



Beat the FBI: How to Send Anonymous Email Without Getting Caught

by Ben Weitzenkorn - November 16 2012

Ahhh, the anonymizing effects of the Internet. From where you sit, I'm little more than a byline and a couple of hundred black words on a white field. It's a fact, or fiction, that gives many Internetusers solace.

But as some people have recently learned in very real and damaging ways, online anonymity is not a guarantee.

Just ask Violentacrez, the Reddit moderator who posted and hosted risqué pictures of women taken without their consent, and whose name was exposed as Michael Brutsch.

Ask CIA Director Gen. David Petraeus and his biographer Paula Broadwell, who used the tried-and-failed technique of leaving communiqués in the draft folders of email accounts.

Ask the members of the hacktivist movement Anonymous, whose leaders have beenouted, arrested and convicted due to their supposedly untraceable online activities.

If anything, the Internet has made the world a less anonymous place. There are more details about more people available from more places than there have ever been. And we all throw it up there willingly.

But that doesn't mean anonymity is impossible. In fact, sometimes it's necessary.

There are lots of reasons someone may wish to send emails anonymously — to disclose sensitive information, report illegal activity, blow the whistle, carry out an extramarital affair or simply annoy others.

Some of these reasons, no doubt, are better than others, but we're trying not to judge.

Is it possible to communicate with others online with absolute certainty that messages won't ever be traced back to you?

The short answer is "no." But the long answer is "sort of," and is much more interesting. It may be the reason you found this page to begin with.

"Security is a function of the resources your adversary is willing to commit," said Julian Sanchez, a policy expert with the Cato Institute in Washington, D.C.

"If you've been flagged as a high-priority target by the NSA [National Security Agency] and are under active observation," Sanchez said, "then no, you can probably never have 'total confidence' that your communications won't be traced."

But for the rest of us, it's definitely a possibility. With the right tools, some vigilance and a little bit of Web savvy, you, too, can best General Petraeus, Hamas, al-Qaida and the Taliban with communiqués so virtually untraceable that they would make James Bond blush.

Biting into the onion

Anytime you want to do something anonymously on the Web, begin by anonymizing your IP address. Begin by trying Tor.

Tor, short for "The Onion Router," is a free system of software and servers scattered around the world that enables anonymous Internet traffic via a decentralized, encrypted peer-to-peer relay process, in which each user is also a relay point.

"Each Tor packet is actually wrapped in layers of encryption, like an onion," Sanchez explained. "So each node in the relay knows where the packet has just come from and where it's going next, but not the ultimate origin or destination."

That makes traffic over the Tor network not only difficult to trace, but also eliminates any third-party culpability.

"The brilliant thing about Tor is that there isn't really anyone to subpoena," Sanchez said. "There isn't any central hub you could go to with a court order and demand they turn over information."

That's the case with your Internet service provider as well. Since Internet traffic hits the Tor proxy client before it goes anywhere else, an ISP would see nothing but the entry-point Internet Protocol address, or the outermost layer of the onion.

Everything you do beyond that is your business and yours alone.

Tor can be accessed through a special Tor browser that's based on Firefox.

This email address will self-destruct in...

Well, almost. Now that your Internet traffic has been anonymized, the hard part is over.

Whatever you do, though, don't log into your primary Gmail or work account. It likely has your name all over it.


That renders Tor useless and, depending on the nature of your messages, will lead to your embarrassment, termination, arrest or worse.

Instead, create a "burner" email account to use over Tor. Depending on what you're doing and how long you plan on doing it for, several services may fit your needs.

AnonEmail is a great service that further obfuscates a message's source by relaying the message several times before it reaches its destination. Some users have reported that the service does not appear to log IP addresses.

AnonEmail will work without Tor, as will many other "anonymizing" email services, but when anonymity is the most important factor, it's best to leave nothing to chance.

AnonEmail's drawback is its lack of support for attachments. So if you're leaking a PDF or sending sexy images, this service isn't for you.

Luckily, there's Amnesty Box, a very similar service that anonymizes messages by placing them on its secure server  and then sending them from a no-reply email address.

If, on the other hand, you need to anonymously send an email, 10 Minute Mail is the most secure. From the moment users point their browser at the page, they have 10 minutes to use their disposable account.

Whether you want to troll, harass, report or disclose, you'd better do it quickly. Once the clock runs out, the entire account implodes, taking correspondence histories into the void with it, along with anything else you would never want anyone to know.

Best of all, visitors to the page are greeted with a preset, random seven-digit string of numbers and letters, such as a169734@rmqkr.net, taking the creative work out of the equation. It's an email address meant to be forgotten.

Not out of the woods yet

Even after you've done all this, your anonymity still isn't a certainty.

"If, for example, [Paula] Broadwell had repeatedly used a Tor connection to access her anonymous account, and then logged into her primary Gmail account or Facebook within the same few minutes," Sanchez said, "there's a fair chance she still could have been traced, or at least been placed on a short list of suspects."

"Tor's not enough," Sanchez added. "You have to be smart about other aspects of your use of it."

At the end of the day, common sense always wins. Are you one of only a few people who have the information you're leaking? Chances are no matter how many proxies or how much encryption you use, you'll be found out.

This guide and the tools outlined in it are just that: tools. How you use them is up to you, and as with other tools, different skills and experience levels will yield different results.