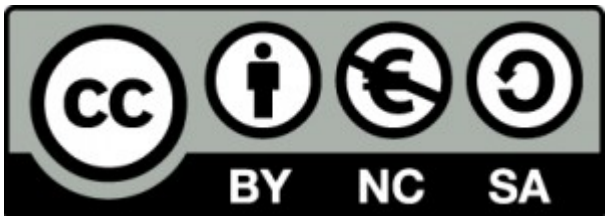
Appunti Privacy

Da Frank |Dic 26, 2023 | Guide

PROGRAMMI/APPLICAZIONI CHE TUTELANO LA PRIVACY



TELEGRAM

Quando si parla di applicazioni di messaggistica Telegram è una di quelle che più consigliamo. Nonostante sia abbastanza lontana dalla perfezione (la sua applicazione è open source significa che il codice sorgente è accessibile a tutti e chiunque può vedere cosa c'è dentro. Ma è obbligatorio usare i server di Telegram) è ad oggi un buon compromesso grazie anche al suo incredibile ecosistema fatto da bot, canali e gruppi giganteschi. Una delle caratteristiche più interessanti di Telegram, infatti, è che non è affatto obbligatorio utilizzare la loro applicazione ufficiale per chattare con gli altri utenti. Telegram è infatti open source e chiunque può creare un'applicazione che si collega ai loro server per modificare o migliorare alcune caratteristiche d'utilizzo.

CHAT - APPLICAZIONI DI MESSAGGISTICA

Signal

Telegram

Session Private Messenger

Secure Messanger

SimpleX Chat

BRIAR

SIGNAL

Su Signal si trovano più o meno tutte le caratteristiche utilizzate dalla maggior parte delle persone come le chat singole, i gruppi, le videochiamate, gli sticker le GIF animate. Così come WhatsApp anche Signal utilizza la crittografia end-to-end. Non solo, non tutti sanno infatti che in realtà utilizzano anche lo stesso protocollo di crittografia, ovvero il Signal Protocol (adottato nel 2014).In oltre Signal è una applicazione open source e anche il codice lato server lo è.
Questo però non significa che le due applicazioni siano identiche, per esempio mentre Signal non mantiene, e siamo sicuri sia così, alcun metadato sui propri server, WhatsApp invece sembra farci un po’ quel che gli pare

THREEMA

Threema, l'app per avere la massima sicurezza nelle tue chat

Threema è un’app di messaggistica istantanea che si differenzia delle altre in quanto permette di comunicare via chat, chiamate e videochiamate in maniera completamente anonima e protetta grazie ad efficaci algoritmi crittografici.Threema (nata nel 2012 in Svizzera) è considerata una delle applicazioni di messaggistica istantanea più sicure disponibili al momento. L’app è dotata di numerose funzionalità che ne rendono semplice l’utilizzo, ma anche di alcune misure di sicurezza che consentono di proteggere le chat

BRIAR

Cos’è Briar? L’applicazione consigliata da Assange

Su Briar si può chattare con una singola persona oppure creare dei gruppi privati. I messaggi sono crittografati end-to-end e non esiste un server centrale, i messaggi sono scambiati infatti peer-to-peer. questo significa che è difficile (non impossibile) da fermare, anche se siete letteralmente sotto le bombe. Briar è inoltre, come potete immaginare, è open source significa che il codice sorgente è accessibile a tutti e chiunque può vedere cosa c’è dentro. Briar scambia i propri messaggi utilizzando la rete Tor. In assenza di internet invece i messaggi vengono mandati e sincronizzati tramite Bluetooth o Wi-Fi.

SESSION

Session non vi chiederà nulla di nulla, potrete registrarvi anonimamente e vi verrà dato un ID generico e casuale. Potrete contattare le altre persone solo inserendo il loro ID. Le chat, inoltre, sono crittografate end-to-end.

Possibilità di aprire gruppi fino a 100 utenti.

SIMPLEX CHAT

Il primo messenger senza ID utente

Le altre app hanno gli ID utente: Signal, Matrix, Session, Briar, Jami, Cwtch,ecc. SimpleX invece no, neanche dei numeri casuali.Ciò aumenta radicalmente la tua privacy. A differenza di altre piattaforme di messaggistica, SimpleX non ha alcun identificatore assegnato agli utenti. Non si basa su numeri di telefono, indirizzi basati su domini (come email o XMPP), nomi utente, chiavi pubbliche o persino numeri casuali per identificare i suoi utenti — non sappiamo quante persone usano i server SimpleX.

wire

Wire è un’ app di messaggistica istantanea che, oltre a un’elevata sicurezza delle chat, offre anche un’interfaccia grafica curata e un’ottima qualità delle chiamate, oltre ad un’attenta gestione della privacy per ogni client registrato sulla piattaforma. Nella versione base, Wire è gratuita e disponibile anche in versione desktop (per Windows, macOS e Linux). Fornisce, inoltre, le estensioni per i principali browser: Google Chrome, Mozilla Firefox, Opera o Microsoft Edge.Un account permette l’uso simultaneo su un massimo di otto dispositivi, collegati allo stesso account (funzione disponibile solo nelle versioni Pro e Ent). I messaggi sono criptati per ogni dispositivo.

TOX

Tox è un client di messaggistica crittografato, Gratuito e open source che ti consente di comunicare in modo sicuro con la tua famiglia, amici e colleghi. È completamente decentralizzato utilizzando messenger peer-to-peer senza dipendere da alcun server centrale. Nessuno sa con chi stai comunicando, tranne il destinatario, ovviamente è un sistema distribuito, peer-to-peer (punto-punto) e con crittografia end-to-end, senza che nessuno o qualcosa possa disabilitare le opzioni di crittografia che incorpora. Non ci sono server che memorizzano i dati alle due estremità della catena.

PROVIDER E APPLICAZIONI PER LEGGERE LE MAIL

PROVIDER *E-MAIL* CRITTOGRAFATE

ProtonMail

Skiff mail

Tutanota

PROTON MAIL

Un'email sicura a tutela della privacy

Proton Mail è un servizio di posta elettronica privata che si serve della crittografia end-to-end open source, verificata con audit indipendenti e con crittografia ad accesso zero per proteggere le tue comunicazioni.In questo modo evita che i tuoi dati vengano violati e garantisce che nessuno (nemmeno Proton) possa accedere alla tua casella di posta. Solo tu puoi leggere i tuoi messaggi,decine di milioni di persone in tutto il mondo hanno scelto Proton Mail per preservare la privacy delle loro comunicazioni.

TUTANOTA

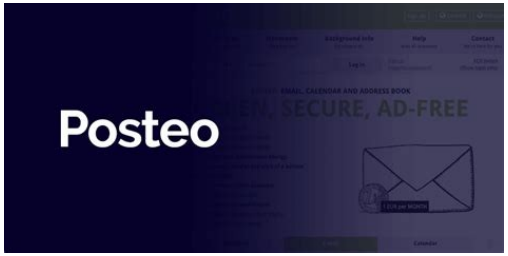
Tutanota è un software open source e libero di posta elettronica che offre una webmail crittografata, viene sviluppato e fornito da un'azienda tedesca Il nome Tutanota deriva delle parole latine tuta nota che significano «messaggio sicuro» Quando Edward Snowden ha rivelato nel 2013 i programmi di sorveglianza di massa della NSA, come XKeyscore, la loro visione è diventata ancora più diffusa.

SKIFF MAIL

SKIFF MAIL

L'account email è sicuro, utilizza la crittografia end-to-end. L'aspetto interessante, essendo un servizio di posta abbastanza nuovo, è che la maggior parte dei nomi sono ancora disponibili, contrariamente a quanto accade in altri servizi di posta in particolare, Skiff Mail offre un account email molto sicuro, archiviazione su cloud e creazione o modifica di documenti. Gli strumenti essenziali per il lavoro giornaliero per la maggior parte degli utenti.I dati associati al tuo account vengono sincronizzati su tutti i tuoi dispositivi. Le app di Skiff sono open source , puoi accedere all’app Web dal tuo browser o installare l’app mobile sul tuo dispositivo iOS o Android o l’app desktop sul tuo computer macOS.

servermx



mailbox.org

StartMail

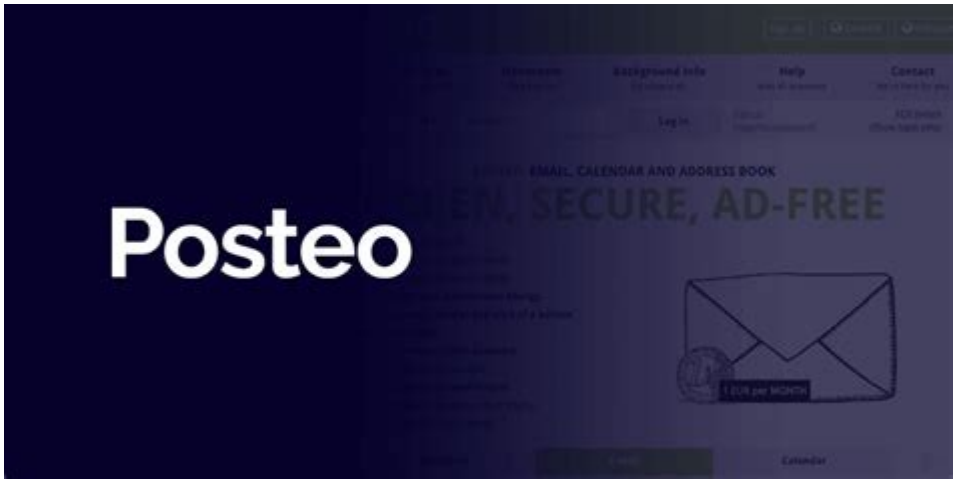
PROVIDER E-MAIL COMMERCIALI

Questi provider offrono una casella email gratuita o a pagamento ma non offrono la crittografia zero-knowledge come le altre.Sono tuttavia tutte aziende per ora considerate affidabili,costi bassi niente crittografia di default

INFOMANIAK

Il programma di posta sicuro per le tue e-mail

Consulta le tue e-mail in tutta sicurezza. Il servizio di messaggistica protegge automaticamente contro i virus ricevuti tramite le e-mail e i messaggi indesiderati. I filtri SPF, DKIM e DMARC sono in funzione per proteggerla da possibili spoofing.Il servizio di messaggistica è concepito per i professionisti, quindi studiato nei dettagli per aumentare la produttività e semplificare la gestione dei collaboratori. È un servizio di messaggistica affidabile, sviluppato e ubicato esclusivamente in Svizzera. Infomaniak gestisce oltre un milione di indirizzi e-mail professionali.



POSTEO

Posteo è un servizio di posta elettronica tedesco di cui l'infrastruttura informatica è basata esclusivamente su programmi open source. Posteo utilizza l'energia sostenibile fornita da Greenpeace Energy ed è senza pubblicità. Posteo non registra l'indirizzo IP dei visitatori e la connessione è sempre fatta in maniera cifrata con TLS et Perfect Forward Secrecy. Dal 2014, Posteo utilizza anche la tecnologia DANE (DNS-based Authentication of Named Entities). È possibile attivare l'autenticazione a due fattori grazie a una on-time password ricevuta su un altro dispositivo

MAILBOX.ORG

Comunicazione sicura - tutto il tempo.

mailbox.org è il provider di posta elettronica che mette al primo posto la protezione dei dati, la libertà dalla pubblicità e l'indipendenza. Rispetta la privacy dei propri clienti e mette le persone (non gli inserzionisti) al primo posto. Per garantire che la comunicazione sia sicura e senza tracciamento in molte situazioni, offre e-mail sicure e un ufficio online, archiviazione cloud e videoconferenza.

STARTMAIL

Invia email criptate a chiunque. Se il destinatario non utilizza la crittografia, può ricevere e rispondere alle tue e-mail crittografate con una password impostata per loro. La privacy europea al suo meglio StartMail si trova nei Paesi Bassi, il che significa che le e-mail e i dati sono protetti dalla legislazione olandese sulla privacy e dal GDPR. Anche i loro server si trovano qui.

SERVERMX

Servermx, è una società con sede nell'UE, e come tale, è soggetta al rispetto del GDPR. Di conseguenza, i dati personali gestiti (ricevuti, memorizzati o trasferiti) da servermx e dai suoi subappaltatori devono essere conformi al GDPR. Servermx memorizza i dati su server situati all'interno e all'esterno dell'UE. Quando si trova al di fuori dell'UE, il paese deve offrire un livello adeguato di protezione dei dati. L'UE regola se un paese non UE ha un adeguato livello di protezione dei dati

MailFence

La privacy è un diritto, non un optional

La criptografia avviene nel browser. Nessuno, incluso noi, può leggere le vostre email in transito. Compatibile con qualsiasi servizio OpenPGP. La crittografia punto-punto è un metodo per rendere sicuri i dati trasmessi da un mittente al destinatario. Con la crittografia punto-punto i dati sono protetti dal sistema di origine e solamente il destinatario potrà decifrarli. Nessun intermediario può leggere o alterare questi dati. Perciò questo metodo assicura un alto livello di protezione per le vostre comunicazioni.

Disroot.org

Autistici & Inventati

PROVIDER *EMAIL* ETICI

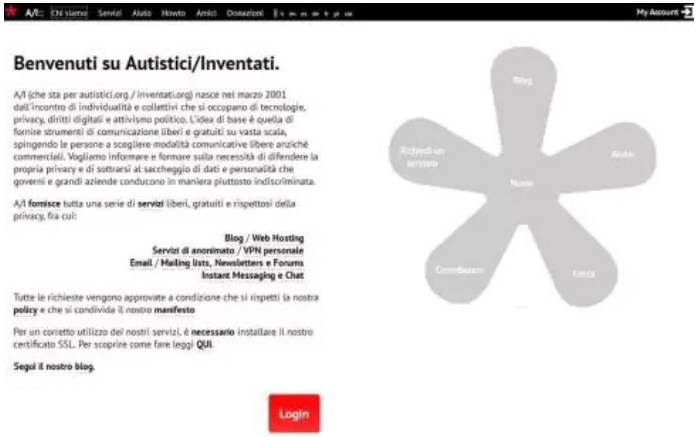
Questi sono provider *etici,*sempre con caselle email non crittografate zero-knowledge,che non cercano profitto e sono generalmente gestiti da associazioni o collettivi, mail gratuite o costi bassi

DISROOT.ORG

DISROOT.ORG

piattaforma gratuita, privata e sicura.

Poiché oggi la sicurezza è qualcosa che gli utenti dei servizi Internet cercano sempre di più, vale la pena conoscere progetti come questo. Disroot è un progetto con sede ad Amsterdam, gestito da volontari e dipendente dal sostegno della sua comunità. Come è nato, è chiaro che Disroot.org utilizza software libero, decentralizzato e soprattutto rispettoso della libertà/privacy. Inoltre, il loro servizio è "gratuito" (aperto alla donazione).



Autistici & Inventati

DISROOT.ORG

Perché crittare le mail. Se non sai cosa significa cifrare, crittare ecc., dai un'occhiata qui: https://it.wikipedia.org/wiki/Crittografia.Una mail che non è stata crittata ed è stata inviata tramite Internet è come una cartolina senza busta: postini, portieri, vicini e chiunque altro possa venirne in possesso sono liberamente in grado di leggere il messaggio che hai scritto.Non ci stancheremo mai di ricordare che l'uso della crittografia non serve a proteggere solo la tua privacy, ma anche quella dei tuoi corrispondenti.

RISEUP

Perché Riseup è necessario

Puoi fare affidamento su un provider di posta elettronica commerciale per quanto riguarda la riservatezza delle tue comunicazioni email? I provider commerciali non solo esaminano e registrano il contenuto dei tuoi messaggi per una vasta quantità di scopi, ma non hanno politiche rigorose riguardo la privacy dei loro utenti e cedono alle richieste dei governi che limitano le libertà digitali. Tutti i tuoi dati, inclusa la tua posta, viene memorizzata da riseup.net in forma crittografata

DOMINIO PERSONALIZZATO

Questi che elenco sono invece provider che offrono posta e dominio personalizzato in un solo pacchetto

SOVERIN

I servizi di posta elettronica 'gratuiti' che la maggior parte di noi utilizza quotidianamente hanno un prezzo. Semplicemente non esiste un servizio di posta elettronica gratuito. Alla fine qualcuno deve pagare per il costo di hosting, supporto e manutenzione. Nella maggior parte dei casi gli inserzionisti raccolgono i tuoi dati e in cambio ottengono l'accesso ai tuoi dati personali.

GANDI.NET

Gandi è un registro di nomi di dominio, un host web e un provider di certificati e-mail e SSL la cui ambizione principale è quella di rendere Internet accessibile a tutti. Ma soprattutto, Gandi è una storia di successo francese

SimpleLogin

AnonAddy

Firefox Relay

INOLTRO ANONIMO

Per non dare la email in giro, potete utilizzare degli inoltri automatici. Potete creare infinite cartelle email (anche con dominio personalizzato)che verranno inoltrate al vostro indirizzo principale,nascondendo il vero vostro indirizzo

FIREFOX RELAY

Perché utilizzare un alias

Con un alias email, si può ottenere un indirizzo email temporaneo usa e getta che consente di registrarsi a siti web o newsletter senza esporre le proprie informazioni personali. L'alias maschera il proprio indirizzo email originale per proteggerlo da abusi, aiutando a mantenere la propria identità e la propria casella di posta al sicuro da email indesiderate, truffe e fughe di dati. Un indirizzo email "mascherato" non può essere ricondotto all'indirizzo reale, rendendolo un'ottima opzione quando ci si iscrive a qualcosa online o si condividono le proprie informazioni di contatto con qualcuno di cui non ci si fida completamente.

SIMPLE LOGIN

In futuro proteggerà gli indirizzi e-mail reali

Inoltre, è open source, il cui codice sorgente è disponibile su GitHub . Inoltre ci consente di rispondere ai messaggi che abbiamo ricevuto direttamente con gli stessi indirizzi e-mail usa e getta utilizzati. E infine, se scegliamo di usarlo sul nostro server ufficiale, abbiamo un generoso piano gratuito, ideale per la maggior parte degli utenti, mentre il piano di pagamento è rivolto a utenti esperti, che tra l'altro potrebbero avere il proprio dominio per i gli indirizzi email usa e getta

ANONADDY

AnonAddy è completamente open source. Significa che il codice sorgente è accessibile a tutti e chiunque può vedere cosa c’è dentro. È Software Libero sia lato client che lato server e dunque potete anche, volendo, self-hostarlo per i fatti vostri se siete utenti esperti potete creare una mail personalizzata per ogni singola registrazione. Questo è utile per due motivi: intanto nel malaugurato caso la vostra email finisca in qualche archivio di spam potete semplicemente sopprimere l’alias e sostituirlo con un altro. Inoltre potrete scoprire se qualcuno ha venduto il vostro indirizzo email a terzi. Se infatti riceverete una mail promozionale su facebook@vostroutente.anonaddy.com non avete dubbi su chi possa aver venduto i vostri dati;