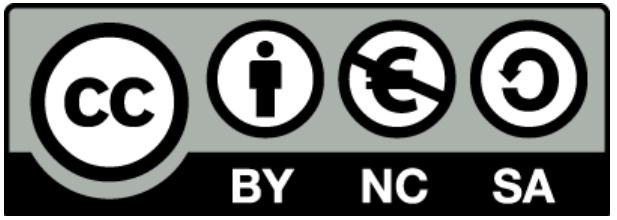
Appunti Privacy

Da Frank |Dic 26, 2023 | Guide

PROGRAMMI E APPLICAZIONI CHE TUTELANO LA PRIVACY



padloc

PSONO

bitwarden

Buttercup
The Password Manager You Deserve.

KeePass

GESTORI PASSWORD

La maggior parte dei gestori di password utilizzano l’Advanced Encryption Standard (AES) con chiavi a 256 bit generate casualmente. Si tratta di una delle forme di protocolli di sicurezza più elevata che i gestori di password possono utilizzare per la crittografia e per proteggere le informazioni. Le chiavi generate casualmente criptano le informazioni memorizzate nel software. Inoltre, la maggior parte dei gestori di password criptano localmente, il che significa che non memorizzano né rivedono mai le vostre informazioni. Prima che le vostre password vengano salvate nel password manager, queste vengono criptate in modo che l’azienda non sia a conoscenza di informazioni sensibili.

BITWARDEN

Caratteristiche:

Open-source Sincronizzazione con il cloud cripta informazioni riguardanti login, carte di credito, documenti d'identità e note testuali crittografia end-to-end, cronologia delle password, in modo tale da poter visualizzare anche quelle usate in passato, auto-riempimento durante i login generatore automatico di password,test della forza di una password,autenticazione a due fattori. Data breach reports basati sul sito Have I Been Pwned? Generatore di codici e deposito di chiavi TOTP applicazioni cross-platform

BITWARDEN

Applicazioni per gestire le proprie password

Bitwarden è un software libero di gestione delle password. Ha il compito di preservare informazioni sensibili (come le password) in un deposito cifrato. La piattaforma di Bitwarden offre molte applicazioni client, come un web interface, applicazioni desktop ed estensioni per browser. Bitwarden permette di creare una sorta di deposito di informazioni sensibili, accessibili solo dall'utente. Egli dovrà infatti impostare una master-password, una password complessa che garantirà l'accesso al software. All'interno dell'applicazione l'utente potrà elencare ogni singola password legata al nome utente e al sito dove ha fatto il login: in questo modo non sarà necessario ricordarsi le password perché di questo si occuperà Bitwarden.È possibile usare Bitwarden su più dispositivi, sincronizzando le password salvate. Il software cripta tutte le password elencate al suo interno, in modo da avere una sicurezza ulteriore.Bitwarden ha la possibilità di generare password sicure per l'utente, basterà infatti che venga indicata il numero dei caratteri e la tipologia di caratteri che si vogliono utilizzare.

CREDIT WIKIPEDIA

PADLOC

Padloc è una soluzione open source che offre una serie di funzionalità interessanti per uso personale, familiare o aziendale. Alzi la mano chi ha meno 20 password e se le ricorda tutte!!! dobbiamo prenderci tutti un impegno: trovare uno strumento semplice che ci consenta di gestire le tante password che le varie piattaforme ci richiedono di utilizzare e che finiamo abitualmente per dimenticare.

KEEPASS

Audit di sicurezza,un password manager offline,leggero e totalmente gratuito. Potete sfruttarlo anche con l’applicazione web https://keeweb.info/ oppure con KeepassXC e Keepass2 Android. Gratuito,open source e libero e più completo di altre alternative. Le password memorizzate nell'applicazione possono essere divise in gruppi; ogni gruppo ha una sua icona, che lo identifica.

BUTTERCUP

Buttercup è un ottimo password manager creato per mettere al sicuro le password degli account sia sui PC Windows, Mac e Linux che sui principali browser come Google Chrome. Questo programma permette di gestire al meglio le molte password che si utilizzano nei vari account. Per garantire la massima affidabilità, il database delle password è protetto attraverso un sistema di crittografia a 256 bit. Buttercup si utilizza molto facilmente, merito di un'interfaccia molto ben strutturata e di facile accesso. Il programma permette anche di creare delle categorie per organizzare al meglio l'archiviazione delle password

PSONO

PSONO

Psono è un gestore di password gratuito per i team,tuttavia con Psono si ottiene un gestore delle credenziali open source, completamente sicuro che è progettato tenendo presente i team. La comodità principale di utilizzare i gestori di password open source come Psono è la possibilità di accedere alle tue informazioni critiche da qualsiasi luogo. Applicazione che permette anche il self-hosting è dedicata sopratutto alle aziende e a chi deve utilizzare password manager in gruppo. Europeo,open source e libero

PASSBOLT

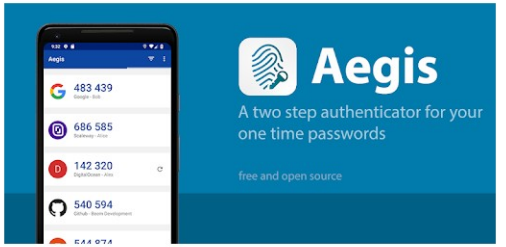
Passbolt è il password manager open source progettato per professionisti e aziende

Passbolt utilizza il protocollo OpenPGP per crittografare le password rendendole irrecuperabili in chiaro dagli utenti non in possesso delle credenziali corrette; inoltre, il software tiene traccia degli accessi all'archivio delle password e delle modifiche via via apportate. Passbolt è un software open source per la gestione delle password progettato per le imprese e i professionisti che desiderano migliorare la sicurezza delle credenziali. L'applicazione funziona come un password manager centralizzato che consente agli utenti di creare, gestire e condividere le proprie password in modo sicuro. Il software utilizza la crittografia end-to-end per garantire la massima sicurezza delle password.

auth
Ente Authenticator

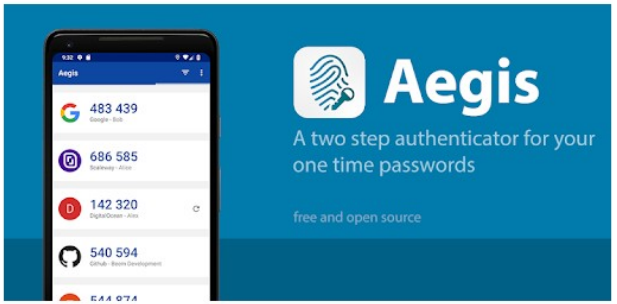
bitwarden

Standard Notes
100% free, 100% private, open-source, and completely encrypted notes app



AUTENTICAZIONE A DUE FATTORI

Si sconsiglia l’uso dello stesso password manager per gestire i numeri creati dall’autenticazione a due fattori



AEGIS

l modo in cui Aegis si differenzia maggiormente da Google Authenticator, oltre all’essere open source (qui il codice sorgente), la si trova nel modo di funzionare: Aegis assicura la massima sicurezza non richiedendo alcun accesso a internet ma funzionando totalmente offline. Seppur l’hackeraggio dei sistemi Google possa sembrare impossibile, è sempre qualcosa che può avvenire. Con Aegis questo problema non c’è.

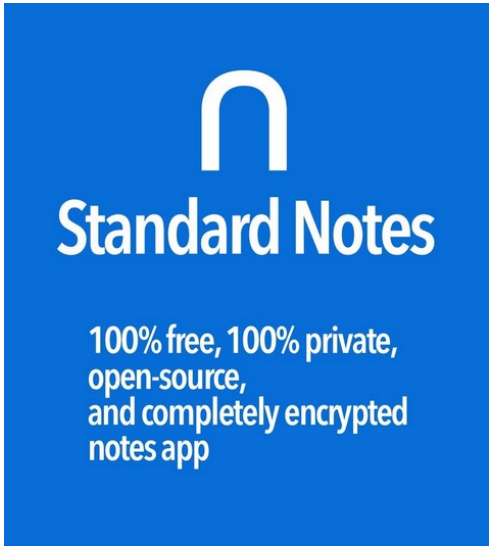
auth

Ente Authenticator

ENTE AUTHENTICATOR

BACKUP SICURI

Ente Authenticator fornisce backup cloud crittografati end-to-end in modo che tu non debba preoccuparti di perdere i tuoi token. Utilizzano gli stessi protocolli utilizzati da ente Photos per crittografare e conservare i tuoi dati. Archivia in modo sicuro i token di verifica in due passaggi (2FA).



NOTA STANDART

Autenticazione a due fattori: migliora la sicurezza del tuo account

L’autenticazione a due fattori (2FA) è una funzione di sicurezza che aggiunge un ulteriore livello di protezione al tuo account. Richiede un token basato sul tempo oltre alla tua password per accedere al tuo account. Questo aiuta a garantire che solo tu abbia accesso al tuo account, anche se la tua password è compromessa.

AUTENTICAZIONE A DUE FATTORI

Non usare come password manager se si usa come autenticazione a due fattori

matrix

APPLICAZIONI DI MESSAGGISTICA FEDERATE E CON PROTOCOLLI LIBERI

Si fa presto a dire *alternativa a WhatsApp*,queste applicazioni sfruttano protocolli liberi e che permettono la federazione dei server

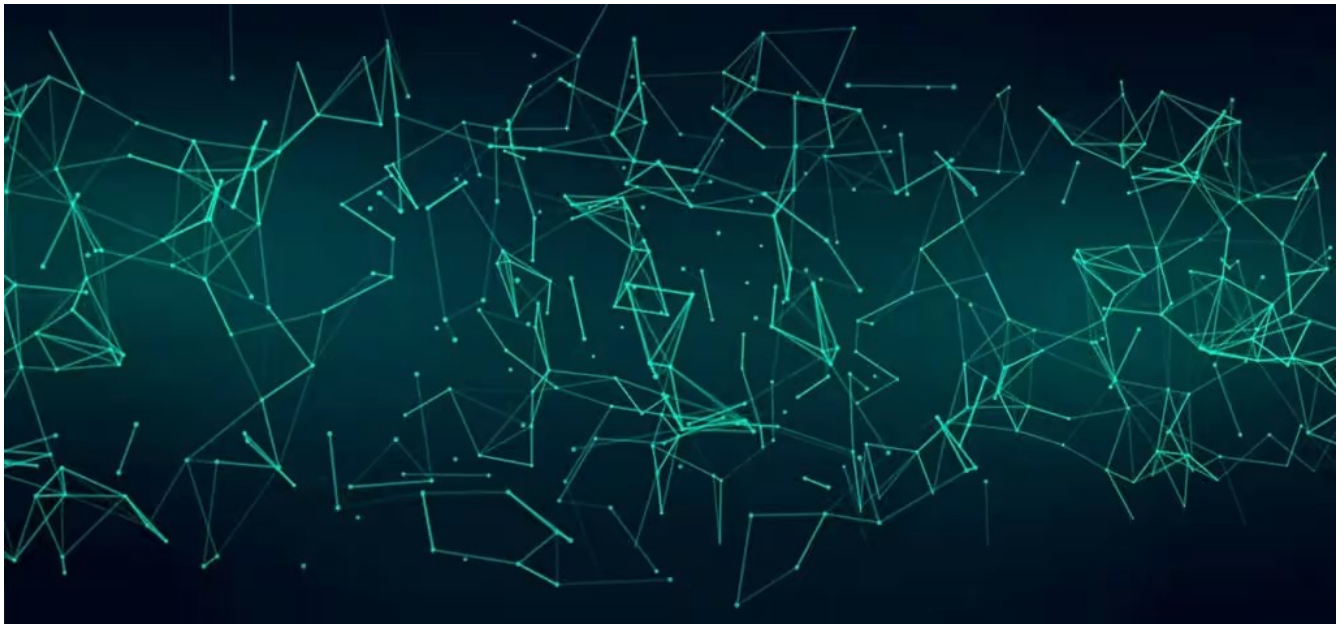
DELTA CHAT

Invia messaggi a chiunque abbia un indirizzo e-mail anche se non utilizzano Delta Chat. Crittografia end-to-end utilizzando i protocolli Autocrypt e CounterMITM, con più controlli di sicurezza. Audit di sicurezza E2E idea folle e geniale utilizzare le email come sistema di messaggistica istantanea. Bella idea ma purtroppo le mail non nascono sicure, disponibile su dispositivi mobili e desktop

MATRIX

Matrix è un protocollo aperto per la messaggistica istantanea. È stato progettato per consentire agli utenti di comunicare tramite chat,Voice over IP e Videotelefonia. Da un punto di vista tecnico, è un protocollo di livello applicazione per la comunicazione decentralizzata in tempo reale. Il protocollo tenta di sostituire i protocolli come XMPP e IRC di risolverne i problemi associati.

Credit Wikipedia



APP Client MATRIX

Element

FluffyChat

Cinny

Quadrix

Fractal

SchildiChat

SYPHON

NeoChat

XMPP

Extensible Messaging and Presence Protocol (XMPP) (precedentemente noto come Jabber) è un insieme di protocolli aperti di messaggistica istantanea e presenza basato su XML. Il software basato su XMPP è diffuso su migliaia di server disseminati su internet; secondo la XMPP Standards Foundation (precedentemente nota come Jabber Software Foundation), già nel 2003 era usato da circa dieci milioni di persone in tutto il mondo. Sistema decentralizzato l'architettura di XMPP è simile alle email; chiunque può realizzare il proprio server XMPP e non si identificano server centrali.

Credit Wikipedia

OpenStreetMap

OsmAnd
Maps & Navigation

ORGANIC MAPS

Qwant Maps

Mappe e navigatori

Le mappe, dopo la ricerca sono una delle cose che Google fa meglio. È anche una delle applicazioni dove Google fa incetta di dati. Ecco alcune soluzioni alternative

OPEN STREET MAP

OpenStreetMap (OSM) è il più grande database geografico libero e modificabile di tutto il mondo, costruito dal lavoro di volontari e rilasciato con una licenza libera. Si tratta di un gigantesco progetto collaborativo, con milioni di utenti registrati in tutto il mondo, il cui scopo è creare e fornire dati geografici liberi a chiunque li voglia utilizzare. La comunità italiana è particolarmente attiva non soltanto nel mantenere la mappa di OpenStreetMap aggiornata, ma anche nell'organizzare eventi di formazione, divulgazione e condivisione.

OsmAnd

OsmAnd (acronimo per OpenStreetMap Automated Navigation Directions) è un’app libera per la navigazione e la visualizzazione di mappe online ed offline per Android e iOS. Tutte le mappe possono essere memorizzate all'interno del dispositivo per l'utilizzo offline. Anche grazie al GPS o altri sistemi di posizionamento OsmAnd offre la possibilità di esplorare le mappe godendo di tutti i punti di interesse (POI, Points of Interest) di OpenStreetMap e di utilizzare l'app come navigatore con voce guida per auto, biciclette e pedoni

ORGANIC MAPS

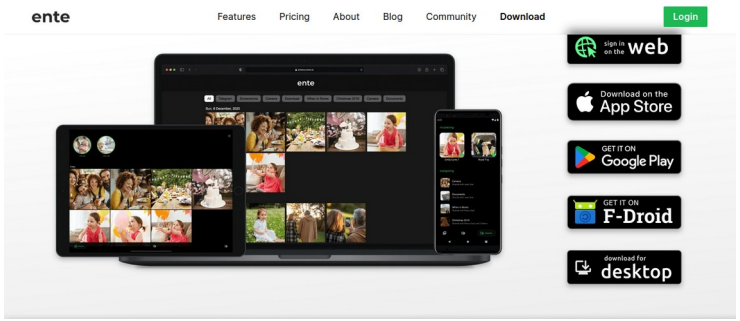
Perché Organic?

Rispetta la tua privacy,risparmia la batteria, nessun addebito imprevisto sui dati mobili, Organic Maps è priva di tracker e di altri elementi negativi: Nessuna pubblicità,nessun tracciamento nessuna raccolta dati nessuna chiamata a casa nessuna registrazione fastidiosa nessun tutorial obbligatorio nessuno spam di e-mail fastidiose nessuna notifica push nessun crapware nessun pesticida puramente organico!

Qwant

Qwant Maps: il meglio della cartografia unito al rispetto della tua vita privata

Zero tracciamento delle tue ricerche Zero tracciamento pubblicitario Zero vendita dei tuoi dati personali. Con Qwant Maps, la vostra posizione non viene mai memorizzata e i vostri dati di geolocalizzazione non vengono mai venduti.



ENTE PHOTOS

Stingle Photos

Jottacloud

PROVIDER PER LA GESTIONE DI FOTO E VIDEO ONLINE

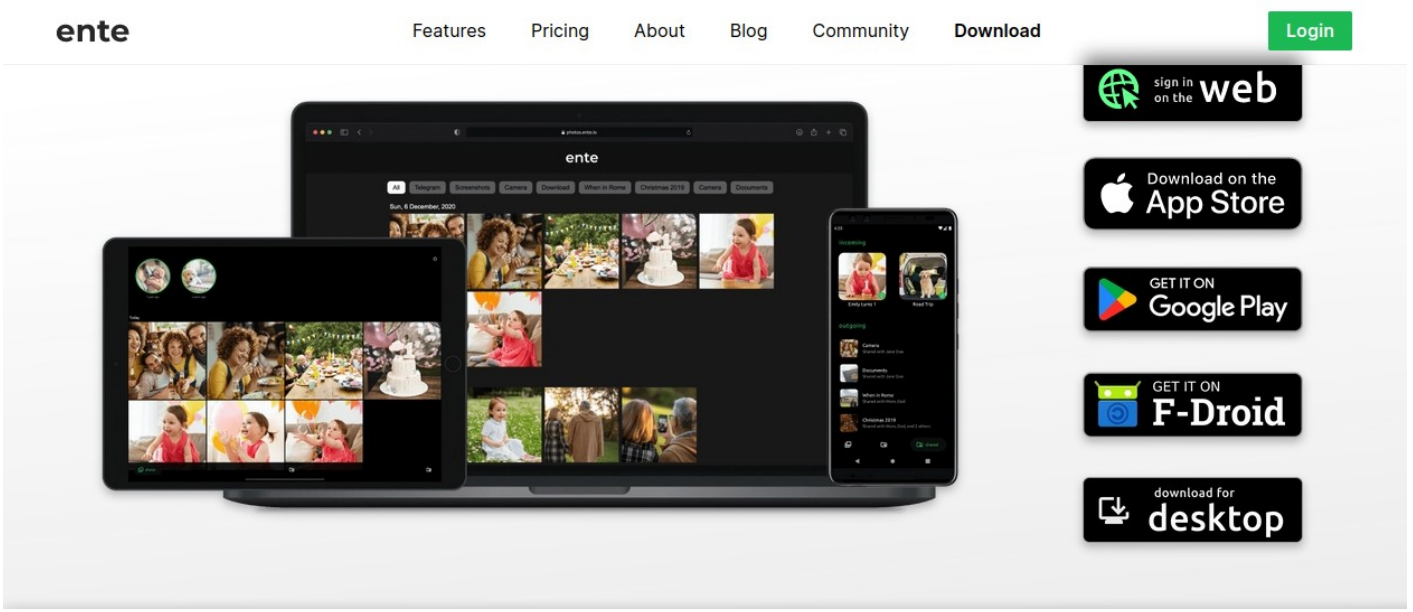
Perché andarsene da Google Foto?

È possibile mettere le foto e i video su uno qualsiasi dei cloud elencati qua sopra

JOTTACLOUD

Privacy di livello mondiale

Jottacloud è una società norvegese che opera sotto la giurisdizione norvegese. La Norvegia ha alcune delle più forti leggi sulla privacy nel mondo. Sono ovviamente conformi al GDPR.



ENTE PHOTOS

È un progetto open source significa che il codice sorgente è accessibile a tutti e chiunque può vedere cosa c’è dentro. Davvero molto interessante: Ente è un’ottima alternativa a Google Photos, probabilmente una delle migliori. L'architettura di Ente permette l’archiviazione di fotografie e video con crittografia zero-knowledge: significa che nessuno, nemmeno loro, possono vedere quello che avete caricato su Ente. Tutto viene crittografato e voi sarete gli unici a possedere la chiave per decriptare il tutto. Tutto è open source e verificabile. È a pagamento

STINGLE PHOTOS

Ha dimostrato nel tempo di essere un’ottima alternativa a Google Photos. Stingle Photos è open source, ne vale sicuramente la pena visto che offre un sistema di crittografia molto interessante. È un’ottima applicazione per le proprie fotografie, bellissima graficamente, veloce e semplice da utilizzare.

CryptPad

Nextcloud

HedgeDoc

Filen

kDrive

Seafile

etherpad

COLLABORAZIONE DOCUMENTI ONLINE

In questa sezione sono elencati i provider che permettono di condividere e modificare documenti contemporaneamente con altre persone

CryptPad

CryptPad

CryptPad

Una suite office completa, criptata e open-source! Le idee migliori non nascono da un singolo, c’è bisogno che più menti collaborino insieme. Esiste anche una istanza gratuita dei Devol Testi,fogli di calcolo,lavagne e anche form crittografia zero-knowledge open source possibilità di collaborare in tempo reale con altri utenti

FILEN

Sicurezza di livello militare

Filen utilizza la crittografia AES-GCM a 256 bit. Tutti i file saranno archiviati in data center di alta sicurezza certificati Tier IV ISO 27001 distribuiti in Germania. Condividi contenuti selezionati in forma crittografata tramite collegamenti pubblici/ privati o direttamente con altri utenti Filen.

NEXTCLOUD

Perché i governi utilizzano Nextcloud?

I governi si stanno allontanando dai fornitori di cloud stranieri a causa delle crescenti preoccupazioni sulla sovranità digitale. Nextcloud è emersa come la soluzione di cloud privato self-hosted più utilizzata dai governi. Nextcloud è progettato per offrire la migliore produttività della categoria e viene sviluppato a un ritmo impressionante, con nuove funzionalità disponibili ogni pochi mesi.

kDrive

KDRIVE

kDrive è compatibile con tutti i dispositivi. Che tu sia in ufficio, a casa o fuori, puoi lavorare, condividere e accedere tranquillamente a tutti i tuoi dati. Le caratteristiche di sincronizzazione di kDrive sono complete e simili a quelle dei concorrenti. La sicurezza dei dati nel cloud ha molte sfaccettature: I dati sono protetti e criptati in caso di hacking sui server kDrive. Cosa succede se i server fisici che immagazzinano i dati vengono distrutti (ad esempio come l’incendio avvenuto in OVH)?

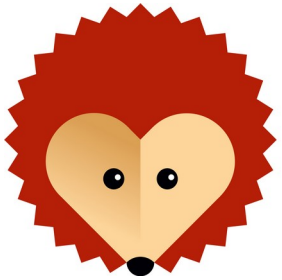
ETHERPAD

L'applicazione permette di vedere in tempo reale tutte le modifiche effettuate dai partecipanti, con la caratteristica di mostrare il testo di ogni autore con un diverso colore. Accanto al testo è presente una finestra di chat che permette ai diversi partecipanti di interagire tra loro. Etherpad è un editor collaborativo in tempo reale. È molto semplice da utilizzare, minimale ma con un editor markdown. Open source e gratuito, chiunque può aprirne un'istanza Server su cui gira un determinato software. Ad esempio mastodon.uno è un'istanza italiana di Mastodon Noi vi consigliamo quella del collettivo italiano Devol: etherpad.devol.it

SEAFILE

Seafile è un software orientato alla sicurezza per la fornitura di servizi di backup, sincronizzazione automatica, file hosting e condivisione di file tramite web. Seafile è un software basato su cloud storage criptato e con supporto multipiattaforma, disponibile per sistemi operativi desktop Windows, MacOS, Linux) e per dispositivi mobili (iOS, Android)

Credit wikipedia



HedgeDoc

HedgeDoc

HedgeDoc è una risorsa software open source, web-based, che consiste in un editor markdown collaborativo. In sostanza, con HedgeDoc è possibile scrivere documenti in markdown utilizzando l’interfaccia web mediante il browser e condividerli con altri, sia in sola lettura sia autorizzando l’editing a seconda dei permessi che si intendono impostare. È possibile utilizzare HedgeDoc in modalità self-hosted, installandolo sul proprio server.Il codice sorgente è disponibile su GitHub.