Personal Encryption 101

A beginner's guide to protecting your messages, masking online movements, and steering clear of digital snoops

Elizabeth Nolan Brown Digital Edition

This article is part of Reason*'s special Burn After Reading issue, where we offer how-tos, personal stories, and guides for all kinds of activities that can and do happen at the borders of legally permissible behavior. Subscribe Now and get fast first class delivery of the July issue at no extra cost!*

In 2016, a lone Romanian hacker going by the name Guccifer 2.0 claimed credit for the leak of sensitive internal Democratic National Committee emails. But the would-be hacker celeb's story was quickly debunked by a single nonmasked login from a device at the headquarters of the Russian intelligence service, thus turning what looked like a tech security problem into an international spy scandal. That high-stakes slip-up shows just how stringent one must be to get away with online chicanery these days, when one's every login and keystroke can be tracked through an array of digital identifiers.

But you needn't be engaged in espionage, or anything illegal, to benefit from better digital privacy practices. From surveillance-happy state actors and data-harvesting advertisers to popular email clients, social media apps, and other ubiquitous web tools, there are plenty of potential peepers looking to glimpse your digital data (and potentially share it with or sell it to others).

Traditional privacy protection methods—strong passwords and security questions, plus two-step authentication—are your first line of defense. But they may not cut it if convoluted terms of service give sites more leeway with your data than you realize, if hackers breach the servers where companies store your data, or if the authorities decide they want to see the contents of your texts, chats, and inbox.

"Email remains one of the least secure means of communication, and has been likened to sending a postcard—basically anyone along the way who's interested can read the contents of a message," writes journalist Jonas DeMuro in the U.K.'s *TechRadar*. This is because "an email is not a direct communication, but rather goes via several intermediaries…with multiple copies of the message stored at each server, and further copies on both the sender and recipient's computer." *Deleting* something, in other words, doesn't come anywhere close to actually eliminating it.

Email also typically lacks strong protections against access by law enforcement agencies. Under the Electronic Communications Privacy Act, authorities can obtain message content without a warrant after 180 days. (Many providers won't agree to give up your data without a warrant, but they could.)

True online anonymity requires elaborate measures—think a separate device for the anonymous identity, separate phone numbers, use of a virtual private network (VPN) for every login. But most people don't need, or even want, *total* anonymity.

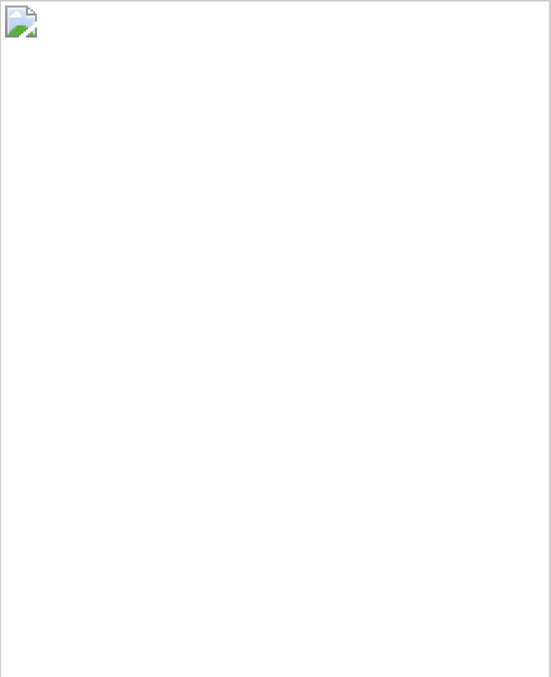
For most of us, privacy can be drastically improved with a few simple (and free) tweaks and tools. In countries like Turkey, where many websites are censored, they can be essential for the most basic online communications. But even in the U.S. and other Western democracies, these services are enjoying a surge in popularity, thanks to sudden skepticism about the data-security practices of social media giants and increasingly invasive government speech codes for the digital sphere. If you too are ready to take back some of your online privacy, this is a guide to getting started.

To Keep Your Email Safe

Encryption, encryption, encryption. Encrypted email services scramble your data so only you and the message recipient(s) can view a readable version. The undecipherable copy is what passes through and gets stored on the email client's servers, so even if they're hacked, subpoenaed, or cursed with nosy employees, your messages can't be read.

The crowd favorite in this arena so far is **ProtonMail**, a Switzerland-based company that says it keeps its primary data center "at a secure facility 1 km under a mountain."

"Because data is encrypted at all steps, the risk of message interception is largely eliminated," the ProtonMail website notes. Emails are first scrambled on the user side, with a key the company can't access—which means even if it wanted to decrypt your mail, it would not have the technical ability to do so. (It also means that if you forget your password, you lose all your previous data.)



Joanna Andreasson

ProtonMail promises not to track user information, including metadata or IP addresses, a numeric designation that identifies a location on the internet; doesn't require personally identifiable information to create an account; and features an optional "self destruct" setting when emailing other ProtonMail addresses that automatically deletes a message from both the sender's and the recipient's accounts after a chosen interval. Basic accounts are free and come with 500 MB of storage. Paid accounts ($48 to $288 per year) offer between 5 GB and 20 GB.

In general, ProtonMail looks and works like regular email. Messages sent between ProtonMail accounts are automatically encrypted during transmission and on both ends. When communicating with a non-ProtonMail user, you must provide a security key if you want the email to be encrypted throughout transmission. Mail recipients will be directed to the ProtonMail site to decrypt the email and reply securely.

Over the past few years, ProtonMail has been rolling out an array of new security features, including encrypted contacts for Android and iOS devices and a service called ProtonMail Bridge, which syncs (paid) ProtonMail accounts with traditional desktop email clients such as Microsoft Outlook.

In addition to all this, the company espouses an old-school anarchic internet attitude that's a welcome contrast to most mainstream email providers. As federal authorities damn encryption as a threat to national security, ProtonMail has pushed back against the idea that only the lawless should embrace anonymous communication tools. "It is incorrect to say that using ProtonMail implies you have 'something to hide,'" said founder Andy Yen in a recent blog post. "ProtonMail provides more security and privacy compared to Gmail or other email services, and security is desirable for practically anyone that uses the internet."

Yen noted that "emails, encrypted or not, can be subject to subpoenas." But at least with services like ProtonMail, "it is not possible to obtain them from the service provider, and instead the subpoena must be served to the individual or organization under investigation."

Another service that gets good marks from privacy types is **Tutanota**, a German company that offers end-to-end encrypted email with 1 GB of storage for free, plus a paid version for those who need more space, multiple addresses, and other features.

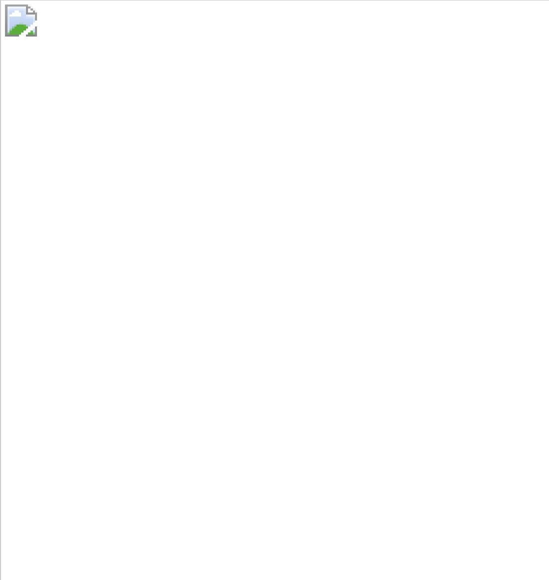
As with ProtonMail, email between Tutanota accounts is always encrypted. Sending encrypted messages to a non-Tutanota account requires setting a password and providing it to the recipient in a separate, nonencrypted email. The recipient will be prompted to visit the Tutanota site and enter the password, and then he or she can read the message.

Like ProtonMail, Tutanota's rhetoric is admirably lofty. Last summer, co-founder Matthias Pfau told *TechCrunch* that "we at Tutanota see ourselves as Freedom Fighters. We believe in human rights such as our right to privacy and freedom of speech. But as these rights are being cut by governments around world, we need to fight back."

Belgium-based **Mailfence** operates much like ProtonMail and Tutanota. Its more robust accounts can be paid for using bitcoin. **Disroot** offers encrypted email as well as cloud storage and a host of other services, including a message board, a Twitter-like social media platform called Diaspora, and a browser-based text editor that can be set to "burn after reading," leaving no trace of the decrypted document on either the author or the reader end. The all-volunteer, Amsterdam-based team says it aims to create digital tools that are "open, decentralized, federated, and respectful towards freedom and privacy."

To Chat, Send Photos, or Make Calls Securely

Encryption is also the answer for protecting the secrecy of your more casual communications. There are several popular services right now that allow for the easy exchange of encrypted chat—consider this your alternative to both texting and the likes of Gchat, Facebook Messenger, and similar direct-messaging services—as well as offering ways to make calls and privately exchange photos or videos. The only catch is that your contacts are limited to those who are also using a particular service or app.



Joanna Andreasson

Which one you choose—**Signal**, **WhatsApp**, and **Telegram** are the three most popular—should depend on where you live, which apps are in use among your social and professional networks, how much security you're willing to exchange for other positive attributes, and how much faith you put in proprietary data systems. Your individual privacy concerns come into play as well: Is it government or service-provider snooping that concerns you? Are you trying to prevent people in your household from reading your texts? Do you need to be able to verify the identity of those you're messaging with? Do you mind giving out your phone number?

Telegram is not built on open-source software—a major strike against it, according to some privacy hawks—and the use of a proprietary encryption process is another potential black mark. The London-based service has also run into trouble in such countries as Iran and Russia, where authorities have demanded Telegram turn over info that would let them decrypt all user emails—Telegram declined—or moved to block the service altogether. But it has around 200 million active users per month and boasts large user bases in former Soviet Union countries and the Middle East, which can make it attractive for people with a lot of contacts there. And founder Pavel Durov at least pays lip service to the privacy-minded ethos that ProtonMail and Tutanota tout. "We don't regard Telegram as an organization or an app," he wrote in a March blog post. "For us, Telegram is an idea; it is the idea that everyone on this planet has a right to be free."

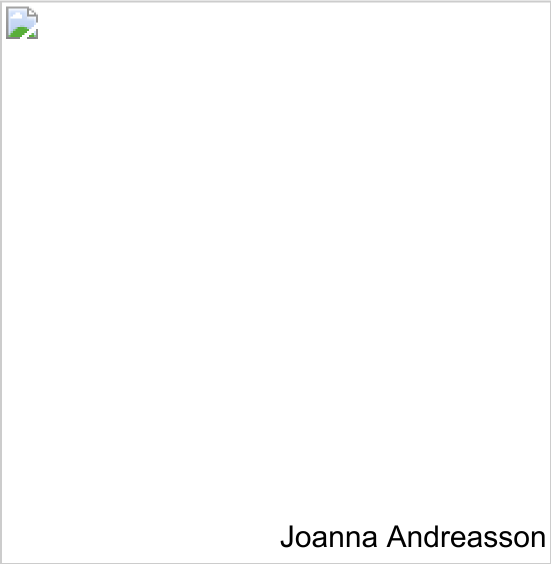
Privacy clearinghouse PrivacyTools.io recommends against both Telegram and WhatsApp, a similar (and even more popular) chat platform. In general, the biggest complaint about the latter is that it collects user metadata—and that its parent company is Facebook.

The Electronic Frontier Foundation (EFF) has said on its blog that if pressed, it would recommend either WhatsApp or Signal, though it notes that it's difficult to "make a recommendation without considering the details of a particular person's or group's situation."

Overall, Signal gets the best ratings from the widest array of groups and people, especially if you're looking for strong security. Both Signal and WhatsApp "employ the well-regarded Signal protocol for end-to-end encryption," EFF noted, but "Signal stands out for collecting minimal metadata on users, meaning it has little to nothing to hand over if law enforcement requests user information. WhatsApp's strength is that it is easy to use, making secure messaging more accessible for people of varying skill levels and interests."

To Browse the Internet Anonymously

Most browsers now offer an "incognito" or "private browsing" mode that doesn't log your search or site-visiting history. But these functions only mask your trail locally (i.e., the pages you visit in an incognito window won't show up when you check your browser history). They don't mask your IP address or hide your identity from sites you visit.


Joanna Andreasson

No one app or fix will let you browse online totally anonymously, but the most simple and comprehensive option is to download the **Tor** browser. Tor—which works on Windows, Mac, Linux, iOS, and Android—is an open-source, modified version of the Mozilla Firefox browser that comes pre-installed with all sorts of privacy features. The bottom line is that it can keep your computer's address from being logged by websites.

"The Tor network is a group of volunteer-operated servers [that] employ this network by connecting through a series of virtual tunnels rather than making a direct connection," the Tor website explains.

This lets people "share information over public networks without compromising their privacy" and serves as "an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content."

To supplement Tor, savvy web surfers may want to use a virtual private network (VPN). Normal browsers let your internet service provider (ISP) see every site you visit, in addition to your computer's personal IP address being visible to the sites themselves. VPNs prevent this by filtering your traffic through their network and serving it up with a new, masked IP address.

This means that your ISP records you going to the VPN but not to the sites you visit thereafter. In addition, the sites you visit see the IP assigned to you by the VPN, not your actual information. This can be especially useful for getting around geography-based content filters, like China's ban on many American sites and apps (often referred to as the "Great Firewall") and Russia's ban on everything from Telegram to, temporarily, Google.

The VPN also encrypts your traffic, so it's not accessible the way your browser history on a normal browser would be. Using a VPN is similar to using web proxy servers, which serve as a screen between your computer and your internet activity, except that VPNs also mask your identity when interacting online with games, torrent apps, and the like.

A word of caution: A VPN alone will not keep your emails safe if you're using a traditional email client. It will mask you from your ISP, but unencrypted copies of your messages will still be stored on email client servers.

VPN clients can be downloaded for use on computers, tablets, and smartphones. Some free VPNs that get consistently good reviews are CyberGhost, TunnelBear, and Windscribe. PrivacyTools.io also has put out a list of recommended VPNs, all of which are based outside the U.S., use encryption, and accept bitcoin. **ProtonVPN** (associated with ProtonMail) is the only one of the most highly rated services that's also free; the others range from around $35 to $125 per year.

Regular browsers *can* be configured to offer more privacy through the use of various plugins. PrivacyTools.io offers recommendations on that score as well. Of the most well-known browser options, **Mozilla Firefox** and **Brave**, from former Mozilla CEO Brendan Eich, are arguably strongest when it comes to security.

To Keep Your Search History Secret

When using typical search engines like Google, Yahoo, and Bing!, clearing your search history from your browser window doesn't mean it's actually gone forever. Your search log is stored by the search-engine company in question. To search without leaving a trail, try **DuckDuckGo**, which doesn't track any user data, or **StartPage.com**, which lets you use Google's search engine without being tracked by the tech giant.

To Make Your Go-To Tools More Secure

Gmail offers email encryption under some circumstances—if a user is on a Chrome browser or using a Gmail app and is emailing another Gmail address. But as *TechRadar* notes, "Google has become the Big Brother of the internet, and is known for reading user's messages, all in the name of targeting them with more relevant ads; there's privacy, and there's Google's idea of privacy."

Microsoft Outlook also has an encryption option, but it only works in limited instances.

If you're using a desktop email client, you may be able to use **ProtonMail Bridge** to add a layer of protection. The service integrates with Outlook, Apple Mail, Thunderbird, and similar options, serving as "a bridge between the unencrypted and encrypted worlds in the sense that it allows your average user to benefit from the added security and privacy of end-to-end encryption without having to make any changes to their email usage behavior," ProtonMail's Yen explained in a statement.

To Manage All Your Passwords

The best encryption plans in the world don't mean anything if you forget your passwords or if your passwords aren't secure. Consider ditching options such as iCloud Keychain, 1Password, and LastPass in favor of **KeePass**, a free, open-source password manager with strong encryption game.

Don't forget to check out the rest of Reason's *Burn After Reading content*.

Photo Credit: Joanna Andreasson. KrulUA/istock

Elizabeth Nolan Brown is an associate editor at *Reason* magazine.