
DATA
PRIVACY
ENCRYPTION
SECURITY
SECURITYNET
DATA SECURITY, ENCRYPTION AND PRIVACY

Thank you for downloading this e-book. My aim here is to show you a number of ***Free*** ways that you can use ***right now*** to protect your privacy online. Plus a few great security products you would have to pay for.

However, you can significantly safeguard your privacy without spending a penny!

My name is Ian Zatman. I am the founder of SecurityNet.global, an easy-to-use encrypted data service for when email or cloud storage is just not secure enough for sharing your confidential files with colleagues, friends, clients.

I am also an IT consultant, and I work primarily in the finance sector in London and Europe, designing and creating software solutions.

On an assignment at a European bank, almost 20 years ago, I was hired to track and document the flow of payments data across Eastern Europe.

And I was horrified at what I discovered – that all network traffic is totally exposed and vulnerable to hackers, trackers, thieves and malicious third parties – including your governments. Of course, this is common knowledge today!

Unfortunately, there is no single silver bullet that can solve the problem of finding a way to protect our privacy and our security.

This document discusses the different types of software or service that you absolutely need to protect your security and privacy online.

I hope you find this paper informative and helpful. It is full of actions you can take ***immediately*** to protect yourself.

Ian Zatman
SecurityNet.global
February, 2020

7 ways to Protect your Online Privacy

1. Your web browsers are tracking you

If you're like most people, you are probably using one of the leading browsers without knowing what this can mean for your online security.

With Google's dominance on the internet, the amount of personal information they collect is mind-boggling. Google Chrome, Firefox, and other popular browsers are easy to use, but they track everything you do – primarily to sell you the things they figure you are interested in.

Trackers collect information about which websites you're visiting, as well as information about your devices.

One tracker might be there to give the website owner insight into their website traffic, but the rest belong to companies whose primary goal is to build up a profile of who you are: how old you are, where you live, what you read, and what you're interested in.

This information can then be packaged and sold to others: advertisers, other companies, or governments.

The companies tracking you are generally unrelated to the website you're visiting. Called "data brokers", they have fancy techy sounding names like ComScore, DoubleClick, and cXense (though DoubleClick is actually owned by Google). Their whole business model is built on the selling of "customer data". YOUR data!

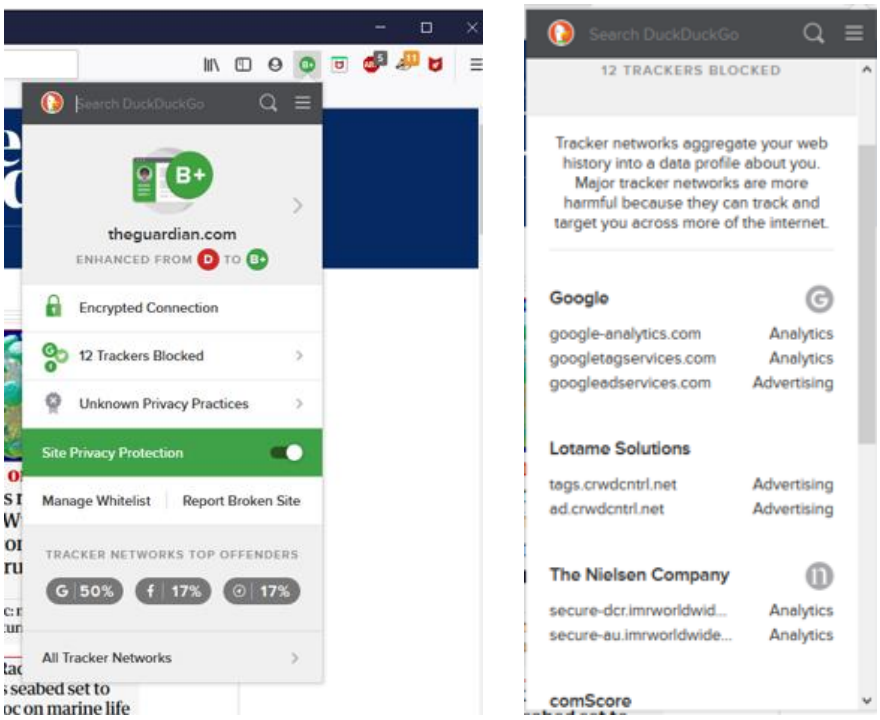
They are also joined by more well-known companies. Some of these trackers are totally visible, hiding in plain sight: Google's red G+ button, for example, is a tracker; Facebook's "like" thumb and Twitter's blue bird are also trackers.

However, with a few ***FREE*** add-on extensions, you can truly enhance your privacy.

i. Install the DuckDuckGo browser extension

This extension has a built-in tracker network blocker, private search facilities, and smart encryption.

It blocks the trackers active on the web and grabbing your browsing habits to make a profile of you. They sell the data on for marketing purposes:



The DuckDuckGo extension adds a toolbar icon that shows you a Privacy Grade rating when you visit a website. This rating lets you see how protected you are at a glance, dig into the details to see who we caught trying to track you, and learn how we enhanced the underlying site's privacy measures.

The Privacy Grade is scored automatically based on the prevalence of hidden tracker networks, encryption availability, and website privacy practices.

Too many people believe you simply can’t expect privacy on the Internet. DuckDuckGo are fighting to change that, and have made it their mission to set a new standard of trust online. Install DuckDuckGo and take back your privacy!

ii. Install the Privacy Badger browser extension

Privacy Badger automatically learns to block invisible trackers. Instead of keeping lists of what to block, Privacy Badger learns by watching which domains appear to be tracking you as you browse the Web.

Privacy Badger sends the *Do Not Track* signal as you browse the net. If trackers ignore your wishes, your Badger will learn to block them. Privacy Badger starts blocking once it sees the same tracker on three different websites.

Besides automatic tracker blocking, Privacy Badger removes outgoing link click tracking on Facebook, Google and Twitter.

You can use both browser extensions as they work in slightly different ways.

This way you can be sure you are catching all the trackers

2. Try some alternative browsers for safe browsing

I must admit that I use Google as much as anyone. But I am also aware that this mega-corporation is tracking everything I do.

You might think it doesn't cost you a thing to search the Internet or to send an email to your friends and clients, right?

Well, maybe there is a cost. If you use the best-known browsers, search engines and email providers, you're doing so at the cost of your privacy.

They are very good at what they do – they provide results that seem to give you the information you are looking for. Or they provide you with links to websites that ***claim*** to offer this information.

And after you visit a web site and continue your search, you start to see all sorts of ads for the web site you have just visited.

They have just got you by the throat!

The truth is that the internet is becoming more and more unsafe, and it's wise to look at the wider selection out there and choose a safe browser that will keep you from having your most sensitive data stolen and/or sold to third parties.

Read on for some more ***FREE*** solutions. Either that, or use the add-ons I recommended above. Or do both!

i. Epic Privacy Browser

Epic Privacy Browser is said to be the most secure browser that protects you from tracking scripts, cookies, third-party widgets and Ad networks.

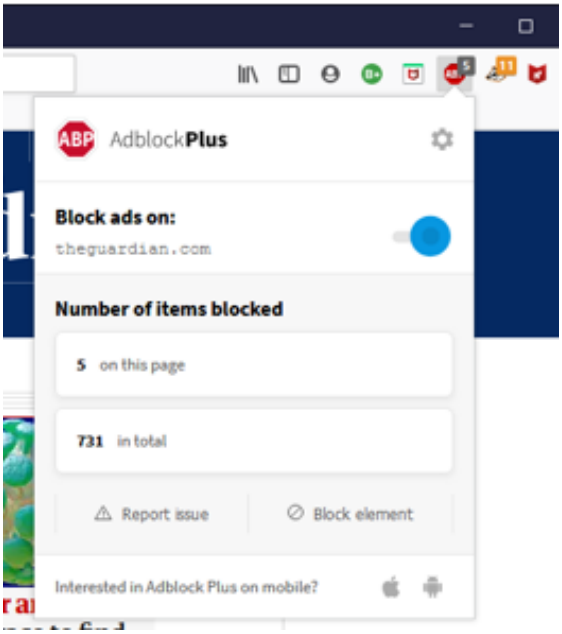
It also lets you access the blocked content from others countries. Using this browser, your searches remain private and it stops search engines saving your IP address.

ii. SRWare Iron Browser

SRWare Iron Browser is a secure browser that mimics Google Chrome - except for its privacy features. It also claims to be the "real alternative" to Chrome.

iii. And get yourself an Ad Blocker while you're at it

And for ad blocking I recommend Adblock Plus – a free ad blocker. You can easily surf the web without annoying ads.



3. Secure Search Engines for safe browsing

These days when I am searching for something that I would consider a private matter, I tend to use alternatives to Google that focus on my privacy – these search engines are designed for privacy, and they do not track you or profile you.

And these, too, are ***FREE***.

i. DuckDuckGo – a safe alternative to Google

I found this search engine a while ago, after getting totally fed up with Google asking me to review and agree to its Privacy Policies.

This is DuckDuckGo's privacy policy: click here for the full story, but basically…

> *DuckDuckGo does not collect or share personal information. That is our privacy policy in a nutshell. The rest of this page tries to explain why you should care.*

It also says:

> *"DuckDuckGo prevents search leakage by default. Instead, when you click on a link on our site, we route (redirect) that request in such a way so that it does not send your search terms to other sites. The other sites will still know that you visited them, but they will not know what search you entered beforehand . . . DuckDuckGo takes the approach to not collect any personal information. The decisions of whether and how to comply with law enforcement requests, whether and how to anonymize data, and how to best protect your information from hackers are out of our hands. Your search history is safe with us because it cannot be tied to you in any way."*

ii. Startpage – another safe alternative to Google

This is another one I found when looking for an alternative to Google.

These guys have a totally different approach. For example:

> *"You can't beat Google when it comes to online search. So we're paying them to use their brilliant search results in order to remove all trackers and logs. The result: The world's best and most private search engine. Only now you can search without ads following you around, recommending products you've already bought. And no more data mining by companies with dubious intentions. We want you to dance like nobody's watching* and *search like nobody's watching."*
>
> *"We don't collect or share your personal information. Ever. There's literally no data about you on our servers. None. We can't profile you, and we can't be forced to hand over your data to authorities, simply because we don't have any data to hand over."*

You can find them here.

These guys are based in The Netherlands which is outside the reach of both the USA and UK jurisdictions. Better for your privacy 😊

4. Email "spoofing" and how to stop it

Email spoofing is where the spammers are using **your** email address to send fake emails to your own customers as well as the world at large.

The first time this happened to me, I noticed I was getting all sorts of mail delivery notices regarding email addresses I had never sent an email to. I was a victim of spoofing!

This was many years ago now - I called my ISP to see what I could do and they kindly told me there was nothing I could do! They told me to wait a week, and they would move on to someone else – which is exactly what happened.

Imagine how you would react if a spammer sent a fake invoice to your customers? This happens, and it is very upsetting to your clients as well as detrimental to your own reputation.

Since then, several email security methods have been developed to try and stop this sort of thing, known as SPF, DKIM and DMARC.

These methods are also ***FREE*** to put in place.

Here is a ***VERY*** brief overview of SPF, DKIM and DMARC…

- **SPF: Sender Policy Framework**
  The Sender Policy Framework, is a way for recipients to confirm the identity of the sender of an incoming email. SPF restricts who can send emails from your domain.

  SPF can prevent domain spoofing – that means, preventing spammers using your stolen email address. It enables your mail server to determine whether or not a message came from the authorised domain. It will help stop people using your email address fraudulently.

- **DKIM: DomainKeys Identified Mail**
  DKIM allows for the identification of "spoofed" emails but using a slightly different process. Instead of a single DNS record that keys off the FROM: address, DKIM employs two encryption keys: one public and one private.

  DKIM ensures that the content of your emails remains trusted and hasn't been tampered with or compromised.

- **DMARC: Domain-based Message Authentication, Reporting, & Conformance.**
  While SPF and DKIM can be used as stand-alone methods, DMARC must rely on either SPF or DKIM to provide the authentication. DMARC ties the first two protocols together with a consistent set of policies.

Now, this is a very technical subject, so I recommend you get in touch with your email service provider. They should be able to set up the SPF, DKIM and DMARC configuration for you.

If they can't (or won't) then it's time to change your service provider!

5. Virtual Private Networks (also known as VPNs)

When you access a website on the internet, you start by connecting to your internet service provider (ISP). They then redirect you to any websites that you wish to visit. They also keep track of who you are and where you go!

For example, in the USA, the Patriot Act allows the government to force any company into secretly spying on their users and, thanks to a Gag Order, legally restrict a company from publicly acknowledging this! The UK isn't much better!

However, VPNs can hide your online activity and protect you from the many dangers on the web – from hacker attacks to data selling, identity theft, and much more. ***But I must stress – they can only protect you so far.*** The VPN will redirect you to any websites that you wish to visit. However, those websites are not necessarily secure and they will probably track your activity!

Also, the best VPNs are ***NOT*** free – but they don't cost very much. There are some free options out there, but they are not worth the risk. In my opinion!

Choosing a VPN can be tricky, so you need to check the home location of the VPN service since the legal jurisdiction can seriously affect your privacy.

For example, the USA along with the UK are the worst jurisdictions for a VPN company to be based in. The most secure privacy-oriented VPN providers are based in locations that actively promote privacy.

For a list of some VPN options, check out this article – but read the small print carefully!!! https://www.techradar.com/uk/vpn/best-vpn.

6. Encryption Software

Just because you have antivirus software, a secure cloud storage system and a VPN installed, it still doesn't mean your personal and business data is safe from being stolen by malware, hackers and even government agencies!

There are all sorts of encryption software solutions out there that can help protect your data. Check out some of these file and folder encryption packages:

i. AxCrypt

AxCrypt makes encryption simple enough for any user, and even offers public key cryptography for secure sharing of encrypted files.

ii. Folder Lock

Folder Lock can lock access to files for quick, easy protection, and also keep them in encrypted lockers for serious protection. It combines a wide range of features with a bright, easy-to-use interface.

iii. CryptoForge

CryptoForge offers a simple, context-menu-based approach to encryption and secure deletion. Secure files on your computer, upload encrypted files and folders to the cloud, or distribute encrypted files among your contacts or partners.

iv. Steganos

Steganos creates secure encrypted storage for your sensitive files. It's very easy to use, and it offers some unique options for maintaining privacy and secrecy.

If you are using a Cloud Storage provider - or even setting up your own cloud storage – you can ensure your privacy by encrypting your files before you store them. And if a hacker, a government or other snooper does get hold of your data, it's encrypted – and you hold the keys!

7. For when email & the cloud is not secure enough…

i. You have taken the steps we have been talking about

- ✓ Identified and stopped the internet trackers
- ✓ Downloaded a safe internet browser
- ✓ Chosen a private search engine
- ✓ Tightened up your email security
- ✓ Got yourself a VPN
- ✓ And encrypted your most private files.

Excellent. Good work 😊

ii. But this is not enough when you have confidential data to share.

The trouble is that there really is no silver bullet when it comes to protecting our privacy on the internet. We generally require a whole layer of software to help us.

For example:

- ☒ Your VPN can only encrypt your activity so far…
- ☒ Your email will still be copied as it bounces around the internet…
- ☒ Even the best anti-virus software may not catch a malicious link you click…

We also need a profound sense of scepticism when it comes to our behaviour online, like clicking on links that we come across that sound interesting.

So, what do you do when you need to send super-sensitive, confidential documents to your clients, colleagues, legal team, tax advisors, business partners?

For your really precious and sensitive data, you need a way to communicate confidentially – from your computer to their computer, safely and privately.

iii. Which is why we developed SecurityNet!

SecurityNet is a simple to use encrypted data transfer service for a global audience of users where each user passes their confidential information *directly* to another user.

By ***directly*** we mean that literally.

- Your data flows from your computer to your contact's computer.
- Your communication is encrypted with ever changing passwords.
- There is no cloud server or middle-man in between you and your contact.
- This means there is no opportunity for spies, hackers, governments.
- And even if someone does intercept a transmission, all they get is garbage!

iv. How does SecurityNet work?

For those times when email and cloud storage is just not secure enough for your private files, we provide you with your own Private Encrypted User Network to effectively eliminate your exposure to risk, easily and conveniently.

How do we do this?

- Firstly, we don't store your data - unlike the big boys of this world!
- We connect you to your contacts only while your files are in-transit.
- Encryption passwords change every minute - even we don't know them.
- Only you and your invitation-only contacts get to see your confidential files.
- We don’t track what you do, and we don’t maintain any logs on our server.
- There is no cloud, no middle-man, no tracking, no profiling, and no logging.
- We cannot hand your data over to authorities as we don’t have any!

SecurityNet is currently available for Windows users and Mac users (running Windows with Parallels or Bootcamp). It installs in minutes, and users can grow a completely private encrypted user network from a couple of users to hundreds.

v. So how can I get SecurityNet?

We are about to launch SecurityNet v3.0 to the world, with great discounts and bonuses. And because you have signed up to get this e-book, you are already on the list to be notified when the launch happens!

For an introduction to SecurityNet, please click here for a brief video as well as contact information.

And for one of our training videos, showing how SecurityNet works, click here.

SecurityNet has been around since 2010, but has not been available to the general public. It was originally designed specifically for banks to protect payments data transmissions across insecure networks.

However, SecurityNet v3.0 has been adapted for use by small businesses and individual user networks as well as larger enterprises.

It is user friendly, with plug-and-play installation, and provides the latest in-transit AES encryption methods to protect the confidential data that you share with your clients, colleagues, business associates.

Please watch your inbox for the launch of SecurityNet v3.0 coming soon!