How To Disappear Online And Fly Under The Radar

There was a time when you didn’t have to look over your shoulder to see if you’re watched. Privacy was as normal and real as paying the bills at the bank, or buying milk from the grocery. Those days are gone. You don’t need to go to the grocery to buy milk or enter the bank for paying the bills. Thanks to internet, they are just one click away.

But even if you can’t see anybody standing right behind you, you know they are there, watching every page you visit, every payment you make, and following your traces through the virtual world. Then they could easily steal your data, empty your card, build your profile and scan your everything till you have nothing private left.

Are you ready to face these scammers and protect your right to privacy? Here’s what you need to know!

This is why conventional survival defense won’t work!

To make it short, there are four things you should keep in mind about going under the radar on internet. Keep reading the article to see what’s to be said about each of them.

- Privacy isn’t typically compromised due to poor SOP, it is typically compromised by human error, complacency, short cuts and failure to adhere to SOP.
- Compartment identities, devices and where you use them. Have separate devices for each identity and use them at different locations.
- Emails, credit cards, phone numbers and even addresses can all be masked at low cost by services such as Blur.
- Tails is an OS that enables you to use TOR to access the

internet, and send encrypted email and text messages from virtually any computer or phone by connecting a multiport USB flash drive, leaving no trace that you were there.

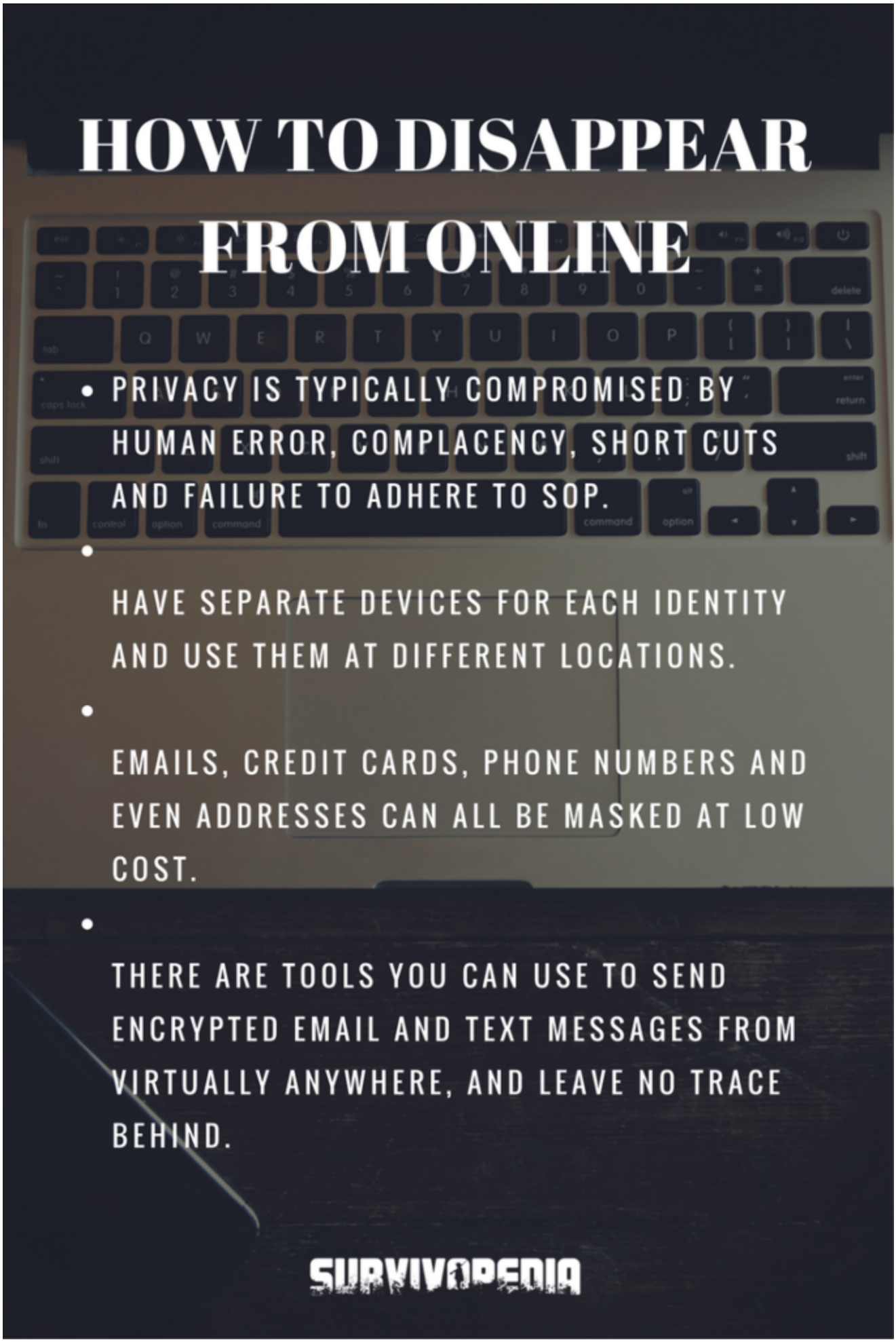
Manage Your Expectations

For most, compartmenting identities mitigates the need to disappear completely, even online. If your needs go beyond compartmenting identities, you will need to learn more than it is possible to teach you in an article, even just to disappear online, but I will touch on the more general aspects of this undertaking.

Make sure your expectations are realistic. Even if you opt out of programs, scour the internet and are successful in getting everything deleted that is currently online, there may still be copies saved in historical internet or government archives.

You may need to ask, petition or compel entities to delete information that you consider to be sensitive, but you will not likely be able to get data deleted from secret archives that you may or may not even know exist.

Nonetheless, though you may not be able to get all your sensitive data deleted, you can still slow it or stop it from spreading and keep it out of the hands of most people by reducing your online footprint.



HOW TO DISAPPEAR FROM ONLINE

- PRIVACY IS TYPICALLY COMPROMISED BY HUMAN ERROR, COMPLACENCY, SHORT CUTS AND FAILURE TO ADHERE TO SOP.
- HAVE SEPARATE DEVICES FOR EACH IDENTITY AND USE THEM AT DIFFERENT LOCATIONS.
- EMAILS, CREDIT CARDS, PHONE NUMBERS AND EVEN ADDRESSES CAN ALL BE MASKED AT LOW COST.
- THERE ARE TOOLS YOU CAN USE TO SEND ENCRYPTED EMAIL AND TEXT MESSAGES FROM VIRTUALLY ANYWHERE, AND LEAVE NO TRACE BEHIND.

SURVIVOPEDIA

Privacy May Not Be Convenient, But It Is Worth It

Privacy reduces stress and keeps you free. One thing privacy is not, is convenient. Many people are addicted to convenience these days, but reclaiming your privacy, like most things worth doing, is neither easy nor convenient.

When I was a kid, long distance phone calls out of country were extremely expensive. So was air mail! So, we sent letters by surface mail and then we would wait over a month for a reply.

I have read journals of my immigrant pioneer ancestors in the old West. They would have thought I was spoiled as a kid because it was not uncommon for them to wait years for letters from family. Now, if the power grid or the internet hiccups, even for a minute, folks just go nuts. In emergencies, people often endanger themselves for a chance to get information that is often nothing more than rumors!

If you are addicted to convenience, you will never know privacy or freedom until you overcome this addiction. The best way to do this is to sufficiently commit yourself to the cause of privacy right from the start.

If you fail for want of motivation, it will not likely be because you lacked self-discipline, but because you were not sufficiently dedicated to the cause. If your motivation wanes as the battle drags on, revisit the reasons why privacy is so important.

Disappear Online and Fly Under the Radar

Develop a Privacy SOP and Stick to It

The quality of your IT OPSEC/PERSEC SOP and the competence and discipline with which you execute it are, far and away, the two most crucial factors in determining whether you will be found or successfully disappear online.

If you are a smart, that's great, but genius hackers get caught all the time.

Identify Who You Are Hiding From

Who are you hiding from and how much money, time and human resources are they willing to invest in finding you?

These are huge factors, because hiding from a stalker with limited financial resources, intelligence and contacts is very different from hiding from an evil genius billionaire or a superpower willing to create entire departments dedicated to your capture.

If the entity you are hiding from can, and is willing to, allocate satellite time and Santa Clause budgets to teams of analysts, you truly have your work cut out for you.

The more money and resources those searching for you are willing to invest in finding you, the more likely it is that they will eventually find you. Will they spend $50, $500, $5K, $50K, $500K, 5M, 50M or more?

It helps if you can estimate that number because every tier, it becomes exponentially harder to hide from them. Up to $500, you will probably go to your grave without being found. 5K gets tougher *if* they hire a competent professional. At 50K their reach extents well across international borders and they can pay for a lot of IT analyst time. At 500K you are in serious trouble.

Compartment

How deep you take it is up to you, but compartmenting is an effective and somewhat idiot-proof way to keep from screwing up the execution of your SOP. Compartmenting should go much deeper than we will take it here, but it will give you the idea and you can extend it to other areas (banking, mailing addresses, vehicles and so on.)

1. **Identities** – Criminals have aliases. Good guys have alternate identities, pen names, stage names, travel names, undercover names and call signs. Separate the identity with which you deal with the government from other identities, including any other identities that you use to access the internet.
2. **Hardware** – You can use the internet and talk on the phone using your legal name and alternate identities, but using separate phone(s) and computer(s) for each identity is a simple and robust way to compartment. This way, the IP for the online identity you want to keep under the radar has different Mac and IP addresses from the person your neighbors know.
3. **Locations** – You can use computer(s) and cell phone(s) with each identity, but do not use them in the same place! Every time your cell phone connects to a cell tower, analysts have an opportunity to get a pretty good idea of where you are at. If your device has a GPS and it is enabled or able to be enabled remotely, they know right where your phone is at, and for most folks nowadays, their phone might as well be surgically implanted, because it is always with them.

The IT forensics bag is a great tool for maintaining compartmented locations because you can drop a phone in one of these bags and its heavy EM shielding prevents it from communicating with cell towers, wireless routers, skimmers and any other wireless technology that could tie the location of the device to locations frequented by your other identities.

If two of your identities frequent the same place or their paths cross, that would be a good place to setup surveillance, search for a dead drop, etc. and connect the two.

Make Your Computers and Devices Hard to Track

1. VPN (Virtual Private Networking) Service

VPN establishes a point to point connection from your computer to another computer somewhere on the internet. Information is then sent and received through an encrypted virtual tunnel, protecting your privacy.

Because the data is encrypted, even if it is intercepted with a packet analyzer, without the correct encryption key the intercepted data will just be a bunch of meaningless characters.

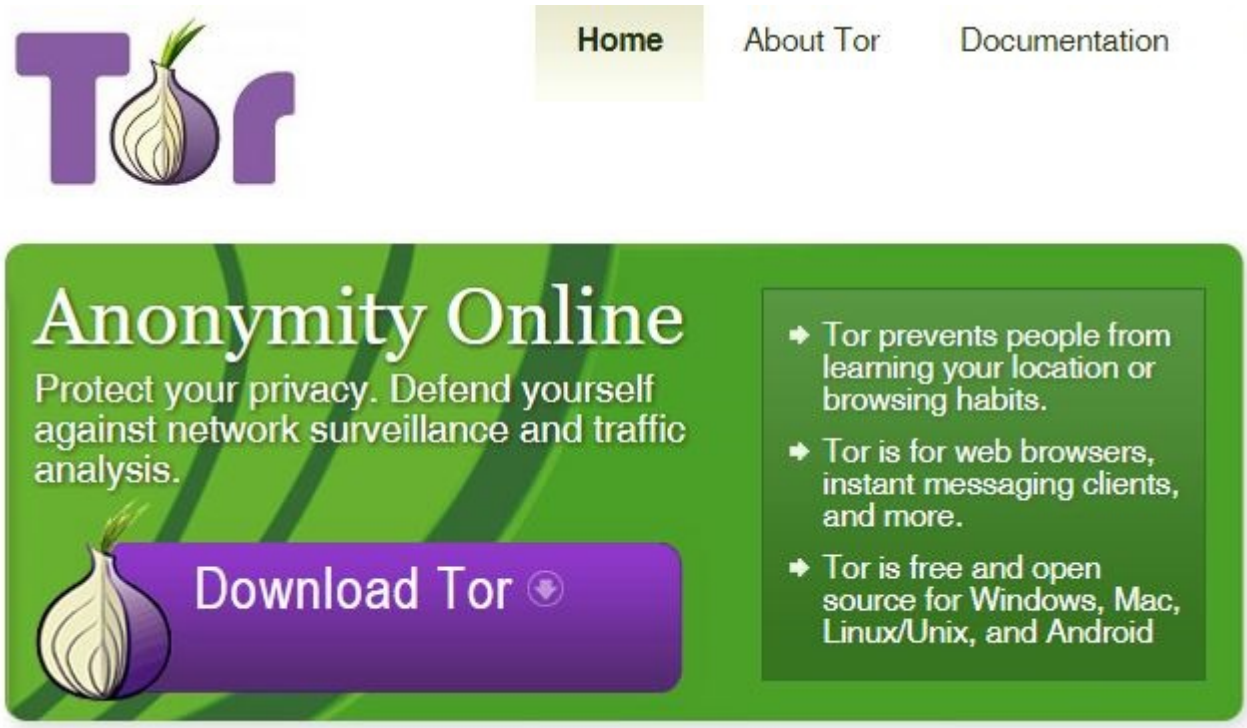
VPN Service is a paid internet service that establishes a VPN connection from your computer, to a random computer at your VPN service provider. This way, when you surf the internet, the websites see the IP address for the computer at the VPN provider, not your computer.

If you choose a VPN service provider that owns vast banks of IP addresses in many countries, all with laws that do not allow good cooperation with your country, even getting your address out of your VPN provider as part of an investigation becomes problematic and expensive, helping to protect your identity and privacy.

Criminals, web sites or stalkers will not likely be able to get you address and private investigators would have to spend a lot of money and time and likely break a lot of laws get ahold of your IP address.

2. TOR (The Onion Router)

It is free software maintained by volunteers that can enable you to share information over public networks, like the internet, without compromising your privacy.



It does this by connecting through a series of virtual tunnels, using the computers of other TOR users instead of connecting directly.

3. ORBOT

This is TOR for Android.

4. Blur

Blur is a service by an online privacy company called Abine. A very common need online is to provide an email address, which needs to be verified to open an account. Blur solves this problem by giving you the ability to create an unlimited number masked emails and forwarding the mail sent to them to another email address that you designate.

If that email is used to spam you, you can block it with a single click. The free service gives you an encrypted password manager, masked emails, tracker blocking and auto-fill, which greatly simplify account creation, which you will be doing a lot of if you maintain multiple identities.

The paid Blur service adds masked credit cards, a masked phone number that also works with text messages and a backup and sync service. If you get unwanted phone calls, you can block them. If you don't want to give your banking information to some shady vendor on eBay, give them a masked card, email and phone number.

Blur is not the only free service that provides masked emails. Some other services are not based in the US, which is a plus, and do this in an even more secure fashion where the email only exists for a short time and is then gone forever without creating any records to subpoena, but Blur is the most comprehensive service I have tried so far.

5. Tails (The Amnesiac Incognito Live System)

A magnificent privacy tool, Tails is a live operating system built on a Unix-like OS called Debian built with one thing in mind: privacy. Tails can start from most USB sticks or a DVD, uses TOR to access the internet anonymously, leaves no trace and includes tools to encrypt files, email and instant messaging … built in. Best installed on a multiport flash drive with iPhone, MiniUSB OTG, and USB connectivity.

So, why aren't you downloading it yet? If you aren't or haven't you should.

6. Panopticlick

A tool by the EFF that tests the uniqueness of the configuration of the internet browser you use to access the

site. If you have a very unique browser configuration, this can be used like fingerprints or DNA for your browser, identifying your computer with a certain probability like 1 in 500K. Or 1 in 200 … even over VPN!

Encrypt, Encrypt, Encrypt

Think of encryption as a final layer of defense in the even that your privacy measures are compromised.

Click here to get your guide to a layered survival defense!

I truly believe that one day, professors will refer to our time as the "Neo-encryption Era" … and that they will point at us and laugh.

You see, they will dig up hard drives and M-Disks in landfills, buy them from junk dealers or study them in museums and still be able to read the data as much as a thousand years later. They will have a look at our lives in unprecedented levels of detail.

They will have HD video, medical records, credit card, bank and other financial records. Customer loyalty records will tell them everything your bought from the grocery store and they will examine it, and likely draw conclusions out of context.

They will have phone records and ISP records that may show everyplace you ever go with your cellphone turned on, every email, every text and secret government records that you probably don't even know exist. They will have records created every time cameras mounted on patrol cars and tow trucks image your license plate in parking lots.

From these records, they will determine, where you go to church and how often. Where you eat and where you shop.

Meetings, work days and gun shows will be analyzed, as will everyone you knew who was also there. They will probably draw all kinds of conclusion that may or may not be correct about why you were there and with who or that that some place you went to regularly was within walking distance of where a friend's spouse worked or a gay bar or mosque, and so on … and they will do this, in part, because we were too ignorant or lazy to encrypt our data.

Some encrypted email providers, like Countermail in Sweden, support hardware (USB) encryption keys and even accept cash payments through the mail. If you don't have a little encrypted server space in another country and the ability to create untraceable email addresses, today would be a great time to start.

Reduce Your Online Footprint

DeleteMe! – DeleteMe! Is a another service by Abine that removes personal info from the major online data brokers, substantially reducing your online footprint. The service ranges from $69-$129 per person per year with discounts if you add additional people or pay for more years. But you can do the same thing yourself if you have more time than money and Abine has a great resource page to help you do just that for free right here. Some data clearinghouses do not make this process convenient, but you are going to need to do a certain amount of legwork even if you pay for some services.

Privacy Badger – Blocks spying ads and invisible trackers.

DuckDuckGo – Search engine that doesn't track you.

Firefox – Internet browser for those concerned about privacy. Firefox has many plugins, such as NoScript, HTTPS Everywhere, Ghostery, Cookie Monster, AdBlock Plus and others that contribute to safer, more private browsing experience.

EFF Surveillance Self-Defense – A great collection of tips,

tools, tutorials, overviews, briefings and how-to articles you can use to education yourself about privacy. Study it and fill in the chinks in your armor.

If you’re tired of all the stuff every employer, cyber stalker, or online criminal can find out about you and your family, this is the right moment to protect yourself and go unnoticed. It’s one big step to a secure existence and stay safe in these turbulent times!

*This article has been written by **Cache Valley Prepper** for Survivopedia.*