

# E-mail zelfverdediging tegen surveillance

Massa-surveillance is in strijd met onze fundamentele rechten en bedreigt onze vrijheid van meningsuiting!

Maar we kunnen onszelf verdedigen.



## Het probleem

Het wachtwoord dat uw e-mail beschermt is niet genoeg om uw e-mails te beschermen tegen de massa-surveillance technologie van geheime diensten.

Iedere e-mail passeert over het internet vele computersystemen op weg naar zijn bestemming. Geheime- en surveillancediensten maken hiervan gebruik om iedere dag miljoenen e-mails te lezen.

Ook als u denkt dat u niets te verbergen heeft: iedereen met wie u via onbeschermd e-mails communiceert is ook kwetsbaar.

## Versleuteling

Verover uw privacy terug door GnuPG te gebruiken! Het versleutelt uw e-mails voordat ze worden verstuurd, zodat alleen de door u gekozen ontvangers ze kunnen lezen.

GnuPG is platformonafhankelijk. Dat betekent dat het werkt met ieder e-mailadres en dat het werkt op bijna iedere computer of recente mobiele telefoon. GnuPG is vrij en gratis.

Duizenden mensen gebruiken GnuPG al, professioneel en privé. Doe met ons mee! Ieder persoon maakt onze gemeenschap sterker en bewijst dat we er klaar voor zijn om terug te vechten.

## De oplossing

Als een met GnuPG versleutelde e-mail wordt opgevangen of in verkeerde handen raakt dan is het waardeloos: zonder de juiste privé-sleutel kan het niet worden gelezen. Maar voor de bedoelde ontvanger – en alleen voor haar – opent het als een geheel normale e-mail.

Afzender en ontvanger zijn nu beide veiliger. Zelfs als enkele van uw e-mails geen privé-informatie bevatten, dan beschermt consistent gebruik van encryptie ons allemaal tegen ongerechtvaardigde massa-surveillance.

## Privé e-mailcommunicatie



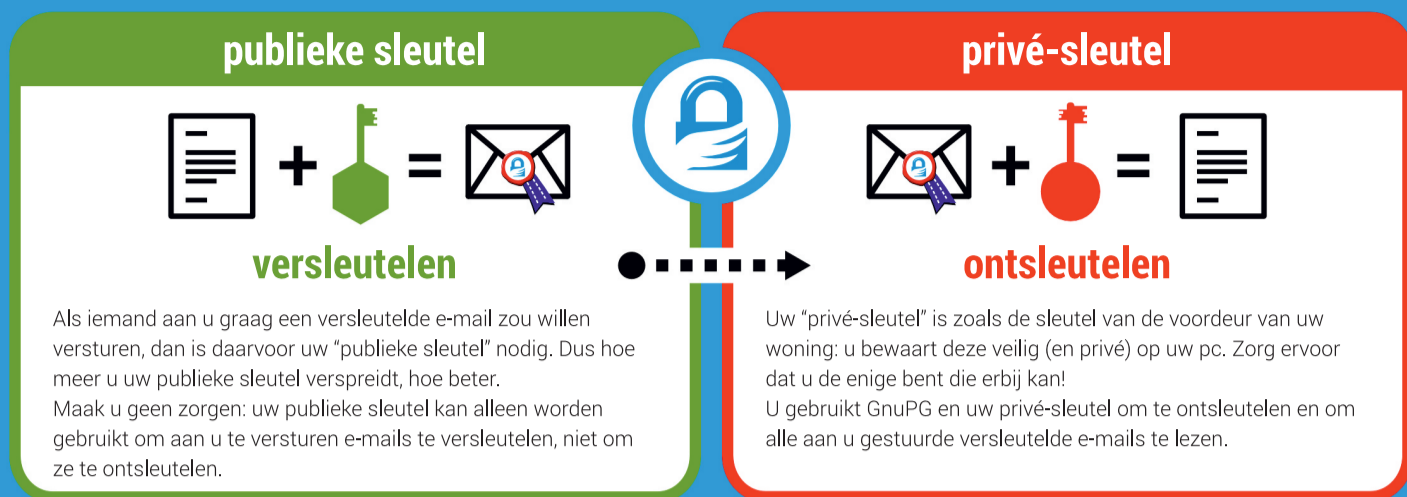
## Verover uw privacy terug! Gebruik GnuPG!



- Vrije Software
- voor alle e-mailadressen
- voor GNU/Linux, Windows, Mac, Android, ...
- geen account of registratie nodig
- gratis

# Hoe GnuPG werkt

Om GnuPG-versleuteling te gebruiken, maakt u een uniek sleutelpaar bestaande uit een publieke en een privé-sleutel. Deze sleutels worden als volgt gebruikt



## Wat maakt GnuPG veilig?

GnuPG is **Vrije Software** en gebruikt **Open Standaarden**. Dat is essentieel om er zeker van te zijn dat software ons echt beschermt tegen surveillance. Met niet-vrije software en niet-vrije bestandsformaten kunnen er dingen gebeuren buiten onze controle.

Als niemand de broncode van een programma mag zien, dan kan niemand er zeker van zijn dat het geen ongewenste spionageprogramma's (zogenoemde "backdoors") bevat. Als software niet openbaar maakt hoe het werkt dan kunnen we het niet blindelings vertrouwen.

Vrije Software is daarmee in tegenstelling en heeft als fundamentele voorwaarde dat het de broncode publiceert. Vrije Software staat iedereen toe, en steunt iedereen bij, het onafhankelijk controleren en publiekelijk herzien van de toegepaste broncode. Dankzij deze transparantie kunnen 'backdoors' worden ontdekt en verwijderd.

De meeste Vrije Software bevindt zich in handen van een gemeenschap die werkt aan veilige software voor iedereen. Als u zichzelf wil beschermen tegen surveillance dan kan u alleen Vrije Software vertrouwen.

## Wat is Vrije Software?

Vrije Software kan door iedereen voor ieder doel worden gebruikt. Daarbij hoort het vrij kopiëren, het lezen van de broncode en de mogelijkheid om het te verbeteren of aan te passen aan uw eigen behoeften (de zogenaamde "vier vrijheden").

Zelfs als u het programma "alleen wil gebruiken", dan heeft u nog steeds voordeel van deze vrijheden. Omdat zij garanderen dat Vrije Software in de handen van onze samenleving blijft en verdere ontwikkeling niet wordt bepaald door de belangen van private ondernemingen of overheden.

Meer weten over hoe Vrije Software ons kan leiden naar een Vrije Samenleving?

[fsfe.org/freesoftware](https://fsfe.org/freesoftware)

## Praktisch advies

De technologie achter GnuPG biedt eersteklas bescherming. De volgende richtlijnen zullen u helpen om er zeker van te zijn dat uw beveiligde communicatie niet wordt gecompromitteerd door andere redenen:

Om uw e-mails te ontsleutelen heeft u uw privé-sleutel en uw **wachtwoord** nodig. Dit wachtwoord zou tenminste acht karakters lang moeten zijn en cijfers moeten bevatten, zowel speciale karakters alswel hoofd- en kleine letters. Verder zou niemand met achtergrondinformatie over u uw wachtwoord moeten kunnen raden.

**Maak een back-up van uw privé-sleutel!** Als uw harde schijf kapot gaat dan hoeft u geen nieuwe te maken en bent u uw data niet kwijt.

**Versleutel zoveel als u kan!** Hiermee voorkomt u dat anderen zich realiseren wanneer en met wie u gevoelige informatie uitwisselt. Hoe vaker u uw berichten versleutelt, hoe minder verdacht versleutelde berichten zullen zijn.

Let op dat het **onderwerp onversleuteld wordt verstuurd!**

## Handleiding

U kan een eenvoudige handleiding voor e-mail zelfverdediging met GnuPG-encryptie hier vinden:

[EmailSelfDefense.FSF.org](https://EmailSelfDefense.FSF.org)

Of houdt u de zogenaamde "**Crypto-parties**" in uw regio in de gaten. Daar vindt u mensen die u graag helpen met het opzetten en gebruiken van GnuPG en ander encryptie-gereedschap.

2016-04-04



Dit vouwblad is een remix van de FSFE gebaseerd op een originele afbeelding van FSF en Journalism++ (CC BY 4.0), beschikbaar op [emailselfdefense.fsf.org](https://emailselfdefense.fsf.org)

## Over de FSFE

Dit vouwblad is gemaakt door de Free Software Foundation Europe (FSFE), een organisatie zonder winstoogmerk die is toegewijd aan het promoten van Vrije Software en het bouwen van een vrije digitale samenleving.

De toegang tot software bepaalt hoe we deel kunnen nemen aan onze samenleving. Daarom streeft de FSFE naar eerlijke toegang en deelname voor iedereen in de informatie-samenleving, waarin zij voor digitale vrijheid vecht.

Niemand zou ooit gedwongen moeten worden om software te gebruiken die de vrijheid niet biedt om haar te **gebruiken**, te **bestuderen**, te **delen** en te **verbeteren**. We hebben het recht nodig om technologie aan te passen aan onze behoeften.

Het werk van de FSFE wordt gesteund door een gemeenschap van mensen die zijn toegewijd aan deze doelen. Als u met ons mee wil doen en/of ons wil helpen onze doelen te bereiken dan zijn er verschillende manieren om bij te dragen. Het maakt niet uit wat uw achtergrond is. U kan hierover en over hoe u ons kan steunen meer te weten komen op:

[fsfe.org/contribute](https://fsfe.org/contribute)

## Word een duurzaam lid!

Donaties zijn essentieel om ons werk voort te zetten en onze onafhankelijkheid te garanderen. U kan ons werk het beste steunen door een duurzaam lid van de FSFE te worden, een "Fellow". Zo helpt u ons direct met het doorgaan met vechten voor Vrije Software waar dat nodig is.

[fsfe.org/join](https://fsfe.org/join)

U kan deze en andere vouwbladen gratis bestellen op:

[fsfe.org/promo](https://fsfe.org/promo)

Free Software Foundation Europe e.V.  
Schönhauser Allee 6/7  
10119 Berlin  
Germany  
<https://fsfe.org>

