

## Goed om te weten

Het belangrijkste om te leren is een stuk **veiligheids-mentaliteit**: een bewustzijn van het feit dat (en hoe) dingen kunnen **falen** of misbruikt kunnen worden.

Er bestaat **niet zoiets** als **100% veilig**, er zijn **geen garanties**, en er is altijd een **zwakste schakel**.

**Veiligheid is een proces**, geen aankoop.

Veiligheid gaat **niet over hulpmiddelen**; het gaat over het **begrijpen** van de gevaren die u loopt en wat u **ertegen kunt doen**. U moet erachter komen **wat** u moet (en kunt) doen om u te **beschermen** en **tegen wie**; en hoe dit **verandert** afhankelijk van wat u doet en hoe en met wie u het doet.

U zult **basiskennis** nodig hebben over hoe het **internet** werkt, wat **metadata** is en wat de **hulpmiddelen** die u gebruikt doen.

Zorg ervoor dat u de **beperkingen** van de hulpmiddelen die u gebruikt kent: u moet weten waartegen ze u *wel*, maar ook waartegen ze u **niet beschermen** en hoe ze kunnen (veroorzaakt worden te) falen.

Als u de **"cloud"** gebruikt, geeft u de controle over uw data aan iemand anders.

Wees bewust van het **vertrouwen** dat u plaatst in diegenen die de software (en hardware) die u gebruikt gemaakt hebben en die de diensten die u gebruikt aanbieden; stel uzelf de vraag of dat vertrouwen verdiend is.

### Zie ook

<https://ssd.eff.org>

<https://securityinabox.org>

<https://toolbox.bof.nl>

"Versleuteling werkt. Juist geïmplementeerde sterke cryptografie is een van de weinige dingen waarop u kunt vertrouwen."

Er is **geen cloud**  
alleen computers  
van anderen

## Vrije Software

### Wie heeft de controle over uw computer?

Vrije Software is software die iedereen vrij kan **gebruiken**, **bestuderen**, **delen** en **verbeteren**. De meeste Vrije Software is gratis, maar Vrije Software gaat over **vrijheid**, niet over geld.

Als u niet de controle hebt over een programma, heeft het de controle over u. Degene die de controle over de software heeft, heeft dus ook de controle over u.

Onvrije software lekt vaak uw data of verbergt andere kwaadaardige functies; het is niet toegestaan de werking ervan te bestuderen en er achter te komen wat het daadwerkelijk doet op uw computer of telefoon.

Het gebruik van uitsluitend Vrije Software op uw computers of andere apparaten geeft u de volledige controle en maakt het u mogelijk uw privacy te waarborgen. Zelfs als u niet over de vaardigheden beschikt om zelf gebruik te maken van alle vier vrijheden, profiteert u van de expertise van levendige gemeenschappen.

### Meer informatie

Technologie moet voor ons werken, niet tegen ons. Organisaties als de Free Software Foundation (FSF) en Free Software Foundation Europe (FSFE) zijn gewijd aan de bevordering van Vrije Software en een vrije digitale samenleving.



<https://fsf.org>

<https://fsfe.org>

## Digitale burgerrechten

Digitale burgerrechtenorganisaties zoals de Electronic Frontier Foundation (EFF), EDRi (Europa) en Bits of Freedom (Nederland) zijn gewijd aan het verdedigen van grondrechten zoals privacy en communicatievrijheid.



**BITS OF FREEDOM**  
VERDEDIGT DIGITALE BURGERRECHTEN

<https://eff.org>

<https://edri.org>

<https://bof.nl>

<https://github.com/obfusk/cryptoparty-privacycafe-menu>



# leer digitale zelfverdediging

# Privacy

# Café



# CRYPTOPARTY

<https://privacycafe.nl>

<https://cryptoparty.in>

## Voorgerechten



**Firefox:** een vrije webbrowser zonder spyware (al wilt u de advertenties in de "new tab page" misschien uitzetten)

<https://mozilla.org/firefox>



**Privacy Badger:** blokkeer tracking (cookies)

<https://eff.org/privacybadger>



**HTTPS Everywhere:** gebruik automatisch vaker HTTPS

<https://eff.org/https-everywhere>



**Startpage & DuckDuckGo:** zoekmachines met (meer) privacy

<https://startpage.com>  
<https://duckduckgo.com>

## Basisveiligheid

Installeer **updates** (automatisch); **verifieer** bron en betrouwbaarheid van software.

Gebruik een **firewall** en **virusscanner** (indien van toepassing); zorg ervoor dat u niet bijvoorbeeld buitenshuis nog het delen van bestanden aan hebt staat.

**Vergrendel** het scherm automatisch met wachtwoord of PIN.

Gebruik sterke **wachtwoorden** (zoals zinnen van minstens 4 willekeurige woorden), aparte wachtwoorden, en eventueel een wachtwoordbeheerder. Pas op met **veiligheidsvragen**: zijn de antwoorden echt geheim?!

Bescherm uw **primaire e-mailadres**: het geeft vaak toegang tot veel andere accounts.

Zorg voor **fysieke veiligheid** van apparaten.

Maak **backups** (versleuteld indien nodig). Maar pas op met (automatische) cloudbackups: u verliest mogelijk onbedoeld **controle over uw data**.

Gebruik **versleutelde verbindingen** voor web (HTTPS) en e-mail (SSL/TLS/STARTTLS).

## Hoofdgerechten



**Tor:** surf anoniem op het internet

<https://torproject.org>



**GnuPG:** versleutel uw e-mails

<https://emailselfdefense.fsf.org>  
<https://gnupg.org>



**OTR (& Pidgin):** versleutel uw chatberichten

<https://pidgin.im>  
+ <https://otr.cypherpunks.ca>



**Versleutel uw harde schijf:** zorg ervoor dat uw data veilig is bij verlies of diefstal



**Tails:** het besturingssysteem dat ernaar streeft uw privacy en anonimiteit te waarborgen (met Tor, GnuPG, OTR, etc.); start van USB-stick

<https://tails.boum.org>

## Android



**Free Your Android:** herwin de controle over uw Androidapparaat

<https://freeyourandroid.org>



**F-Droid:** App Store met Vrije Software

<https://f-droid.org>



**The Guardian Project & Open Whisper Systems:** veilige mobiele apps (inclusief Tor en versleutelde e-mail en berichten)

<https://guardianproject.info/apps>  
<https://whispersystems.org>



**Versleutel uw apparaat:** zorg ervoor dat uw data veilig is bij verlies of diefstal



**Controleer de privacyinstellingen:** zoals locatiegegevens en backups.

## Nagerechten



Gebruik een vrij besturingssysteem zoals **Debian** (of een andere GNU/Linux distributie).

<https://debian.org>



**PRISM Break:** Privacybewuste alternatieven voor onvrije software (& diensten)

<https://prism-break.org>



**Terms of Service; Didn't Read (ToS;DR):** geanalyseerde en beoordeelde algemene voorwaarden en privacybeleid

<https://tosdr.org>



**xkcd:** A webcomic of romance, sarcasm, math, and language.

<https://xkcd.com>

## iOS



**Versleutel uw apparaat:** zorg ervoor dat uw data veilig is bij verlies of diefstal



**Controleer de privacyinstellingen:** zoals locatiegegevens en backups.



**ChatSecure:** OTR-versleutelde tekstberichten

<https://chatsecure.org>

Bezoek ook eens een **hackerspace** of **Linux gebruikersgroep bij u in de buurt**; de mensen daar spreken graag met u over belangrijke zaken als privacy. U kunt ook online hulp vinden door u te abonneren op **mailinglijsten** of een bezoek te brengen aan **internetfora** over specifieke projecten of meer algemene onderwerpen.

**NB:** Zelfs bij gebruik van de hier aangeraden software kan uw privacy aangetast worden; bijvoorbeeld door onvrije besturingssystemen als Windows, OS X, iOS en standaard Android.