

# Veilig en privé e-mailen, kan dat wel?



E-mail is voor veel mensen niet meer weg te denken uit het dagelijks leven. Maar hoe veilig is e-mail eigenlijk? En wat gebeurt er met je berichten als je op "verzenden" drukt? En wat gebeurt er als je ze ontvangt?

Dit document geeft een helder overzicht voor iedereen die meer wil weten over veilig en privé e-mailen. Je hebt geen technische vakkennis nodig! Het begint met een korte geschiedenis van e-mail, gevolgd door praktische tips over veilig inloggen en spamfilters. Daarna komt de privacywetgeving aan bod en wat end-to-end encryptie precies inhoudt — en wanneer het wel en niet werkt.

## Inhoudsopgave

Veilig en privé e-mailen, kan dat wel?.....	1
E-mail - door de jaren heen.....	2
Veiliger e-mailen.....	3
Inloggen met 2-traps verificatie.....	3
Spam- en phishing filters.....	4
Herstel van je account.....	5
E-mail privacy wetgeving.....	6
Het e-mail briefgeheim?.....	6
Europese privacywet: General Data Protection Regulation (GDPR).....	7
End-to-end e-mail encryptie (E2EE).....	8
Metadata is slechts gedeeltelijk versleuteld.....	9
Blijft je e-mail veilig als je een e-mail stuurt naar iemand buiten je eigen netwerk?.....	9
Wachtwoord-beveiligde optie om volledig privé e-mail te versturen.....	10
E-mail advies?.....	10

## E-mail - door de jaren heen



E-mail begon in de jaren '60. Mensen konden toen alleen berichten sturen als ze op dezelfde grote computer zaten. In 1971 bedacht Ray Tomlinson het @-teken. Dit is nog steeds belangrijk voor elk e-mailadres. In die tijd waren er nog geen e-mailaanbieders zoals nu. E-mail werkte alleen op universiteiten, bij het leger en bij grote bedrijven.

In de jaren '80 en '90 kwamen de eerste e-mailprogramma's. Deze programma's noem je **e-mailclients**. Je installeerde ze op je computer.

Om e-mail te kunnen gebruiken, had je een account nodig bij een e-mailaanbieder. In Nederland waren dit bedrijven zoals KPN of Tiscali. Later kwamen daar ook de kabelbedrijven bij, zoals tegenwoordig Ziggo.

De e-mailaanbieder stuurde de e-mails naar de e-mailclient op je computer. Dit is alsof de postbode de post bij jou thuis brengt. Daarna bewaart het programma de e-mails op je computer. Zo kon je je e-mails lezen in het programma.

In 1996 begon Hotmail. Dit was de eerste belangrijke webmail-dienst. Later kwamen Yahoo! Mail en Gmail (in 2004).

Met **webmail** hoef je niets op je computer te installeren. Je gebruikt alleen een internet-browser. Je kunt inloggen op elke computer of telefoon. Je gaat naar de website van je e-mail-aanbieder, bijvoorbeeld:

<https://mail.yahoo.com/>

<https://gmail.com>

Met webmail lees je e-mails op de website van de aanbieder. Dit is alsof je je post leest en bewaart op het postkantoor.

Vandaag de dag zijn er grote e-mail aanbieders zoals Google (Gmail), Microsoft (Outlook.com) en Apple ( iCloud Mail). Er zijn ook nieuwe aanbieders zoals Proton Mail en Tuta en Startmail. Die richten zich sterk op je privacy.

Veel mensen hebben accounts bij verschillende aanbieders. Soms gebruiken mensen een e-mail-programma op hun telefoon of computer. Soms gebruiken ze webmail in de browser. Beide methodes werken goed.

Met een e-mail account heb je toegang tot een mailserver bij je e-mailaanbieder. De mailserver is de software die achter de schermen al het zware werk doet. Het is verantwoordelijk voor het ontvangen, versturen en opslaan van e-mails. Zonder mailserver zou je e-mail nergens heen gaan. De mailserver is als het ware het sorteercentrum van de post. De mailserver werkt samen met webmail en de e-mailclient.

Hieronder staan de belangrijkste termen:

- E-mail aanbieder: Het bedrijf dat je e-maildienst geeft. Heet ook wel provider.
- Account: Je persoonlijke toegang tot e-mail bij een e-mailaanbieder.
- E-mailadres: Je unieke adres voor e-mail (bijv. jan.jansen@gmail.com).
- E-mail client: Een programma op je computer of telefoon. Heet ook wel e-mail programma of e-mail app.
- Webmail: E-mail in je browser, zonder extra programma op je computer of smartphone
- Mailserver: Is verantwoordelijk voor het ontvangen, versturen en opslaan van e-mails.

## Veiliger e-mailen

De e-mail aanbieders zorgen ervoor dat je e-mail veilig verstuurd en ontvangen wordt. Transport van de mailserver van de ene aanbieder naar de andere is steeds versleuteld. Het transport is daarmee goed beveiligd. Ook over de verbinding van je eigen apparaat naar de e-mail aanbieder.

## Inloggen met 2-traps verificatie

De meeste gebruikers loggen in met hun e-mail adres en een wachtwoord. Dat heet 1-traps verificatie. Je krijgt toegang tot een systeem met slechts één verificatie stap, meestal alleen een wachtwoord. Een kwaadwillende heeft toegang tot je e-mail als hij je wachtwoord kent of het raadt.

Bij 2-traps verificatie doorloop je twee stappen. Dat staat ook bekend als 2FA (Twee-factor authenticatie).

Bij 2FA voeg je een extra stap toe. Je bewijst eigenlijk twee keer wie je bent.

1. Iets wat je weet: Je wachtwoord of pincode.
2. Iets wat je hebt: Je telefoon (voor een sms of app) of je vingerafdruk.

De 2FA standaard is niet voor niets de standaard bij DigiD. Dat is ook zo bij de banken.

Tweetrapsverificatie kan heel eenvoudig zijn. Bij het inloggen ontvang je één keer een sms met een code. Vul je deze code correct in, dan onthoudt de e-mailprovider dat apparaat voortaan.

Achter de schermen controleert de provider wel altijd of je inlogt met een vertrouwd apparaat. Voor jou is het daarna gewoon inloggen met je gebruikersnaam en wachtwoord. Log je in op een nieuw apparaat, dan krijg je opnieuw een sms met een code.

Bekijk de website van de consumentenbond voor een duidelijk verhaal over twee-factor authenticatie (2FA) <https://www.consumentenbond.nl/veilig-internetten/activeer-tweestaps-authenticatie>.

Ook Seniorweb heeft hierover uitleg: <https://www.seniorweb.nl/artikel/wat-is-tweestapsverificatie>

## Spam- en phishing filters



Het woord "spam" heeft een grappige herkomst. Het komt van spam, het ingeblikte vleesproduct uit Amerika. Spam (het vlees) was tijdens en na de Tweede Wereldoorlog overal. Je kon er niet omheen.

De digitale betekenis stamt uit een beroemd Monty Python-sketch uit 1970. Een stel klanten in een café probeert het te bestellen, maar in elk gerecht op het menu zit spam. Gebruikers die chats of discussies wilden verstoren riepen steeds spam. Die gewoonte werd "spammen" genoemd.

Een **spamfilter** blokkeert ongewenste berichten zoals bijvoorbeeld reclame, nieuwsbrieven en "koop dit nu"- berichten. Het is erg fijn als het spamfilter dit soort ongewenste berichten automatisch afvangt en in de spam map plaatst in plaats van in de inbox.

Een **phishing filter** dient om fraude en diefstal te voorkomen. Zoals valse websites en nep berichten die zich voordoen als een echt bedrijf.

Net als bij vissen gooit een aanvaller een "aas" uit, bijvoorbeeld een nep-e-mail of nepwebsite, en wacht tot iemand "bijt". Het slachtoffer geeft dan zelf zijn gegevens prijs, zonder dat de aanvaller hoeft in te breken.

Er zijn hele slimme filters met AI, die meer dan 95% tegenhouden. Het systeem leert dan steeds bij van de gebruikers. En aan de andere kant zijn er ook basis-filters, die veel minder afvangen. En ook nauwelijks bijleren.

Professionele e-mailbedrijven gebruiken vaak betere filters dan bijvoorbeeld Ziggo en KPN.

Als een spamfilter te weinig spam tegenhoudt, is dat vervelend. Dan komt er veel ongewenste e-mail in je inbox. Maar als een spamfilter te streng is, is dat ook niet fijn. Dan komen echte e-mails in de spammap terecht. Je kunt deze berichten dan makkelijk missen.

De meeste spamfilters filteren op zowel spam als phishing.

Het is erg lastig om uit te zoeken hoe een e-mail aanbieder spam filtert. Daarom is de AI chatbot Claude gevraagd om na te gaan wat de verschillen zijn tussen 8 e-mail aanbieders:

De conclusie is dat alle acht providers standaard beveiligingscontroles gebruiken als fundament. Het grote verschil zit in de filosofie:

- Gmail, Apple en Outlook onderzoeken ook de inhoud van je e-mail en gebruiken AI
- Privacy-gerichte diensten (Proton, Tuta) onderzoeken niet de inhoud van je e-mail. Ze kunnen technisch gezien de inhoud niet lezen. Ze onderzoeken met Machine Learning andere gegevens, zoals wie je belt. Die gegevens zijn versleuteld.
- Mailbox.org gebruikt een openbaar e-mailcontroleprogramma (SpamAssassin). Dit onderzoekt ook de inhoud van het bericht.
- KPN vertrouwt op een externe leverancier en onderzoekt ook de inhoud van het e-mail bericht.

## Herstel van je account

Wanneer je je wachtwoord vergeet, wil je natuurlijk wel weer toegang tot je e-mail of andere diensten. Daarom bieden de meeste e-mailaanbieders een herstel-methode aan.

Als je het wachtwoord vergeten bent, gebruik je normaal gesproken de "Wachtwoord vergeten"-optie bij het inloggen. Herstel is alleen mogelijk als je dit van te voren hebt voorbereid. Anders wordt het heel vervelend en ben je echt je account kwijt! Met alle opgeslagen e-mails.



Herstel gegevens vul je in bij e-mail instelling.  
Hieronder staan de meest gebruikte herstel-methoden.

### Herstel-e-mailadres

Van te voren geef je een werkend ander e-mailadres op. Je moet dat account zelf kunnen openen.

Als je je wachtwoord niet meer weet, stuurt de e-mailaanbieder een link naar het andere e-mailadres. Met die link kun je dan je wachtwoord opnieuw instellen.

### Herstel telefoonnummer (SMS of oproep)

Van te voren geef je een herstel telefoonnummer op. De e-mailaanbieder stuurt je een verificatiecode per sms of belt je met een code. Je voert die code in om je identiteit te bevestigen.

### Herstel Back-up codes

Bij het instellen van tweestaps-verificatie krijg je een lijst met eenmalige codes.

Elke code kun je één keer gebruiken om in te loggen.

De lijst met codes moet je goed bewaren. Bijvoorbeeld een papieren print-out of een foto.

## E-mail privacy wetgeving

Je kunt het versturen van een e-mail vergelijken met het sturen van een brief in een envelop. De postdienst moet de brief rechtstreeks op het goede adres afleveren. Je wilt niet dat iemand de brief stiekem leest. Je wilt ook niet dat je brief snel even doorgelezen wordt om te kijken of er mooie trefwoorden inzitten voor latere reclame.

En je wilt ook niet dat de postdienst alle enveloppen lang bewaard. Dit om te onderzoeken naar wie je allemaal brieven stuurt. En van wie je ze krijgt!

En het zou ook mooi zijn als de bewaarde brieven alleen door jezelf geopend kunnen worden.

### Het e-mail briefgeheim?

“Artikel 13 in de Nederlandse Grondwet - Brief- en Telecommunicatiegeheim” beschermt de burger tegen overheidsinmenging. E-mails worden, net als gewone brieven, beschermd door het briefgeheim.

De Telecommunicatiewet regelt in Nederland hoe artikel 13 in de praktijk werkt. Daarin staan de regels voor de diverse aanbieders.

Dat betekent:

- De overheid mag niet meekijken: Niemand van de overheid mag zomaar je e-mails lezen. Dat is verboden.
- Uitzondering: Ze mogen alleen kijken als ze een speciale toestemming van een rechter hebben (bijvoorbeeld bij een ernstig misdrijf).

Jouw e-mails zijn privé en niemand van de Nederlandse overheid mag ze zomaar openen.

In een ander land gelden de regels van dat land. In de EU zal dat in de praktijk vaak lijken op de regels in Nederland. Buiten de EU is dat vaak anders.

## Europese privacywet: General Data Protection Regulation (GDPR)

Binnen de EU hebben we een gemeenschappelijk Europese privacy wet. De GDPR is een brede privacywet die voor vrijwel iedereen en elke organisatie geldt. In Nederland heet de Nederlandse uitvoering van die privacywet AVG.

Hieronder staan een aantal e-mail aanbieders en onder welke wetgeving ze vallen. Binnen de EU valt elke e-mailaanbieder onder de GDPR.

E-mailaanbieder	Land van vestiging	Toepasselijke wetgeving
KPN, Ziggo	Nederland	AVG + Telecommunicatiewet
StartMail	Nederland	AVG + Telecommunicatiewet
Gmail, Outlook, Apple	VS	GDPR (voor EU-gebruikers) + Amerikaanse wetten
Proton	Zwitserland	GDPR + Zwitserse privacywetten
MailFence	België	GDPR + Belgische privacywetgeving
Mailbox.org	Duitsland	GDPR + Duitse privacywetgeving
Tuta	Duitsland	GDPR + Duitse privacywetten

De EU wetgeving voor privacy is veel strenger dan de Amerikaanse. Wetgeving uit de USA kan botsen met Europese regels. Ook kan je toegang tot diensten worden geblokkeerd. Een voorbeeld: de hoofdadvoaat van het Internationaal Gerechtshof verloor de toegang tot Microsoft-diensten (zoals Outlook en Teams) omdat de Amerikaanse overheid sancties oplegde.

Elk bedrijf heeft verplichte service voorwaarden en een privacy verklaring. EU-e-mailaanbieders moeten zowel hun privacy-beleid als servicevoorwaarden openbaar maken en de gebruiker laten instemmen.

In de privacy verklaring staat welke gegevens het bedrijf verzamelt en wat het ermee doet. Bijna niemand leest die verklaring omdat het meestal erg veel tekst is. Ook is de inhoud moeilijk om te begrijpen.

Gelukkig is er een website die dat voor ons doet. Op de Nederlandse pagina van ToS;DR (<https://tosdr.org/nl/>) kun je informatie daarover vinden over een aantal bedrijven. Vrijwilligers bestuderen service voorwaarden en privacy verklaring en beoordelen het bedrijf. Score A is goed en score E is slecht. Microsoft Services krijgt bijvoorbeeld een score E, Apple een C en Tuta scoort hoog met een A.

Op de website kun je goed zien naar welke punten allemaal gekeken wordt om tot een score te komen.

Het is goed dat er privacy wetten zijn en dat je het privacy beleid van een e-mailaanbieder kunt doorlezen.

**Maar....** het enige wat echt privacy geeft is een volledig versleutelde verbinding tussen afzender en ontvanger. En versleuteling van je opgeslagen e-mails. **Dat heet end-to-end e-mail encryptie (E2EE).**

De e-mail aanbieders versleutelen wel de verbinding tussen de e-mail servers. Het transport is veilig. Maar de inhoud van de e-mails zelf ligt op de server vaak leesbaar opgeslagen.

De overheid, je e-mail aanbieder en hackers kunnen in principe alles lezen! Je e-mail is alleen veilig als de inhoud versleuteld is.

## End-to-end e-mail encryptie (E2EE)

Een e-mail is net als een brief.

- De brief zelf – dit is de inhoud van de e-mail, de tekst die je leest.
- De envelop – dit bevat extra informatie die niet in de brief zelf staat, maar wel belangrijk is om de brief te kunnen bezorgen en te begrijpen. Die extra informatie noemen we **metadata**.

Hieronder zie je 4 voorbeelden van metadata van een e-mail.

Envelop-onderdeel	Wat het betekent	Voorbeeld
Afzender	Wie heeft de e-mail gestuurd.	Jan Jansen < <a href="mailto:jan.jansen@gmail.com">jan.jansen@gmail.com</a> >
Ontvanger (adres)	Aan wie de e-mail is gericht.	Piet Pietersen < <a href="mailto:piet.pietersen@gmail.com">piet.pietersen@gmail.com</a> >
Onderwerp	Waar de e-mail over gaat, in één korte zin.	“Wat zijn je vakantie plannen?”
Tijdstempel	Wanneer de e-mail is verzonden (en soms ook wanneer hij is gelezen).	07-02-2026

De end-to-end versleuteling, bewaakt de inhoud zelf. Meestal worden twee sleutels gebruikt. Elke gebruiker heeft een publieke sleutel en een privé sleutel. Alleen met beide sleutels is het bericht onleesbaar.

### Stap voor stap voorbeeld: Jan mailt naar Piet en beiden hebben een Proton account.

Stap 1 — Proton geeft Jan automatisch het open hangslot (publieke sleutel) van Piet.

Stap 2 — De e-mail wordt versleuteld met Piets publieke sleutel. Het open hangslot van de e-mail is nu op slot. Niemand — zelfs Jan niet meer — kan het openen.

Stap 3 — De e-mail reist via internet. Hackers, providers, zelfs Proton zelf zien alleen een op slot zittende e-mail. Geen letter van de inhoud is leesbaar.

Stap 4 — Piet ontvangt de e-mail en opent deze met zijn privésleutel. Alleen Piets privésleutel past op het slot. Hij opent de e-mail en kan deze lezen.

Waarom is dit zo veilig?

Het wiskundige trucje is: het hangslot dichtdoen en het hangslot openen vereist een verschillende sleutel. Je kunt van het hangslot niet afleiden hoe de privésleutel eruitziet — ook niet met de snelste computer ter wereld.

De e-mailaanbieders Tuta en Proton leveren standaard end-to-end e-mail encryptie. Bij andere veilige e-mail aanbieders moet je die versleuteling zelf handmatig instellen. Vermoedelijk gaan ze op termijn ook over naar automatische sleutels.

Gmail en Outlook hebben geen end-to-end e-mail encryptie voor gewone gebruikers. Ze hebben wel iets soortgelijks voor zakelijke klanten. KPN en Ziggo hebben geen end-to-end e-mail encryptie.

Bij o.a. Proton en Tuta worden ook je opgeslagen e-mails versleuteld. Dat geldt zowel voor e-mails van afzenders met versleuteling als e-mails van afzenders zonder versleuteling. De overheid, eventuele hackers en de e-mailaanbieder zelf kunnen de opgeslagen e-mails niet lezen. Dat kan alleen met je eigen wachtwoord.

## Metadata is slechts gedeeltelijk versleuteld

Metadata is meestal beperkt versleuteld. Dat is nodig omdat de e-mail server moet kunnen zien waar de e-mail naartoe moet. Net zoals bij de envelop. Veilige mailservers versleutelen zo veel mogelijk informatie in de metadata en bewaren het zo kort mogelijk. Andere mailservers doen dat niet en bewaren en onderzoeken de metadata. Ze willen er hun voordeel mee doen. Je kunt dat nalezen in hun privacy beleid.

## Blijft je e-mail veilig als je een e-mail stuurt naar iemand buiten je eigen netwerk?

Voor het overgrote gedeelte van het e-mailverkeer is er geen E2EE. De e-mailaanbieders kunnen dan in principe meelesen. In de privacy verklaring van de aanbieder staat of ze meelesen en wat ze met je gegevens doen.

Volledig beveiligde e-mail verkeer tussen verschillende e-mail aanbieders komt niet veel voor. De drempel is vaak te hoog. Je moet sleutels genereren en uitwisselen. Voor de gemiddelde e-mail gebruiker is dat veel te moeilijk.



Voor gebruikers binnen het Proton netwerk en binnen het Tuta netwerk wordt E2EE automatisch toegepast. Daar werkt het goed. Daar zie je dan ook het blauw/groene webmail-slot in je e-mail bericht van Proton. Dat geeft aan dat de e-mail inhoud volledig versleuteld is tussen verzender en ontvanger.

E2EE stopt zodra het e-mail bericht de grens van het netwerk overgaat. Dat geldt ook voor e-mail van een Tuta gebruiker naar een Proton gebruiker. Tuta heeft namelijk een eigen sleutelsysteem.

Proton en Tuta hebben altijd automatisch E2EE voor e-mails binnen het eigen netwerk. Bij andere providers is dat dus niet zo.

## Wachtwoord-beveiligde optie om volledig privé e-mail te versturen

Je kunt vaak wel op een speciale manier een volledig beveiligde e-mail sturen naar iemand buiten je eigen netwerk. Bijvoorbeeld als Jan een Proton account heeft en Piet een Gmail account.

Jan wil een beveiligd bericht naar Piet e-mailen. Piet krijgt dan een e-mail met daarin alleen een link. Als hij op de link klikt komt hij rechtstreeks met een beveiligde verbinding bij de e-mail server van Jan. Hij moet dan een wachtwoord invullen om de e-mail te kunnen lezen.

Het wachtwoord moet je op een andere manier doorgeven, bijvoorbeeld via Signal. Anders heeft de ontvanger nog niets aan de link!

Zakelijk kun je denken aan versturen van vertrouwelijke personeelszaken of contracten met partners. Privé kun je denken aan het binnen de familie versturen van bv. een testament of eigendomsakten. Een aantal veilige e-mail aanbieders bieden deze optie aan.

## E-mail advies?

Veilig en privé e-mailen kan dus! Maar helaas is erg veel e-mail verkeer in principe onveilig. Alleen als afzender en ontvanger onderling een E2EE verbinding hebben is het echt veilig. In de praktijk betekent het vaak dat beiden op hetzelfde netwerk moet zitten. Bijvoorbeeld het netwerk van Proton of van Tuta.

Je kunt ook WhatsApp of Signal gebruiken.

Bij WhatsApp is de berichtinhoud goed versleuteld en onderweg afluisteren kan bijna niet. Maar het is minder privé omdat WhatsApp veel metadata verzamelt. Het probeert je gedragspatronen in kaart te brengen.

Voor maximale privacy is Signal het beste alternatief. Het heeft dezelfde encryptie, maar verzamelt zo weinig mogelijk metadata. Het is een bedrijf zonder commercieel winstoogmerk met “privacy” als missie!

Het is moeilijk om onafhankelijke adviseurs te vinden voor de keuze van je veilige e-mailaanbieder. Er zijn wel websites die adviseren maar het is niet duidelijk hoe onafhankelijk hun advies is. Hieronder staan er twee.

- 1) Het hosting bedrijf Kinsta heeft onderzocht welke de 14 best beveiligde e-mailaanbidders zijn. Hun artikel begint met de vraag “Wat zijn beveiligde e-mailproviders?” Kinsta geeft voor iedere leverancier de belangrijkste kenmerken en de prijs. <https://kinsta.com/nl/blog/beveiligde-e-mailproviders/>
- 2) VPNgids.nl heeft begin 2026 op de website de 15 veiligste e-mailproviders op een rijtje gezet. Op de website <https://www.vpngids.nl/privacy/anoniem-browsen/veilige-e-mailproviders/> zijn hun functies in eenvoudige en duidelijke taal uitgelegd.



En nu mijn eigen keuzes. Google en Microsoft verdienen veel geld. Zij bieden gratis diensten aan, maar gebruiken je persoonlijke gegevens als verdienmodel. Daarom wil ik hun diensten langzaam verlaten.

Mijn plan is om Outlook en Gmail niet meer te gebruiken voor mijn persoonlijke e-mail. Ik ga overstappen naar andere, betaalde en veilige e-mailaccounts.

Vanwege de huidige politieke situatie moet het een Europese e-mailaanbieder zijn. Begin 2025 heb ik een betaald abonnement afgesloten bij [www.mailbox.org](http://www.mailbox.org). Nu staan mijn e-mail, agenda en contacten bij mailbox.org.

Halverwege 2025 ben ik gestart met een Proton-account. Dit gratis account heeft volledige veiligheidsfuncties met E2EE. Sinds kort heb ik ook een Tuta-account. Zowel Proton als Tuta worden beschouwd als veilige en privé-gerichte diensten. Bij beide diensten wordt E2EE automatisch ingeschakeld.

Ook de e-mail wereld verandert snel. Het lijkt me goed om dat te blijven volgen en te blijven aanpassen!