Security poster

Stack - veilige online opslag

https://www.transip.nl/stack/

Met stack van TransIp heb je de beschikking over maar liefst 1000 GB aan veilige opslagcapaciteit. Al je bestanden worden opgeslagen in Nederland en beveiligd met een 256-bit AES sleutel.

Geen analyse van je bestanden, geen spiekende ogen naar je foto's, jij bepaalt met wie je jouw data deelt.

Met STACK synchroniseer je automatisch al je bestanden naar al je apparaten. Zo heb je altijd toegang tot de meest recente versie op je telefoon, tablet of desktop en is vergelijkbaar met DropBox of Google Drive.

Stack werkt op basis van invites. Met de URL aan de linkerzijde (onder het logo) kun je voor jezelf een invite aanvragen. Hou er wel rekening mee dat het enige tijd kan duren voordat je invite wordt geaccepteerd.

ProtonMail - veilig emailen

https://protonmail.com/

Als je veilig wilt e-mailen, is Pretty Good Privacy (PGP) een goede optie. PGP wordt gebruikt door mensen als Edward Snowden en Glenn Greenwald en maakt gebruik van krachtige end-to-end-encryptie om een bericht te versleutelen. Alleen de ontvanger heeft de sleutel om het bericht te openen. Maar hoe je het wendt of keert: PGP blijft een verdraaid lastige technologie om in je dagelijks leven efficiënt te gebruiken. Dat vinden ook de oprichters van ProtonMail, een e-maildienst à la Gmail die standaard end-to-end-encryptie biedt, ook. ProtonMail is gratis te gebruiken en versleuteld berichten standaard tussen ProtonMail-gebruikers.

Wil je een versleuteld bericht veilig naar een ander persoon sturen, zoals een Gmail-gebruiker? Dan kun je jouw e-mail beveiligen met een wachtwoord dat je via een ander veilig kanaal aan de ontvanger geeft. Daarnaast wordt je gehele inbox versleuteld waardoor zelfs ProtonMail geen toegang heeft tot jouw e-mails.

Aanmelden is gratis, maar het kan enige tijd duren voor je gratis account wordt aangemaakt. Reken op weken!

VPN - veilig surfen op het (WiFi) internet

https://www.privatetunnel.com/home/

VPN One Click is een van de vele aanbieders van VPN, een continue beveiliging (versleuteling) van je internetverbinding. Je surft met een VPN (Virtual Private Network) als het ware via een beveiligde 'tunnel' over internet. Wel loopt al het internetverkeer dan via een server van de VPN-aanbieder.

Het bedrijf belooft privacy ('wij houden geen logbestanden bij') en de dienst is voor de meeste platforms gratis.

De VPN-dienst installeer je met gratis software, of met een app. Heb je geen VPN meer nodig op je apparaat (verlaat je het publieke wifinetwerk), zet de VPN dan weer uit, want een VPN vertraagt meestal wel je verbinding.

Krachtiger, maar niet gratis zijn OpenVPN en HotSpot Shield Elite (beide circa $30,- per jaar).
Open VPN is tot 2GB nog gratis te gebruiken. Daarna moet je upgraden.

Signal - veilig chatten

https://whispersystems.org/

Een stap die we allemaal zonder te veel moeite kunnen nemen, is het installeren van Signal. De app is beschikbaar voor Android en iOS en laat gebruikers veilig met elkaar communiceren. Dat kan via chatberichten, maar ook middels VoIP-gesprekken (bellen via een internetverbinding).

Signal maakt bij beide gebruik van end-to-end-encryptie, waarbij de inhoud van een bericht zodanig wordt versleuteld dat alleen de ontvanger het kan openen. De technologie achter Signal is ook geïntegreerd in Messenger, waardoor de chat-app van Facebook opvallend genoeg als relatief veilig wordt gezien.

Tails- veilig OS

https://tails.boum.org/

Heb je nog ergens een oude USB-stick slingeren? Steek hem in je computer en installeer het besturingssyteem Tails, dat door onder andere Snowden wordt gebruikt. Tails is een besturingssysteem dat specifiek is gebouwd om anonimiteit te bieden en veilig te zijn. Je steekt het apparaatje in een willekeurige computer, start hem op vanaf de usb-stick en komt in een speciaal beveiligde Linux-omgeving die geen sporen achter laat.

Tails beschikt standaard over de Tor-browser, een e-mailprogramma met ondersteuning voor PGP en een chatprogramma om veilig te communiceren. Je gaat Tails niet snel dagelijks gebruiken, maar het is wel een fijn idee dat je op elke computer een veilige omgeving kunt creëren.

Tor - veilig browsen

https://www.torproject.org/

Tor is één van de weinige technologieën die heeft bewezen enorm lastig te kraken te zijn. Het netwerk van Tor zorgt ervoor dat jouw verstuurde en ontvangen data via verschillende computers wordt gestuurd, waardoor je internetgedrag wordt geanonimiseerd.

Tor wordt regelmatig door dissidenten gebruikt om anoniem kritiek te uiten op totalitaire regimes, maar ook door criminelen om bijvoorbeeld drugs en wapens te verhandelen. Dat is het nadeel wanneer software je zodanig goed anonimiseert. Je hoeft de Tor-browser niet constant te gebruiken, maar als je ooit een keer écht anoniem wilt surfen: gebruik dan Tor.

Gebruik maken van Tor kan ook echter ook verdacht zijn...