STAYiNG SAFE ON THE INTERNET

STEPS TOWARD COMPUTER SECURITY

THREATS

- Phishing Attacks
- Password Theft and Credential Stuffing
- Malware and Ransomware
- Social Engineering and Impersonation Scams
- Public Wi-Fi and Man in the Middle Attacks
- Data Harvesting

COUNTERMEASURES

- Antivirus Software
- Secure Email
- VPNs
- Secure Messaging
- Paying Online
- Password Managers
- Private Browsing

WHAT DOES ANTIVIRUS SOFTWARE DO?

- Scanning for Malware
- Detecting and Identifying Malware
- Blocking and Quarantining Threats
- Updating Malware Definitions
- Protecting Against Phishing and Malicious Websites
- Monitoring Email Attachments and Downloads
- Providing System Security Features
- Reporting and Alerts

ANTiVIRUS SOFTWARE

- Antivirus is necessary but not foolproof
- Regular updates are essential
- Free versions have limits
- False sense of security is dangerous
- Performance and privacy vary by product

ANTiVIRUS – YOU GET WHAT YOU PAY FOR

- **Bitdefender Antivirus Plus**
  - Excellent malware detection
  - Minimal system impact
  - Great phishing and ransomware protection
- **Norton 360**
  - Comprehensive security suite
  - VPN included
  - Strong identity theft protection (in higher-tier plans)
- **McAfee Total Protection**
  - Good malware protection
  - Includes a VPN and identity monitoring
  - Often bundled for multiple devices
- **Trend Micro Maximum Security**
  - Good anti-phishing and ransomware protection
  - Extra privacy protection tools

ANTiVIRUS – FREE OPTiONS (CAVEAT EMPTOR…)

- **Bitdefender Antivirus Free**
  - Simple, no-nonsense protection
  - Great detection rates
- **Avast Free Antivirus**
  - Good protection and extra tools
  - Some past privacy controversies — now better regulated
- **AVG AntiVirus Free**
  - Owned by Avast (uses the same core engine)
  - Includes basic web & email protection

- **Microsoft Defender (built into Windows)**
  - Very good baseline protection, especially with Windows 10/11
  - No nagging ads or upsells
  - Improved a lot in recent years
- **Microsoft Defender (built into Windows)**
  - Very good baseline protection, especially with Windows 10/11
  - No nagging ads or upsells
  - Improved a lot in recent years

EMAiL

- Gmail, Yahoo, AT&T, etc.
  - All work the same
  - All leak data
- “If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.”
- If something is free, it’s because you are the product, not the customer.

PRIVATE OPTIONS

- **Tutanota (www.tuta.com)**
  - Based in **Germany** (strong privacy laws, GDPR)
  - Full **end-to-end encryption**, even for subject lines and metadata where possible
  - No tracking or ads
  - Open source
  - Free and paid versions
  - **Limitation**: Limited third-party client support (mostly works through their apps and web interface).
- **Mailfence (www.mailfence.com)**
  - Based in **Belgium** (also strong privacy laws)
  - **End-to-end encryption** (OpenPGP-based)
  - Focus on compatibility with external email (better than Proton in some use cases)
  - Calendar and document storage included
  - Paid service; limited free tier

VPNS

- **Encryption of Internet Traffic**
  - A VPN encrypts the data traveling between your device and the VPN server.
  - This protects your traffic from **eavesdropping** by:
    - Hackers on public Wi-Fi
    - Your internet service provider (ISP)
    - Potentially malicious actors on local networks
  - Even if someone intercepts your traffic, it will appear as **gibberish** without the encryption key.
- **Protection on Public Wi-Fi**
  - Public Wi-Fi networks (cafes, hotels, airports) are often poorly secured.
  - A VPN shields your activity from **other users on the same network**.
  - Prevents **man-in-the-middle (MITM) attacks** that can steal passwords or data.

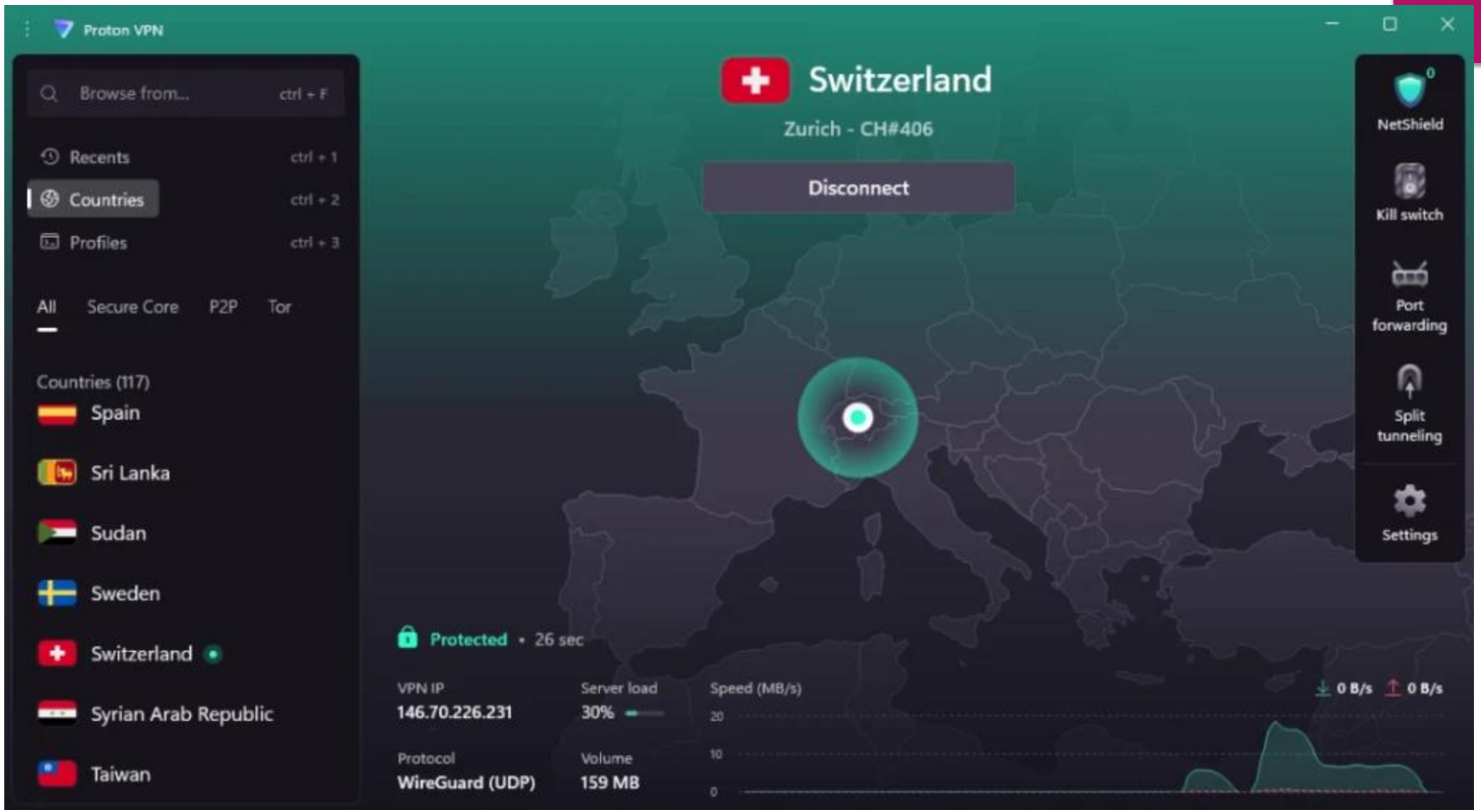
VPNS – CONTINUED

- **IP Address Masking**
  - The VPN server masks your **real IP address**, replacing it with its own.
  - This helps obscure your physical location and makes it harder to link activity to your device.
  - Good for:
    - Evading tracking
    - Countering IP-based restrictions
    - Protecting against targeted attacks
- **Bypassing Censorship and Geo-restrictions**
  - Not strictly a "security" benefit, but related:
    - VPNs let you access **blocked or restricted content** by appearing to be in a different country.
    - This can be vital in **authoritarian countries** or for journalists/activists.
- **Avoiding ISP Tracking and Throttling**
  - ISPs can no longer easily **track your browsing** if you're using a VPN.
  - VPN encryption also prevents ISPs from selectively **throttling** certain types of traffic (e.g. streaming services).

SOME VPN CHOICES

- **Mullvad VPN**
  - Based in **Sweden** (GDPR-compliant, strong privacy culture)
  - Unmatched **privacy focus**: no email required, no account required — you can pay anonymously (even cash!)
  - **No logs**, open-source clients, fully audited
  - Very transparent company
  - Fast and stable
  - No tracking, no advertising
  - Simple flat pricing ($6/month), no complicated tiers
  - **Ideal for**: Power users, privacy maximalists, people concerned about surveillance or anonymity

- **NordVPN**
  - **Strong Security** and **Fast Speeds**
  - **Extra Security Features**
  - **Double VPN**: traffic routed through two VPN servers
    - **Onion over VPN**: combines VPN with Tor network
    - **Kill switch**: cuts internet if VPN connection drops
    - **Threat Protection**: blocks malware, phishing sites, and ads
  - **Good value**
    - Frequently discounted multi-year plans
    - Allows up to **10 devices** on one subscription (recently expanded)
  - **Cons**
    - **Not as privacy-pure as some competitors**
      - NordVPN is a **commercial service**; part of Nord Security group (owns other brands like Surfshark now).
      - It is reputable and audited, but **not as privacy-committed** as, say, Mullvad.

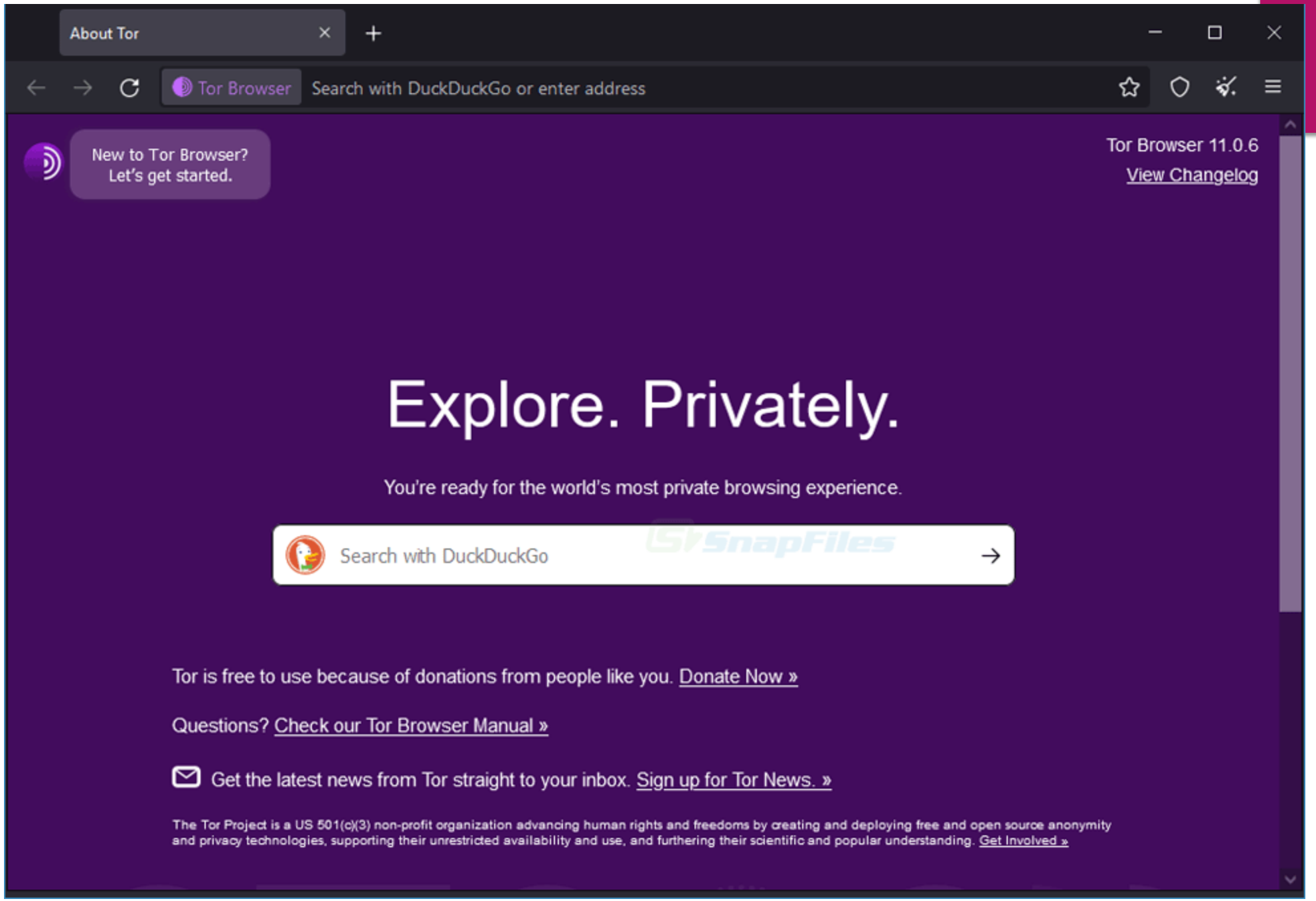

Proton VPN
Browse from... ctrl + F
Recents ctrl + 1
Countries ctrl + 2
Profiles ctrl + 3
All
Secure Core
P2P
Tor
Countries (117)
Spain
Sri Lanka
Sudan
Sweden
Switzerland
Syrian Arab Republic
Taiwan
Switzerland
Zurich - CH#406
Disconnect
NetShield
Kill switch
Port forwarding
Split tunneling
Settings
Protected • 26 sec
VPN IP
146.70.226.231
Server load
30%
Protocol
WireGuard (UDP)
Volume
159 MB
Speed (MB/s)
20
10
0
0 B/s
0 B/s

BROWSING – TOR (PROS)

- **Hides your IP address**
  - Your connection is routed through **three randomly selected Tor relays** (nodes).
  - The website you visit sees only the **exit node's IP**, not yours.
  - Your ISP sees only that you're connecting to Tor, but not what you're doing.
- **Encrypts traffic within the network**
  - Your data is **encrypted multiple times** (hence the "onion" metaphor).
  - Until it reaches the **exit node**, no one — not even the relays — can see what you are doing.
- **Defends against traffic analysis**
  - Tor makes it very hard for adversaries (like ISPs, corporations, governments) to track your browsing behavior across sites.
  - Defeats many forms of **fingerprinting and tracking**.
- **Tor Browser is hardened**
  - It is based on **Firefox ESR**, with added privacy protections.
  - Blocks trackers, disables many types of fingerprinting.
  - Forces HTTPS where possible.
  - Regularly updated and audited by privacy/security researchers.
- **Free and open source**
  - No need to trust a company — code is public and globally scrutinized.

BROWSING – TOR (CONS)

- **Exit node sees unencrypted traffic**
  - The **Tor network itself does not provide end-to-end encryption beyond the exit node**.
  - If you're visiting a **non-HTTPS** website, the **exit node can see your traffic**.
  - Always use **HTTPS** websites with Tor!
- **Slow speeds**
  - Tor is **much slower** than VPNs or normal browsing — it's not built for speed.
  - Not good for streaming or large downloads.
- **Some sites block Tor users**
  - Many websites either block known Tor exit nodes or present extra CAPTCHAs.
- **Known to be used**
  - Your ISP can see that you're using Tor (though not what you're doing).
  - In some authoritarian countries, using Tor may itself attract scrutiny (though bridges and pluggable transports can help).
- **Does not protect you from endpoint compromise**
  - If your computer is compromised, or you enter identifying info into websites, Tor cannot save you.
  - JavaScript can still be risky (though Tor tries to mitigate this — safest to use **Safest Mode**).


About Tor
Tor Browser
Search with DuckDuckGo or enter address
New to Tor Browser?
Let's get started.
Tor Browser 11.0.6
View Changelog
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Tor is free to use because of donations from people like you. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

THE WHOLE PACKAGE...

- **Proton.me** (formerly ProtonMail)
- Based in Switzerland (strong privacy laws, outside US jurisdiction)
- End-to-end encryption for emails and data
- Zero-access to user data (even Proton can't read your emails)
- Open-source and transparent security practices
- Free tier available, paid plans with extra features (storage, custom domains)
- No ads or tracking
- Strong commitment to user privacy and security
- Ideal for: Privacy-conscious individuals, secure communication, users looking for encrypted email services