ObscureIQ's guide to

Which Email Services Offer the Most Privacy & Anonymity?

Secure Cloud	Privacy Level	Anonymity Potential	Cyber Security	Ease of Use	Score	Features	Notes
Anonymous Email Aliasing & Forwarding Services							
SimpleLogin	5	4	4	5	18	Unlimited aliases, custom domains, PGP support	Open-source, supports self-hosting
AnonAddy	5	4	4	3	16	Unlimited aliases, custom domains, PGP encryption	Open-source, supports self-hosting
Firefox Relay	4	3	3	5	15	5 free aliases (premium for more)	Owned by Mozilla, limited features
Apple Hide My Email	4	3	3	5	15	iCloud+ required, auto-generates aliases	Apple ecosystem only
DDG Email Protection	4	3	3	5	15	Strips trackers, provides forwarding	Not full aliasing, just privacy filtering
Disposable & Temporary Email Services							
Guerrilla Mail	3	4	2	5	14	No sign-up, emails last 1 hour	Temporary only
Best for Anonymity & Sending Emails: Allows sending emails (most temp email services only receive). Can maintain a persistent inbox if used frequently. Accessible over Tor, making it better for anonymous use.							
Temp Mail	3	4	2	5	14	No sign-up, temporary inbox	Emails can be public
Best for Mobile Use: Has a mobile app, making it more convenient if you need temp emails on the go. Provides longer inbox retention than 10 Minute Mail.							
10 Minute Mail	3	4	2	5	14	Auto-deletes after 10 mins	One-time use only
Best for Quick One-Time Use: Simple and fast - if you only need an email for a single-use signup, this is ideal. No storage beyond 10 minutes, so best for immediate verifications.							
EmailOnDeck	3	4	2	5	14	Quick temp email, no reg	Not for long-term use
Long-Term Private Email Accounts							
Proton Mail	5	4	5	3	17	End-to-end encryption, Tor access	Requires sign-up (can use aliases)
Best for Mainstream Privacy & Security: Strong encryption, aliases, and legal protection under Swiss law. Tor access for anonymity. Custom domains, biz plans = flexible. Easier to use than Tutanota but reqs a recovery email.							
Tutanota	5	4	4	3	16	Zero-access encryption, anonymous sign-up	Requires account creation
Best for Maximum Anonymity: No recovery email req (unlike Proton). Fully encrypted emails, contacts, calendar. No IMAP/SMTP support, must use Tuta app. Better for activists, journalists, those who want true anonymity.							
Skiff Mail	4	4	4	5	17	End-to-end encrypted, no phone required	Web3 focus, limited features
Best for Web3 & Crypto Users: Decentralized approach with IPFS storage integration. Integrates with crypto wallets (e.g., Ethereum, Solana). Better suited for blockchain and privacy enthusiasts.							
Mailbox.org	5	5	3	5	18	PGP encryption, anonymous sign-up, secure office suite	Germany, strong EU privacy laws
Best for Professionals & Power Users: PGP encryption, anonymous sign-ups, and a full productivity suite (email, calendar, contacts, cloud storage, etc.). Requires some technical knowledge to configure PGP encryption correctly.							
StartMail	5	4	3	5	17	PGP encryption, unlimited aliases, IMAP/SMTP support	Startpage team, Netherlands-based
Best for Ease of Use with Strong Privacy: simpler than Proton and Tutanota but still offers PGP encryption, unlimited aliases, and IMAP/SMTP support. Integrates w/ third-party clients (Outlook, Thunderbird, Apple Mail, etc.).							

🔷 Privacy: Measures how well the service protects your data and metadata from unauthorized access, tracking, or leaks. This includes encryption strength (both in transit and at rest), data collection policies, backup security, and third-party access. Higher scores indicate strong encryption, minimal data collection, and strict safeguards against leaks.
🔷 Anonymity Potential: Evaluates how effectively you can use the service without linking your identity. This considers pseudonymous sign-ups, minimal verification requirements, and whether personal data is optional. Higher scores mean you can register and us/e the service with little to no personal information exposure.
🔷 Ease of Use: Assesses the service's intuitiveness, accessibility, and overall user experience. Factors include interface design, setup complexity, and learning curve. Higher scores reflect a service that is straightforward, user-friendly, and requires minimal effort to use effectively.
🔷 Cybersecurity: Measures the service's encryption strength, protection against breaches, and account security features like 2FA. Higher scores indicate strong encryption, no known security incidents, and third-party security audits.