SOVEREIGN MAN'S

Guide to Offshore Hosting

SURVIVE AND THRIVE IN THE AGE OF TURMOIL

Table of Contents

Why Offshore Hosting?

That's a good question.

Offshore hosting is yet another flag you can plant to reduce your sovereign risk.

The reason to host your website and email offshore is because if you host your website in your home country your government can basically take down your site and confiscate your servers as they please if they don't like what you're doing.

Sure there are Freedom of Speech laws in many countries that does protect you to a certain extent, but you don't even have to do anything wrong or illegal. It's enough if there's one infringing site on the same server as your website, or even if they're on different servers belonging to the same hosting company. That's what happened to customers of the Swedish hosting company PRQ (former host of WikiLeaks) when police raided them to take down the filesharing site The Pirate Bay back in 2006. A lot of legitimate customers got their websites shut down and files confiscated, and if they managed to get them back at all it probably took months.

That's why you should host your website outside the jurisdiction of your home country. It provides an extra layer of protection and offers a higher degree of privacy. Anonymous hosting is often easier to find if you look outside your home country.

So let's get down to business. Here's a couple different offshore hosting providers. As always you should do your own due diligence before you choose a provider for your website. We do not have any experience with most of these companies and can't be held responsible for their quality or service. However all of them claim to offer 99.9% uptime, which is the least you should expect from any good hosting company.

Offshore Hosting Providers

Hetzner

http://www.hetzner.de
Base of operations: Germany

Hetzner is a German based hosting company with great reviews all over the internet. While their setup cost is high for the more high end dedicated servers their monthly cost is low. Prices for domain registration is also above average. If you plan to register domains other than the usual .com/net/org/info you should definitely find a cheaper company to register your domains.

Shinjiru

http://shinjiru.com
Base of operations: Malaysia, Singapore and Europe

Shinjiru has been in business since 1998 and operate in seven data centers world wide. Their headquarter is in Kuala Lumpur, Malaysia, with data centers in Malaysia, Singapore, United Kingdom, Moscow, and Holland. They offer a range of different services and you can pay with

credit card, wire transfer, Western Union, Paypal, Liberty Reserve, Moneybookers, cash, or local bank transfer.

Services:

Domain Registration
Cloud Hosting
Personal Hosting
E-Shop Hosting
Business Hosting
Basic Email Hosting
Private Email Hosting
Microsoft Exchange Servers
Virtual Private Server (VPS)
Virtual Private Desktop (VPD)
Virtual Trading Desktop (VTD)
Offshore Dedicated Server (DS)
Content Delivery Network (CDN)
Server Colocation
SSL Certificates
Microsoft Sharepoint

Regarding their email hosting Shinjiru is HUSHMAIL's official partner & reseller in Malaysia. Starting from USD1.90/month you get secure and offshore email hosting, with full support for strong encryption technology.

Ninja Panther Hosting

http://www.ninjapanther.com/
Base of operations: Netherlands

Ninja Panther Hosting only offer shared hosting, with their cheapest package starting from $2.95/month. They might not be your best choice if you plan on having a very large website, but for smaller websites what they offer is more than enough.

AlibabaHost

http://www.alibabahost.com/
Base of operations: Netherlands

AlibabaHost offer shared hosting, VPS and domain registration in the Netherlands, as well as dedicated servers in France, Netherlands and Romania. Currently they host over 10,000 websites, which isn't much when compared with the biggest in the US but still, it shows that they must be doing something right.

They also offer:

1 Gbps network port
Cloud Offshore Hosting
Free website transfer
No content restrictions

99.9% uptime gurantee
100% anonymous hosting
Anytime money back guarantee

Offshore Racks

http://www.offshoreracks.com/
Base of operations: Panama

Offshore Racks offer dedicated servers starting from $129.95/month as well as cheaper cloud server solutions starting from $24.95/month. They have even cheaper shared hosting solutions starting at $10.50, but the features are nothing like what you'd get on a shared hosting company in the US. So if you're after shared hosting you might want to look for a company that offers higher bandwidth.

CCIHosting

http://www.ccihosting.com/
Base of operations: Panama

CCIHosting has been providing offshore hosting in Panama since 2002. They offer shared hosting, VPS, dedicated servers, co-location, SSL, and have high privacy hosting, 24x7x365 live technical support and proven 99.9% network uptime(their words not ours). You can pay with credit card, paypal, Liberty Reserve, Western Union and bank wire.

Unless you feel like paying more than triple the normal price we don't recommend registering your domains at CCIHosting.

Glesys

http://glesys.com/
Base of operations: Sweden

This is a solid web hosting company with cloud VPS starting from €8/month, as well as dedicated servers. With their cloud VPS you can create/delete servers instantly, upgrade/downgrade without restarts, have full root access to your server and use both IPv4 and IPv6 addresses. If you're wondering about their stability, they have:

Redundant Internet connections
Tempered data centers
Dual power supplies
UPS & Diesel generators
Redundant storage
Three physical facilities
Guaranteed memory
RAID-10 * SAS 15.000 RPM
Backup once every day

Non-US Citizens

Hosting your website in the US might actually not be a bad choice if you're a non-US Citizen. Everything is better than having your site in your home country.

Domain TLDs and why they're important

You probably have or want to get a .com/net/org domain. All of those domain endings are essentially owned by the US government, meaning it's very easy for them to shut down a domain with one of those endings.

If you've got a .cc or .co domain on the other hand they will have to go through the governments of Cook Islands or Colombia to take down your website(or email address).

It's understandable that you want a .com/net/org domain for your website, but how about getting a .co or .cc domain for your email? That way even if your .com domain is confiscated your email will still be up and running.

More on Planting Electronic Flags

Planting your Electronic Flag

http://www.sovereignman.com/personal-privacy/planting-your-electronic-flag/

We all know that Google is in bed with the government… I suppose it's nice that CEO Eric Schmidt is at least open about it.

In a recent interview with CNBC, Schmidt effectively admits that Google archives everything about a user– web searches (google), email and contact lists (gmail), online office documents (google docs), photographs (picasa), text and voice messages (google voice), and even a user's current location (google maps).

The depth of this information is a bureaucrat's fantasy, and as Schmidt indicates, Google is obliged to hand it over.

Google is obviously very convenient; its features are powerful and can make life very easy… it's really unfortunate, however, that they are subject to the oversight of an increasingly intrusive and corrupt government.

This is simply a choice that you as a user have to make– privacy over convenience. If you fall in the 'nothing to hide, nothing to fear' camp, giving the government access to your entire electronic life may be perfectly acceptable.

For the rest of us, there are great solutions that provide a lot of conveniences.

I've discussed electronic privacy in the past and promised to give you a list of countries that don't snoop on phone and email conversations. You can obviously scratch off most of North America and Europe, but there are still countries that respect individuals' privacy.

The folks at Cryptohippie were kind enough to do the heavy lifting for me, ranking 52 major countries on issues such as constitutional protection of privacy, data retention, 'loose' warrants, financial tracking, and likelihood of data inspection at border checkpoints.

You can download the full report here.

Although their list is definitely incomplete and needs updating, I generally agree with their rankings. Sweden and Thailand, which have strong elements of electronic snooping, need to be moved higher up the list.

According to CryptoHippie, the top 10 electronic police states include North Korea, China, Belarus, Russia, UK, France, Germany, and of course, the United States.

From my assessment, countries that respect electronic privacy include Panama, Costa Rica, most developed Caribbean nations like the Bahamas, Brazil, the Philippines, and Switzerland.

One email provider you may want to consider is Australia-based Fastmail. As the name suggests, the technology is incredibly fast, and contains some of the most customizable features I have ever seen. For example, you can set a 'distress' password that, when typed in, will lock down your email account for a defined period of time.

Best of all, while Australia is a 'middle of the road' electronic police state, the Fastmail founders have taken on a multiple flags approach, basing their primary and backup servers in different countries outside of Australia.

If you have your own domain for email, e.g. yourname@yourdomain.com, you can easily change your domain's setting to point your email servers to Fastmail. You will never notice a difference in service and can rest a bit easier knowing your email archives aren't feeding bureaucrats.

I think it's a sharp idea for anyone who takes privacy seriously to plant an 'electronic flag' somewhere other than his country of residence. In terms of living a more free, multiple flag lifestyle, it's definitely the easiest, most cost effective thing you can do.

Planting Multiple Electronic Flags

http://www.sovereignman.com/expat/planting-multiple-electronic-flags/

Now, I'm normally a pretty laid-back guy, and there's not a whole lot that bothers me. But when technology that's supposed to make our lives easier suddenly doesn't work, I become unglued.

After 12-hours of our website being down, the tech support folks at our hosting company finally determined the root cause of the issue: a faulty network cable. That's it… nothing sinister, nothing complicated, just a 19th century solution to a 21st century problem.

It's amazing how reliant on technology we have all become; this is not necessarily a bad thing. Every successive generation in the history of the world has had its own emerging technology that became integrated into their society.

Furthermore, each caused the older generations and social critics of the day to bemoan how that new fangled technology was ruining their civilization, making people 'soft', etc. Electricity, indoor plumbing, the telephone, etc. were all met with resistance by some measure of the population.

The chief difference between then and now is that our technology, at least in the consumer's perspective, is in digital or electronic form… and that the rate of technological progression is exponential (according to Moore's Law). Naturally, the government has been keen to adapt (somewhat reactively) to these changes.

Curiously, a lot of people think that the government actually spearheads and innovates technological advances. This may have been true 50-years ago when many of the world's brightest tech minds aspired to government service. Today they aspire to Apple, Google, and their own startups.

Governments now rely on the private sector for their technology needs, and the latest issue with Blackberry is an excellent case in point. For its enterprise service, the popular data handset uses a series of complex encryption algorithms that are frankly too difficult for most government security agencies to break.

So, instead of spending all of that time, money, and effort trying to break Blackberry's encryption, a handful of governments have issued its maker, Canada-based Research in Motion (RIM), an ultimatum: hand over your encryption key, or we'll ban your product.

The United Arab Emirates and Saudi Arabia, among others, are the first to do this. Ironically, while authoritarian governments may or may not be successful in a deal with RIM, they are still going to be behind the learning curve when it comes to new technology.

Simply put, the market will continue to adapt, and new technologies will emerge that thwart the best efforts of government to intercept every bit of data flying through the air.

In my opinion, though, this Blackberry case underscores a critical point that we have discussed before– technology is an important flag that you should consider planting in order to diversify your sovereign risk.

For example, if your email provider is based in the same jurisdiction where you live, work, and hold citizenship, the chances of being locked out of your account, or having your private messages used as evidence against you, increase dramatically.

Switching over to an offshore email provider can be done at no cost, an often you don't even need to change your email address.

For technology entrepreneurs, I would strongly advise planting multiple flags and spreading your sovereign risk across multiple jurisdictions; for example, you can base your company in one country, your web server in another, your email server in another, your bank account in another, and your merchant processor in another.

This safeguards your business, as well as your information, from the ridiculous and often unpredictable acts of impetuous bureaucrats who know no other means but to confiscate and regulate their way to achieving their own agenda.

Why you want an offshore email account

http://www.sovereignman.com/personal-privacy/why-you-want-an-offshore-email-account/

Not long ago a Wyoming bank employee was routinely emailing some loan documents to a customer's personal Gmail account. It sounds like a simple enough task, yet somehow the employee made an enormous error.

Not only did he erroneously attach a file to the email that included the names, addresses, tax IDs, and loan information for 1,325 customers, but he sent it to the **wrong Gmail address!**

We've all been there… victims of our own fat-finger negligence– good intentions gone horribly wrong because our technology moves so quickly.

And so, with pulse pounding and panic setting in, the bank employee immediately sent a follow-up email to the mistaken address, pleading with the account owner to delete the sensitive data and contact him as soon as possible. And then he waited…

After several days had passed without response, the bank contacted Google for help. They wanted information about the unintended email recipient– is the Gmail account even active? What is the account holder's name? Would Google take steps to ensure that the confidential information is not open or disclosed?

Google refused to comply without a court order, so the bank sued… and in this particular case the wheels of justice moved rather swiftly– within a few weeks, US District Judge James Ware ordered Google to temporarily deactivate the recipient's Gmail account and disclose information about the account to the court and to the bank.

Days later, Google and the bank jointly announced that the issue had been resolved… but because of the court order, the user's email account has to remain deactivated until the judge hears the case

again on October 5th.

I read through the case files with great interest because, frankly I was disgusted that 'the honorable' Mr. Ware could compel Google to deactivate an individual's email account.

Sure, the bank employee made an unfortunate mistake. But email accounts are deeply personal, even more than physical home mailboxes. I wondered if the employee had accidentally put a physical package in the mail to the wrong mailing address, would a federal judge direct FBI agents to beat down the recipient's door?

Doubtful. Rather the judge would have told the bank, "Sorry guys, but you'd better start notifying customers of the security breach pronto."

Advances in technology have a significant impact on the world; as I am fond of saying, technology is key economic growth engines over the long-term. But governments and regulatory authorities have a bad habit of abusing the ease and comforts that technology provides as a means to erode personal privacy.

Email usage, web searches, e-commerce, credit cards, etc. all make life easier and more convenient for consumers. They also make it easier for the government to keep tabs on our activity and whereabouts– and as this Google case demonstrates, the burden of proof required to violate an individual's electronic privacy is quite low.

To take a page from WG Hill's 'Three Flags' approach, I believe wholeheartedly in spreading one's sovereign risk among different jurisdictions– establishing residency in a country that values foreign visitors, while maintaining citizenship in a country that doesn't tax worldwide income and basing assets in yet another no-tax/low-tax jurisdiction.

To this approach, however, I would add another 'flag': jurisdictions in which an individual should base sensitive and electronic assets. The goal is to ensure that the computer server where your email is hosted, as well as the company which owns/manages the servers, are both outside of your country of residence and citizenship.

Clearly there is going to be some element of counterparty risk in any transaction that involves more than one person; but if the Gmail recipient had been using an email account in, say, Singapore or Switzerland, the chances of a foreign judge ordering the account to be deactivated are slim to none… and slim's out of town.

Below I provide a links to a few offshore email providers whose servers are located overseas. With a properly configured account, you can switch to an offshore provider and still keep your existing email address:

Neobox

http://www.neomailbox.com

Base of operations: Netherlands

e-mail.ph

http://www.e-mail.ph

Base of operations: Philippines

Swiss Mail

http://www.swissmail.org

Base of operations: Switzerland

Remember, using these providers decreases the likelihood of your email account being confiscated or deactivated by your home government– offshore email hosting does not guarantee privacy or security unless you use encryption schemes (to be discussed in the future).

What now?

Again, you don't have to do anything wrong to be targeted by your home government. It might be bad luck, a bureaucrat in a bad mood, or simply hosting your site in the wrong place at the wrong time. The point is that hosting your website offshore will give you that additional layer of protection that makes you sleep better at night.

We'd suggest you look through the offshore hosting companies above and see if one of them fit your needs. Search for reviews of these companies, and not the usual fake review from affiliates, but from real people.