Tips om veiliger te e-mailen

Stel, je maakt gebruik van Gmail. Google, het bedrijf achter Gmail, kijkt met je mee zodra je aan het mailen bent. Gmail is weliswaar gratis, maar Google wil in ruil wel graag jouw data inzien waarmee het onder meer gericht en op persoonlijke maat adverteerders kan binnenhalen. Voor Google betekent gratis dus niet voor niets. Google heeft een betaalde versie van gmail waarbij het bedrijf zegt dat het de e-mails niet scant.

http://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify
http://digiwonk.wonderhowto.com/how-to/you-cant-stop-gmail-from-scanning-your-emails-but-you-can-limit-their-ad-targeting-0154412/

Je kunt echter ook veiliger mailen waarmee je de kans dat jouw data commercieel geëxploiteerd wordt verkleint. De mogelijkheden daartoe die in het onderstaande geboden worden zijn natuurlijk niet 100 procent waterdicht. Live communiceren zonder gebruik te maken van digitale middelen is natuurlijk altijd veiliger. Wil je veiliger mailen dan heb je verschillende opties.

1. Maak gebruik van e-mail van het bedrijf dat het internet bij je thuis verzorgt, bijvoorbeeld xs4all, Ziggo, KPN, UPC of een ander bedrijf, ook wel aangeduid als provider.

Kijk in het contract met de internetprovider of je ook een eigen e-mailadres hebt en maak er gebruik van. Van Gmail is bekend dat zij de e-mails van haar gebruikers doorzoekt. De meeste providers doen dat niet, althans dat zeggen ze in hun privacyverklaringen. Tot nu toe zijn er ook geen gevallen bekend van bedrijven, los van Google, die actief de inhoud van e-mails doorzoeken. De providers bewaren wél de verkeersgegevens, meestal voor het berekenen van de kosten, verbetering van de diensten en sommige gegevens in verband met de bewaarplicht. Die bewaarplicht is wel van tafel op dit moment.

http://tweakers.net/nieuws/101909/alle-grote-providers-zijn-gestopt-met-de-bewaarplicht.html
http://fd.nl/economie-politiek/1096172/rechter-zet-streep-door-bewaarplicht-van-providers

2. Vertrouw je het bedrijf dat jouw internetaansluiting aanbiedt onvoldoende of niet, of heb je geen eigen aansluiting, dan kan je ook kiezen voor een alternatieve organisatie die e-mail verzorgt en zich meer inzet voor de veiligheid van haar gebruikers. Dit zijn

onder andere riseup, autistici. Bij sommige van deze bedrijven/organisaties moet je betalen.

Stap 1: Bezoek de website van deze organisaties/bedrijven en vraag een e-mailadres aan.
Hier vind je een lijst,
https://help.riseup.net/en/security/resources/radical-servers

https://nadir.org represents politics by undogmatic leftists in the internet, including electronic services such as mail-providing and web-hosting.

Some random descriptions of https://aktivix.org from the aktivix description generator: Aktivix is a donation-funded herd of sweaty techies who desire to enable computer-users to disrupt capitalism in a fluffily non-hierarchical manner. Aktivix is a donation-funded co-operative of fluffy hacktivists who wish to empower collectives to challenge authority in an entirely sustainable manner. Aktivix is a consensus-based network of tired activists who wish to facilitate community-groups to communicate in a open and non-hierarchical manner.

3. Vertrouw je optie 2 ook niet, dan kun je altijd nog je e-mails 'beveiligen'/'versleutelen' in plaats van ze openlijk over het internet te versturen. Beveiligen is het versleutelen op het internet, weer wat veiliger.

Stap 1: Je hebt voor versleuteling twee programma's nodig. Op de eerste plaats het e-mailprogramma Mozilla Thunderbird. Hiermee download je je e-mails op je eigen computer. Je bent zelf verantwoordelijk voor een backup. Download dit programma en installeer het op je computer, laptop, tablet.

https://support.mozilla.org/en-US/kb/installing-thunderbird-windows

Ten tweede maak je gebruik van het versleutelprogramma GPG4Win voor het verpakken van je e-mails. Download dit programma en installeer het op je computer, laptop, tablet. Hier iets meer over GPG en verpakken/versleutelen van mails.

http://gpg4win.org/download.html
http://gpg4win.de/handbuecher/novices_5.html
http://www.reddit.com/r/DarkNetMarkets/comments/1qdzl8/guide_pgp_4_n00bz/

Stap 2: Nu moet je de twee programma’s aan elkaar koppelen, even lastig maar is zo gebeurd.
Stap 3: Maak twee sleutels. Een 'publieke' sleutel voor anderen waarmee ze een e-mail gericht aan jou kunnen verpakken en een 'private' sleutel die je met niemand deelt. Maak eerst de publieke sleutel en dan de private sleutel.

https://www.bestvpn.com/blog/7063/secure-your-email-with-gpg4win-part-1-introduction-and-installation/
https://www.bestvpn.com/blog/7117/secure-your-email-with-gpg4win-part-2-use-gpg4win-with-mozilla-thunderbird/