How to Create an Anonymous Email Account

BY ERIC GRIFFITH (/AUTHOR-BIO/ERIC-GRIFFITH) JANUARY 20, 2017 0 COMMENTS

The Internet doesn't make it easy to go completely anonymous. Here's how you can stay hidden even when emailing.

Not long ago, the sharing economy seemed to take over. Privacy was dead, and no one cared. But that was a **pre-Snowden era (http://www.pcmag.com/article2/0,2817,2453128,00.asp)**. Now, for some, the need to go truly anonymous is more important than ever.

(http://securitywatch.pcmag.com/) But when you go to a service online and its first three choices for signup are to use existing Google, Facebook, or Twitter account credentials, it's almost like a subtle background check. Other services—like Google—expect you to share a phone number or an older email address to sign up, so you're not exactly hiding your tracks.

What do you do if you want to set up an email address that is completely secret and nameless, with no obvious connection to you whatsoever without the the hassle of setting up your own servers?

This goes beyond just encrypting messages. Anyone can do that with Web-based email like Gmail by using a browser extension like **Secure Mail by Streak (https://www.streak.com/securegmail)**. For desktop email clients, **GnuPG (https://www.gnupg.org/)** (Privacy Guard) or **EnigMail (https://www.enigmail.net/home/index.php)** is a must. Web-based **ProtonMail (https://protonmail.com/security-details)** promises end-to-end encryption with zero access to the data by the company behind it, plus it has apps for iOS and Android.

But those don't hide who sent the message.

Here are the services you should use to create that truly nameless, unidentifiable email address. But be sure to use your powers for good.

First Step: Browse Anonymously

Your Web browser is tracking you. It's that simple. Cookies, and so-called **unstoppable "super cookies" (http://www.pcmag.com/article2/0,2817,2476078,00.asp)** know where you've been and what you've done and they're willing to share. Sure, it's mostly about making sure you see targeted ads, but that's not much consolation for those looking to surf in private.

Your browser's incognito/private mode can only do so much—sites are still going to record your IP address, for example.

If you want to browse the Web anonymously (and use that private time to set up an email), you need not only a **virtual private network (http://www.pcmag.com/article2/0,2817,2403388,00.asp)**, but also the **Tor Browser (https://www.torproject.org/projects/torbrowser.html.en)**, a security-laden, Mozilla-based browser from the Tor Project. If you don't know about Tor, it's what used to be called The Onion Router; it's all about keeping you anonymous by making all the traffic you send on the Internet jump through so many servers, people on the other end can't begin to know where you really are. It'll take longer to load a website than it would with Firefox or Chrome, but that's the price of vigilance.

The **Tor Browser (http://www.pcmag.com/article2/0,2817,2498303,00.asp)** is available in 16 languages, for Windows, macOS, and Linux. It's self-contained and portable, meaning it'll run off a USB flash drive if you don't want to install it directly. It's totally free. Even Facebook has a **Tor-secure address (https://www.facebookcorewwwi.onion/)** to protect the location of users—and let users get access in places where the social network is illegal or blocked, like China. An **estimated 1 million people (http://www.pcmag.com/news/343969/facebook-now-has-more-than-one-million-visitors-from-tor)** use it. There is also a version for getting **Tor access to Facebook on Android (http://www.pcmag.com/article2/0,2817,2498148,00.asp)** devices.

Tor is not perfect and won't keep you 1,000 percent anonymous. The criminals behind the Silk Road, among others, tried that **and failed (http://www.reuters.com/article/2015/02/04/us-usa-bitcoin-trial-idUSKBN0L82H920150204)**. But it's a lot more secure than openly surfing. It took **law enforcement agencies with a lot of resources (http://gizmodo.com/tor-is-still-safe-1669011966)** to get those bad guys.

Second Step: Anonymous Email

You can set up a relatively anonymous Gmail account, you just have to lie like a bathroom rug. That means creating a full Google account, but not providing Google your real name, location, birthday, or anything else it can use when you sign up (while using a VPN and the Tor Browser, naturally).

You will eventually have to provide Google some other identifying method of contact, such as a third-party email address or a phone number. With a phone, you could **use a burner/temp number (http://www.pcmag.com/article2/0,2817,2497669,00.asp)**; use an app like **Hushed (http://hushed.com/)** or **Burner (http://www.pcmag.com/article2/0,2817,2408578,00.asp)** or buy a pre-paid cell phone and lie through your teeth when asked for any personal info. (Just know that **even the most "secure" burner has its limits (http://www.b3rn3d.com/blog/2014/01/22/burnerphone/)** when it comes to keeping you truly anonymous.)

As for that third-party email, there are anonymous email services you can use, so why use Gmail at all? The **Electronic Frontier Foundation (https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts)** (EFF) says it's smart to use a different email provider from your personal account if you crave anonymity—that way you're less likely to get complacent and make a compromising mistake.

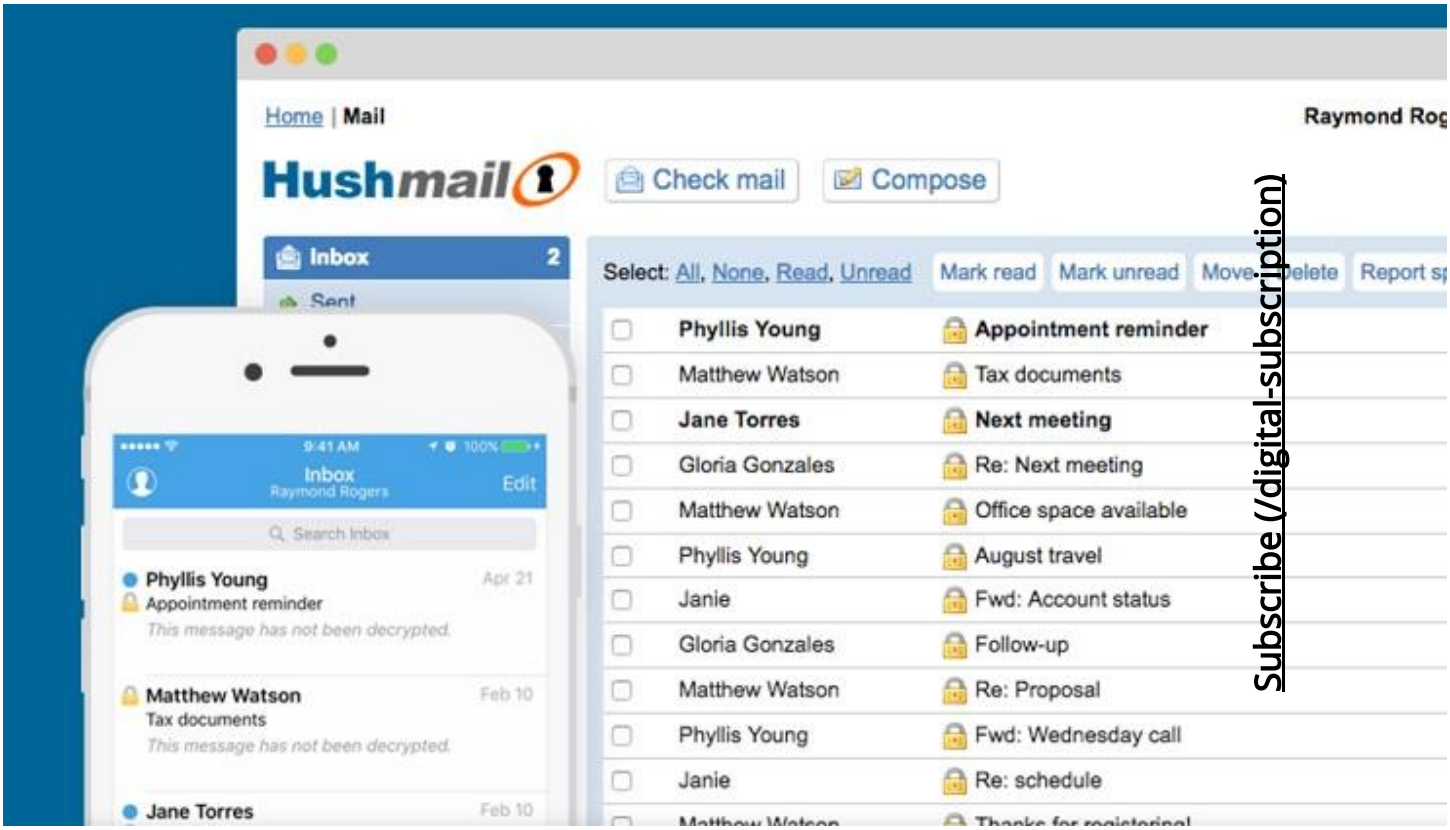
Note that you also should use an email service that supports secure sockets layer (SSL) encryption. That's the basic encryption used on a Web connection to prevent casual snooping, like when you're shopping at Amazon. You'll know it's encrypted when you see HTTPS in the URL, instead of just HTTP. Or a lock symbol shows up on the address bar or status bar. The big three webmail providers (Gmail, Yahoo Mail, and Outlook.com) all support HTTPS. Get the **HTTPS Everywhere extension (https://www.eff.org/https-everywhere)** for Firefox, Chrome, Opera, and on Android, to ensure that websites default to using the protocol.

That's great for Web surfing, but neither HTTPS nor VPN is enough to stay hidden when emailing. You know that.

Pseudonyms in email (like anonguy55@gmail.com) aren't enough, either. Just one login without using Tor means your real IP address is recorded. That's enough for you to be found (if the finder can get your provider to give up some records). It's how General Petraeus got nailed.

The point is, once you've gone this far, there's no reason to go back. Use a truly anonymous Web-based mail service; here are some of the best.

Hushmail



Recommended by the EFF and others, **Hushmail's (https://www.hushmail.com/)** entire claim to fame is that it's easy to use, doesn't include advertising, and has built-in encryption between members. Of course, to get all that, you have to pay for it, starting at $49.98 per year for 10GB of online storage; a **free version (https://www.hushmail.com/signup/?source=website&sp=true&tag=page_personal,btn_free)** offers 25MB of storage. Access it on the Web or **iOS (https://www.hushmail.com/ios/)**.

Businesses can use Hushmail starting at $3.99 per user/month for nonprofits (going up to $5.99 for small businesses and $9.99 for legal and healthcare entities), plus a one-time $9.99 fee setup fee for everyone (though then you need to obfuscate your info for the Whois database).

Note that Hushmail has **turned over records to the feds before (http://www.wired.com/2007/11/encrypted-e-mai/)**, and its terms of service state you can't use it for "illegal activity," so it's not going to fight court orders. But at least it's honest about it up front.

Hide My Ass! Anonymous Email

Hide My Ass (https://www.hidemyass.com/) is a well-liked private VPN service that makes it a breeze for users to access content blocked at their location, not to mention providing a much higher level of privacy (hence the name). Base price is $11.52 a month, but you only pay $8.33/month if you commit to six months or $6.55 per month for a year.

HMA's **Anonymous Email (https://securemail.hidemyass.com/)** service is not just for VPN customers. You get an address @hmamail.com that can be set to last 24 hours, one week, one month, six months, or 12 months. There's a countdown clock to indicate just how long you have left when reading messages. At signup, it does ask for your existing email address, so HMA can send it a note when you get a message on the anonymous account, but it's not required. The interface won't win any awards—Hushmail's is infinitely nicer—but it gets the job done. Note that this is for receiving only; you can't send a message out.

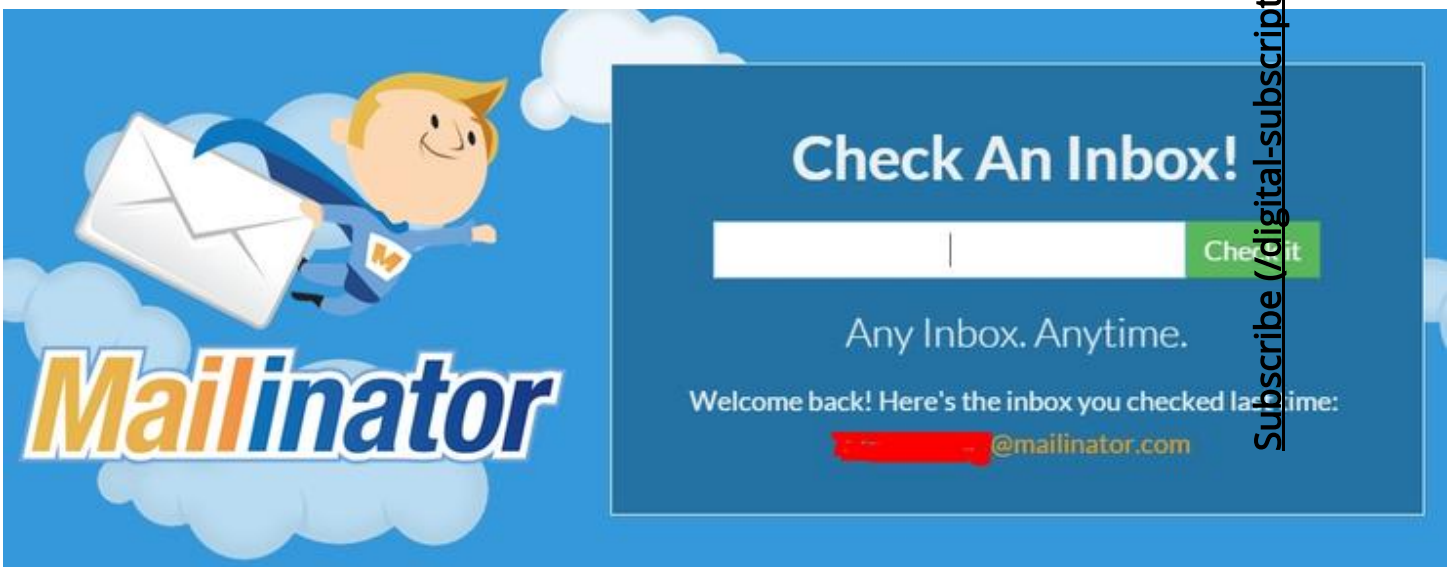
HMA also has **iOS (https://itunes.apple.com/us/app/vpn-hide-my-ass-pro-wifi-security/id675102189?mt=8)** and **Android (https://play.google.com/store/apps/details?id=com.hidemyass.hidemyassprovpn&hl)** apps that provide secure mobile connections, plus privatized SMS texts and chat services with other HMA users.

Guerrilla Mail

Guerrilla Mail (https://www.guerrillamail.com/) provides disposable, temporary email. Technically, the address will exist forever, and never be used again. Any messages received at the address, accessible at guerrillamail.com, only last one hour. You get a totally scrambled email address that's easily copied to the clipboard. There's an option to use your own domain name as well, but that's probably not keeping you under the radar.

Guerrilla Mail is the perfect way to create an email address to sign up for a different, more permanent-yet-anonymous email address, or to send a quick, anonymous email instantly—no signup required. You can even attach a file if it's less than 150MB in size, or use it to send someone your excess bitcoins. Coupled with the Tor browser, Guerilla Mail makes you practically invisible. It's also available on **Android (https://play.google.com/store/apps/details?id=com.guerrillamail.app)**.

Mailinator



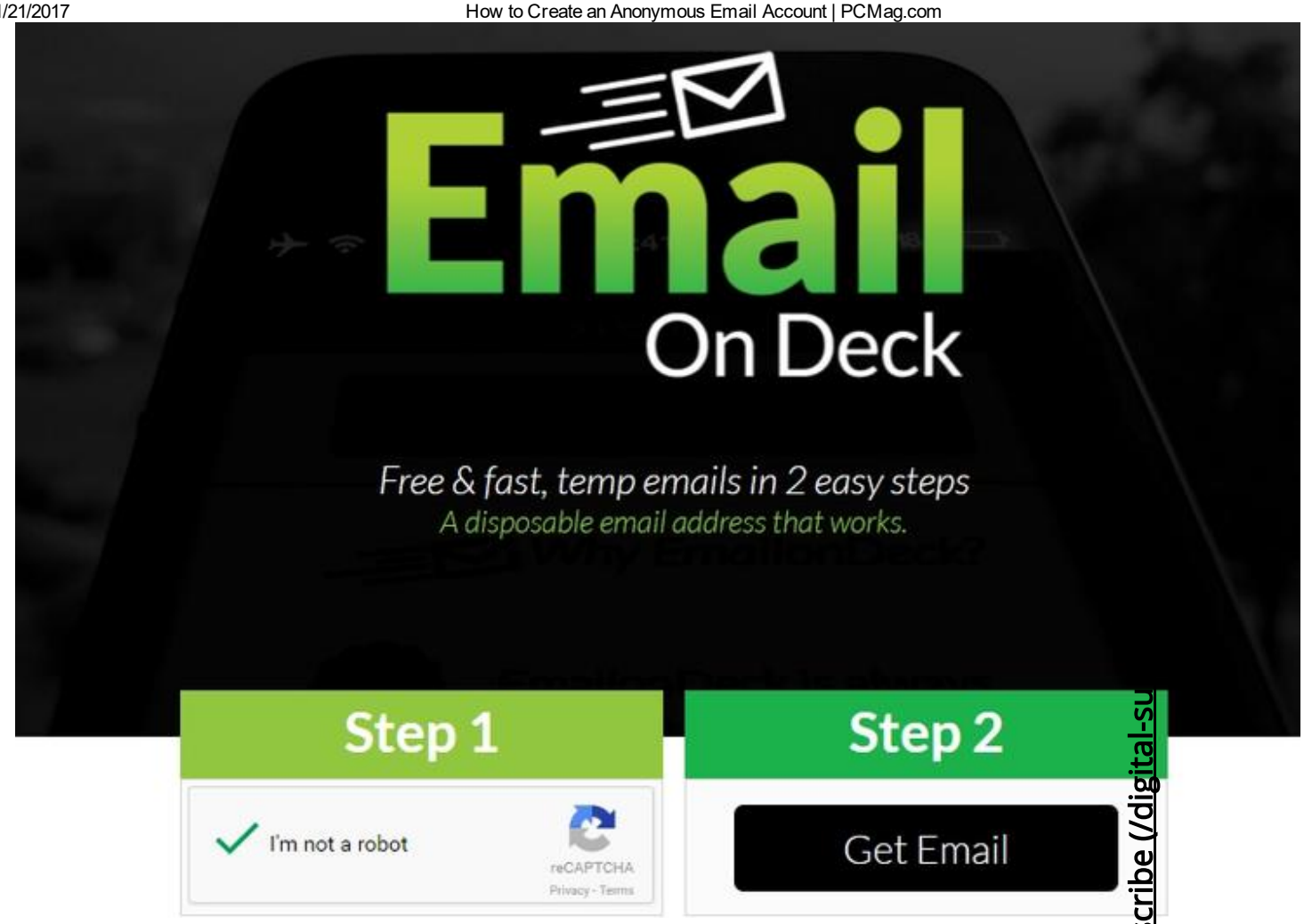
Mailinator's (https://mailinator.com/) free, disposable email has a slick interface, but you probably don't even need it. Whenever you're asked for an email, just make up a name and stick @mailinator.com at the end. Then visit the site, enter the name, and you'll see if it's received any messages. No signup required, though you can sign in with a Google account.

Here's the problem. If someone else comes up with the same name, then you both get access to the messages received. There are no passwords. There's also no sending possible. Its FAQ states if you get an email *from* Mailinator, it's a guaranteed forgery. This one is for quick service signups only, and only with the most obfuscated, obscure name you can come up with. Of course, you can pay $29/month if you want to get a 10MB storage inbox that is private just for you.

Hide-Your-Email.com

You don't get **interfaces as simple (http://hide-your-email.com/)** as this very often is. With no signup required, you enter the email name you want for an @pidmail.com address you can hand out. The messages sent to it immediately show up. It's that simple, though it's not for sending messages. You can reserve the address of your choice with a password, again at no cost to you.

Email On Dek



There's a two-step process to getting a free email for receiving messages at **Email On Deck (https://www.emailondeck.com/)**, but only because step one is a CAPTCHA to make sure you're a human being, not a Web-based robot. It randomly assigns you an obfuscated email address (like "cynthia@l7b2l48k.com"). You can click a button to get assigned another, but they're all temporary. You don't want to use this service if you plan to ever use the address assigned beyond, say, an hour or two.

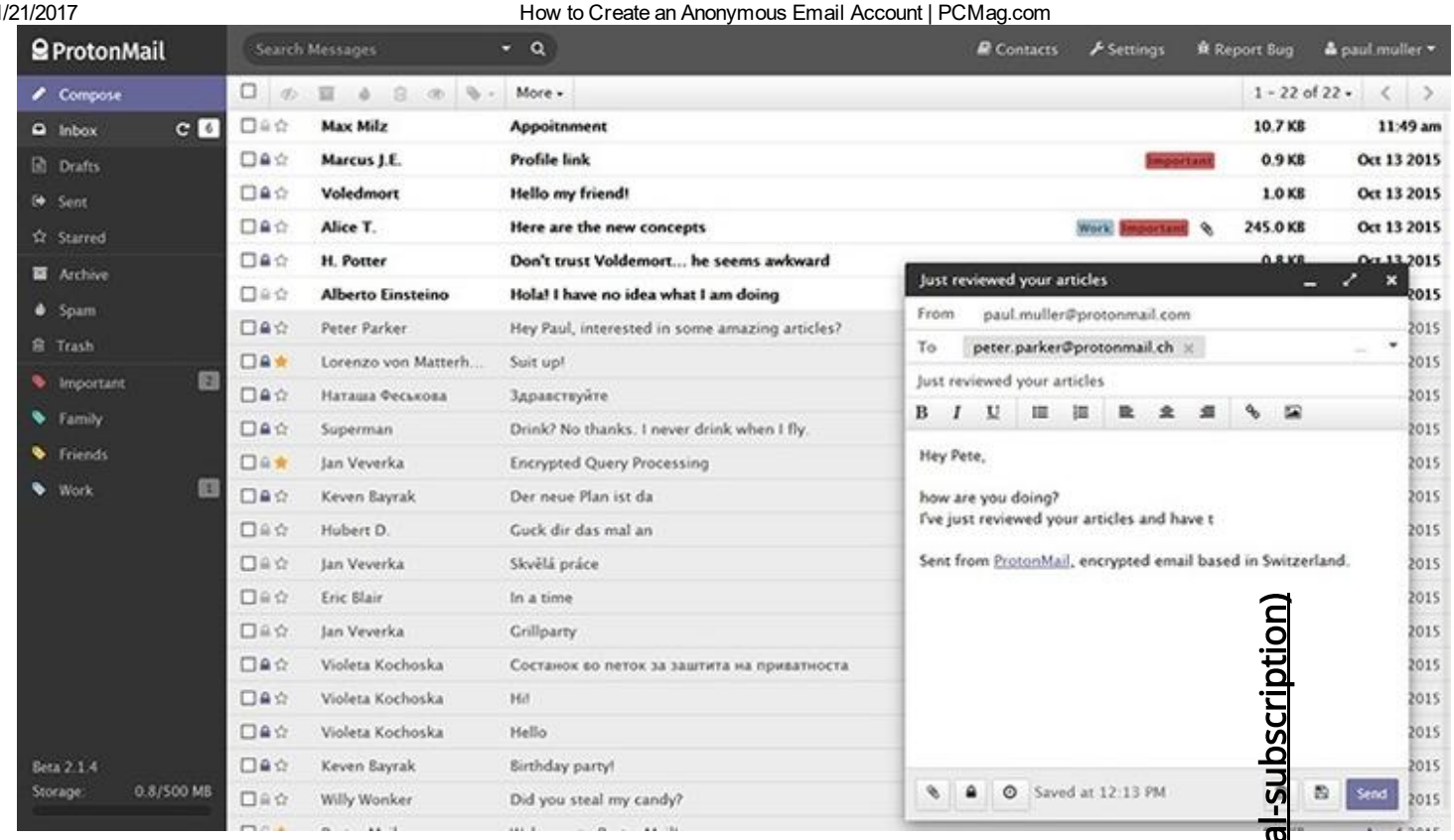
TorGuard Email

TorGuard (https://torguard.net/anonymoustorrentvpn.php) is another global VPN service, which goes for around $9.95/month to start. The service also provides a separate **Anonymous Email (https://torguard.net/anonymous-email.php)**, with service from free (10MB offshore storage) all the way up to $49.95/year service with unlimited storage. They all have secure G/PGP encryption of mail and no ads. For more, see **PCMag's full review (http://www.pcmag.com/article2/0,2817,2479420,00.asp)**.

TrashMail.com

TrashMail.com (https://trashmail.com/) isn't just a site, but also a **browser extension for Google Chrome (https://chrome.google.com/webstore/detail/trashmailcom-create-dispo/fihbdpohplcdnhllhliaeapefmmpcdjo?utm_source=chrome-ntp-icon)** and **Firefox (https://addons.mozilla.org/en-US/firefox/addon/trashmailnet/)**, so you don't even have to visit the site. Create a new email from a number of domain options, and TrashMail.com will forward it to your regular address for the lifespan of the new address, as determined by you. The only limit is how many forwards you can get; to go unlimited, you **pay $12.99 a year (https://trashmail.com/?cmd=register&lang=en)**. The site provides a full address manager interface so create as many addresses as you like to stay anonymous and ubiquitous.

ProtonMail over Tor



Maybe saving the best for last: **ProtonMail (https://protonmail.com/signup)** is a nice service with servers in Switzerland (a country that appreciates secrecy) that provides fully encrypted messages. Anyone can get an account for free that holds 500MB of data and up to 150 messages per day, or pay 4 euros per month to get the advanced features. Encryption is one thing, but anonymity comes with the ProtonMail's specific support for Tor via an onion site it sets up at **protonirockerxow.com (https://protonirockerxow.com)**. It also provides full instructions on how to set up Tor on your desktop or mobile phone. Having anonymous users is so important to ProtonMail, it doesn't require any personal info when you sign up. It even supports **two-factor authentication (http://www.pcmag.com/article2/0,2817,2456400,00.asp)**.

BACK TO TOP

PREVIOUS : *Living in Glass Houses* (http://www.pcmag.com/article/350563/living-in-glass-houses)

BY ERIC GRIFFITH (/AUTHOR-BIO/ERIC-GRIFFITH)
(/author-bio/eric-griffith) **FEATURES EDITOR**
(HTTP://TWITTER.COM/ERICGRIFFITH) (MAILTO:ERIC_GRIFFITH@PCMAG.COM)

Eric narrowly averted a career in food service when he began in tech publishing at Ziff-Davis over 20 years ago. He was on the founding staff of Windows Sources, FamilyPC, and Access Internet Magazine (all defunct, and it's not his fault). He's the author of two novels, BETA TEST ("an unusually lighthearted apocalyptic tale"--Publishers' Weekly) and KALI: THE GHOSTING OF SEPULCHER BAY. He works from his home in Ithaca, NY. **MORE » (/AUTHOR-BIO/ERIC-GRIFFITH)**