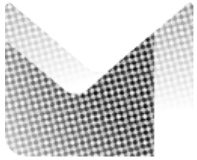
Here, we take a look at easy-to-use ProtonMail—and why we the CLDC can't recommend it (or its security model) for people opposing the powerful.

Outrun the Bear:
ProtonMail is Not for Activists

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.



Proton Mail

Outrun the Bear: ProtonMail is Not for Activists

Original text in English

Michele Gretes for the Civil Liberties Defense Center

2017

cldc.org/protonmail

Layout

No Trace Project

notrace.how/resources/#protonmail

I do really like that ProtonMail offers end-to-end encryption and the possibility to create anonymous accounts—this latter choice is especially important for at-risk activists. The only issue with it is that you might have to refresh your Tor circuit a few times. Two-factor authentication can be a nice layer of protection, too. But fundamentally, its incompatibility with GPG and the ease with which PM could actively attack you to gain access to your encrypted email makes it impossible for us to recommend for anyone at elevated risk.

Once Ed Snowden disclosed the scope and scale of U.S. global surveillance, many folks began to take their digital privacy and security seriously. Not everyone did: "Well I have nothing to hide!" bleated certain liberals and Obama supporters. That might be a fair point. If you're willing to ignore/destroy your Fourth Amendment right to privacy AND totally conform your beliefs, words, and actions to those of an ecocidal/racist/colonial State, then I suppose you *might* have less to hide. Also, if you don't mind gaining security by making bait out of the masses or your erstwhile comrades, ProtonMail might be for you! But when you decide to take solidarity-minded, effective action in defense of our planet and its peoples and creatures, making good secure-tech choices is worth thinking about carefully. Get in touch. We can help you prepare.

And remember, there is no such thing as total security these days when it comes to digital communications. It is imperative for our movements to take ourselves and our political organizing seriously, which means keeping up to date on the best practices available to us. Become a CLDC member[21] and support our continued efforts to provide digital security expertise for activists. Check out our digital defense posts[22] for updates often and regularly!

[21] https://cldc.org/get-involved

[22] https://cldc.org/category/security

3. ProtonMail doesn't work with a local email client (IMAP), so you can't use it with our recommended option (Thunderbird/Enigmail GPG). There is a Closed-Source Beta IMAP Client[15] in the works that will let you use an email client, but there's no way right now for anyone to assess its security[16].
4. You have to rely entirely on PM servers to play nice. (Someone is working on a project to run your own PM server if you wanted to, but this effort is unsupported by PM[17] itself, and we haven't examined how well it works or how secure it is.)
5. PM doesn't issue a warrant canary[18], which is a way for online service providers to reliably let their users know if they have been compromised in the event they are served with a warrant or other court order containing a gag order (Riseup[19] does this.)

[10] https://cldc.org/signal-activist-best-practices

[11] https://cldc.org/authenticity

[12] https://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems

[13] https://www.wired.com/2015/10/mr-robot-uses-protonmail-still-isnt-fully-secure

[14] *N.T.P. note:* As of 2021, it is now possible for ProtonMail users to exchange encrypted messages with non-ProtonMail users using PGP[20]. However, the other reasons for not using ProtonMail are still valid.

[20] https://protonmail.com/support/knowledge-base/how-to-use-pgp

[15] https://protonmail.com/bridge

[16] *N.T.P. note:* As of 2021, it is possible to use ProtonMail with a local email client, but it requires a "Plus" ProtonMail account at 4€/month.

[17] https://github.com/emersion/neutron/commit/4aab8d9f154a2b191d9427ff404bde3f30d4b291

[18] https://www.eff.org/deeplinks/2014/04/warrant-canary-faq

[19] https://riseup.net/canary

"You don't have to outrun the bear" is a security model where you stay safe from predators on camping trips by taking your chain-smoking, out-of-shape buddy along. In case of bear attack, you can feel secure knowing you can outrun your (former) friend. This security model is offered by many Snowden-era startups claiming to provide digital security to the masses. Can this be good enough for activists? Here, we take a look at easy-to-use ProtonMail—and why we at the CLDC can't recommend it (or its security model) for people opposing the powerful.

First off, if you currently rely on ProtonMail for your organizing, please don't feel you need to quit using it straight away. We're not saying it's downright dangerous or totally insecure, or that we have a specific reason to distrust the developers. That said, please, please stop telling other activists to use it. It might be OK for a quick fix when you need something more trustworthy than Gmail or Facebook Messenger. But it's not the right choice for your org's long-term communications security.

Before we get into any technical discussion, the straight-up dealbreakers for activists with ProtonMail are:

1. There's no clear way to confirm that you are encrypting messages (only) to the right person.
2. It's a (mostly-)closed system: easy to send private messages inside, but complex or impossible to exchange encrypted emails with people not using ProtonMail. This risks herding diverse movements into a single system for secure comms. Not good, if that system turns out to be not-all-that-secure after all.
3. The ProtonMail developers say ProtonMail is only trying to help businesses or "Private Citizens with Privacy Concerns" avoid totally untargeted, mass surveillance[1] (in other words, they say they only keep you safer than all those other people who may be prey for

the info-hungry bear eagle State). So as an activist who could be targeted for political reasons, you'd have good reason to feel unprotected.

For verifiable, resilient, solidaristic email security, we recommend GPG/OpenPGP[2] (Mozilla Thunderbird+Enigmail plugin[3]) combined with a trusted movement email provider like riseup.net—and if you can, support all of these efforts with money or time. Get in touch[4] if you want a hand getting set up.

And now, the gritty tech details!

ProtonMail claims a number of security[5] and user-experience advantages: end-to-end encryption[6]; the possibility of anonymous accounts[7]; open source[8] (for their client—the app you run—but it's not clear if their server software is all open-source); two-factor authentication; physical and legal protection of their servers (located at CERN, guarded by Swiss privacy laws[9], for whatever that's worth); simple to use encryption (PM manages encryption keys for you); fancy webmail and custom mobile app; no-cost (freemium). However, in constructing such a slick user experience, a lot of disadvantages are created:

- A) Security issues

[1] https://protonmail.com/blog/protonmail-threat-model

[2] https://cldc.org/gpg

[3] *No Trace Project (N.T.P.) note:* As of 2021, the Enigmail plugin is not required anymore, because the PGP functionality it provided has migrated into Thunderbird.

[4] https://cldc.org/about/contact

[5] https://protonmail.com/security-details

[6] https://protonmail.com/blog/what-is-end-to-end-encryption

[7] https://protonmail.com/blog/bitcoin-secure-email

[8] https://protonmail.com/blog/protonmail-open-source

[9] https://protonmail.com/blog/switzerland

1. ProtonMail wants to make strong, end-to-end encryption completely invisible to the user. They do this by managing all encryption keys for you on their server. This means that there is no way to independently confirm (like we recommend you do for Signal[10]) that you are using the authentic[11] keys for your contacts.
2. This is a security weakness because it allows the ProtonMail server (if ProtonMail were so compelled) to send you an alternative key that would encrypt to someone else (an eavesdropper)—this is the same design flaw present in Apple's iMessage[12].
3. The JavaScript that does the encryption is sent to you each time you open a web browser, making it easy for ProtonMail to target an attack against you[13].
4. Even if ProtonMail isn't evil and wouldn't do these things, the ProtonMail server could be compromised by a State or corporate attack (via legal or extra-legal channels) and made to do these things.

- B) Centralized design

1. You can only exchange encrypted messages with other ProtonMail users (locking your community in to ProtonMail)[14].
2. If all political activists jump onto the same email bandwagon it may make that wagon a bigger target for State and Corporate surveillance and/or Neo-Nazi attacks as compared to GPG email encryption, which lets you use your existing email address and spread the target, eliminating a single point of failure for social movements.