

# En hoe bescherm je jezelf tegen meelesen?

## Drie tips voor Veilig internetten

Een uurtje is genoeg om digitale zelfverdediging te leren, vindt Bits of Freedom. Je leert het in het Privacy Café.

Door onze redacteur  
**Carola Houtekamer**

**AMSTERDAM.** Je kunt jezelf beschermen op internet tegen meelesen en af luisteren door inlichtingendiensten. Gratis. Je moet er alleen wel „even je best“ voor doen, want supersimpel is het niet. Maar zeventig vrijwilligers van burgerrechtenbeweging Bits of Freedom willen er wel bij helpen. Door heel Nederland organise-

ren ze Privacy Cafés, vertelt Xander Bouwman vanaf de CCG in Hamburg.

In die workshops leren „mensen met veel en minder technische kennis“ hoe ze mails, chats, surfgedrag, bestanden en telefoongesprekken beter kunnen afschermen. „Met een uurtje tijd kan iedereen digitale zelfverdediging leren.“ Vergeet niet, zegt hij: „Iedereen die weleens internetbankiert en een slotje in z'n browser ziet, maakt al gebruik van encryptie.“

Afgelopen jaar heeft Bits of Freedom in tien steden vierhonderd geïnteresseerden geleerd hoe ze met allerlei encryptieprogramma's moeten omgaan. Dat zijn de programma's die deze week in *Der Spiegel* als onkraakbaar worden bestempeld. „Fijn dat het bevestigd wordt dat die veilig zijn“, zegt Bouwman.

Of ze waterdicht zijn, is niet gega-

randeerd. Maar omdat de broncode van de software vaak openbaar is, is het moeilijker voor overheidsinstanties om stiekem achterdeurtjes in te bouwen. Alvast een paar tips.

## Iedereen die weleens internetbankiert, maakt al gebruik van encryptie

### 1 Surf met een TOR-browser

Met een TOR-browser kun je anoniem op het internet surfen. Niet alleen naar obscure pagina's in het Dark Web waar drugs en wapens worden verkocht, maar ook naar gewone webpagina's. Doordat de verbinding

met het web via heel veel computers loopt, is niet te achterhalen wie een pagina opvraagt. Met een TOR-browser ontloopt je ook variabele prijzen van bijvoorbeeld vliegtickets. Je kunt je eigen browser makkelijk uitbreiden tot een TOR-browser. De software die je daarvoor nodig hebt, is gratis te downloaden via [torproject.org](http://torproject.org).

### 2 Mail met PGP

Wie geheime mails wil sturen, versleutelt zijn berichten met PGP, wat staat voor *pretty good privacy*. De encryptiemethode PGP werd al in 1991 ontwikkeld door Philip Zimmerman en werkt nog steeds. Er bestaan gratis plug-ins voor mailprogramma's die met PGP werken, zoals het open source GnuPG. PGP is niet bijzonder gebruiksvriendelijk. Zo moet je een publieke en een private sleutel genere-

ren en je vrienden moeten ook meedoen. Als de software eenmaal geïnstalleerd is, is versleutelen niet zo ingewikkeld meer.

### 3 Chat met OTR, bel met Signal

Chats beveilig je met OTR, van *off the record*. De software is te downloaden via [otr.cipherpunks.ca](http://otr.cipherpunks.ca). De apps Signal voor de iPhone en RedPhone voor Android werken met ZRTP, een encryptiemethode die net als PGP is ontwikkeld door Philip Zimmerman. Deze encryptie komt standaard in de Blackphones die KPN gaat uitbrengen. Wie hulp nodig heeft, kan aanschuiven bij een Privacy Café.

[+] **Tips en software** vind je via [toolbox.bof.nl](http://toolbox.bof.nl) van Bits of Freedom. Informatie over nieuwe workshops vind je op [privacycafe.nl](http://privacycafe.nl).