bewust bent van het bestaan van frauduleuze brieven, e-mails en phishing en dat u die herkent, om uzelf te beschermen tegen diefstal en gelijkaardige misdaden. Dit zijn de meest voorkomende aanwijzingen dat een e-mail frauduleus kan zijn:

Gebrekkige opmaak: Een e-mail met vervormde of onregelmatige logo's

Slechte grammatica: Grammaticafouten en een overdreven gebruik van uitroeptekens

Spelfouten: Verkeerd gespelde woorden of links naar gewijzigde websites (bijvoorbeeld, wijzigingen of variaties van het echte websiteadres www.ups.com, zoals www.unitedparcelservices.com.)

Dringende oproepen: Alarmerende berichten die oproepen tot onmiddellijke actie, zoals "uw account wordt binnen 24 uur afgesloten" of "neem onmiddellijk contact op met ons om uw pakket of prijs op te eisen".

Onverwachte vragen: Vragen die proberen geld, financiële informatie (vb. bankrekening of creditcardnummers) of persoonlijke informatie te verkrijgen in ruil voor de levering van een pakket of een ander artikel

Beperkte communicatiemogelijkheden: Een e-mail die geen alternatieve methode voorstelt om de gevraagde informatie te verstrekken (zoals telefoon, post of fysieke vestigingen)

Misleidende link: Een link verwerkt in een email die uw browser lijkt te leiden naar een gekende website, maar u eigenlijk naar een andere, mogelijk onveilige of frauduleuze site brengt. U kunt dit herkennen door de cursor over de link te laten zweven. Zo verschijnt de echte bestemming van de link rechts onder de statusbalk. Indien de adressen niet overeenstemmen is dit verdacht. Let ook op bij links met daarin nummers in plaats van letters, afkortingen of kleine typfouten in de link