

Forum:[Hack Forums](#)

Thread: [\[TUT\]9 steps to make you completely anonymous online](#)

Hastur - June 13, 2016, 12:50 pm

1. Find a safe country

First, you would have to be physically located in a country that doesn't try its hardest to spy on you. That's a tall order. Almost any country with any type of cyber awareness and talent is spying on its citizens "for their own protection." Your best option is to find a country with good Internet connectivity that doesn't have enough resources to monitor everything its citizens are doing.

2. Get an anonymizing operating system

Next, you'll need an anonymizing operating system that runs on a resettable virtual machine running on secure portable media. The portable media device should use hardware-based encryption or a secure software-based encryption program. One of the top products on that list is Ironkey Workspace. It offers good encryption, locks out users who enter too many bad passwords, and comes with Microsoft's portable OS, Windows to Go, on several USB key models.

Many privacy advocates prefer a Linux Live distro, such as Tails or ZeusGuard. Live OSes are designed to be booted from removable media for each session, and Tails is one of the best, built for and focused on privacy and security. The NSA has stated in an internal, leaked presentation that Tails and Live OSes like it are a threat to its eavesdropping mission. That's a ringing endorsement.

Whether or not you use a Live OS, make sure the OS doesn't store information that can be used against you. If you're not using read-only, bootable media, consider using a VM solution that resets itself after every use. Better yet, do both. Use a Live OS stored in a VM. Let the VM assign random DHCP and ARP addresses on every start.

3. Connect anonymously

Next, you'll need to connect to the Internet using an anonymous method. The best approach would probably be to jump around random, different, open wireless networks, public or otherwise, as much as possible, rarely repeating at the same connection point. Barring that method, you would probably want to use a device built for anonymous wireless connections, like ProxyGambit. I'll let ProxyGambit describe itself:

ProxyGambit is a simple anonymization device that allows you to access the Internet from anywhere in the world without revealing your true location or IP, fracturing your traffic from the Internet/IP through either a long distance radio link or a reverse tunneled GSM bridge that ultimately drops back onto the Internet and exits through a wireless network you're no where near. While a point to point link is possible, the reverse GSM bridge allows you to proxy from thousands of miles away with nothing other than a computer and Internet with no direct link back to your originating machine.

4. Use Tor

Whatever Live OS and Internet connection method you use, make sure to go with an anonymizing browser, such as a Tor-enabled browser. Tor is actually an entire system -- tools, browsers, APIs,

and network -- dedicated to helping you and your connection remain anonymous.

Once you enter a Tor network path, the traffic to and from your destination will be routed through a random set of "Tor nodes." Although Tor's anonymity can be defeated, it remains one of the best ways to stay anonymous when combined with these other recommendations. You can even buy hardware-based Tor solutions like Anonabox.

5. Don't use plug-ins

It's very important to remember that many of today's browser plug-ins, particularly the most popular ones, leave clues that reveal your identity and location. Don't use them if you want to preserve your anonymity.

6. Stick with HTTP/S

Don't use any protocols other than HTTP or HTTPS. Typically, other protocols advertise your identity or location. When working with HTTPS, use only handpicked, trusted certification authorities that don't issue "fake" identity certificates.

7. Avoid the usual applications

Don't install or use normal productivity software, like word processors or spreadsheets. They, too, will often "dial home" each time they're started and reveal information.

8. Set up burner accounts

You'll need a different email address, password, password question answers, and identity information for each website if you take the risk of creating logon accounts. This particular solution is not only for privacy nuts and should already be practiced by everyone already.

9. Never use credit cards

If you plan to buy anything on the Internet, you can't use a normal credit card and stay anonymous. You can try to use online money transfer services such as PayPal, but most have records that can be stolen or subpoenaed. Better, use an e-currency such as bitcoin or one of its competitors. You'll need a bank or service to convert your real money into one of these alternative forms (and to get it back out), but once you're using the currency, buying anonymity is easier to maintain.

The hard work of privacy

Each of these anonymizing methods can be defeated, but the more of them you add to your privacy solution, the harder it will be for another person or group to identify you. There are hundreds of thousands, if not millions, of privacy advocates that take one or more of these precautions to protect their privacy.

Of course, most people aren't looking for the best privacy possible. Everything you do to protect your privacy causes inconvenience in your online life. Serious privacy advocates don't mind going to this trouble, but most of us aren't willing to do what it takes to accomplish even a modicum of privacy, such as configuring settings in our OS or on social media sites. Most people simply accept the defaults -- which rarely protect privacy.

I found all those steps on a [website](#) and I decided to share this usefull information here.

Kind Regards ?

Tadus - *June 13, 2016, 12:51 pm*

Thanks for the tutorial man!

Drakeav - *June 13, 2016, 12:54 pm*

I found this very usefull man, keep up the good work. =)

ACuriousNoob - *June 13, 2016, 8:05 pm*

Very interesting, some stuff here I haven't seen before(Not that I've seen a lot, but still).

That proxygambit thing sounds cool.

Anti Democratic - *June 14, 2016, 7:00 pm*

Seen some of these methods before, but always great to learn a new thing or two, thanks for this helpful thread.