

2

Working with the Deep Web

What goes on in the Dark Web? What can you do there?

In Chapter 9, *What Goes on in the Dark Web - Case Studies*, Chapter 10, *The Dangers of the Dark Web*, and Chapter 11, *Using the Dark Web for Your Business*, we will discuss case studies and stories of what goes on the Dark Web, and in this chapter, we'll discuss what you can do there. We'll talk about Dark web markets, and digital currency, browsing the Dark Web and more.

In this chapter we will cover the following topics:

- Maintaining privacy on the Dark Web
- Transacting on the Dark Web
- Deep web emails - Onion Mail

Maintaining privacy on the Dark Web

Privacy and anonymity are the underlying reasons for using the Dark Web, but why?

And how?

Privacy and anonymity are necessary for a functioning society. People want to feel safe and not monitored or investigated.

Even with the proliferation of social networks, and the oversharing of personal information there, many people still want to keep their data private, and to keep their personal information to themselves.

The internet provides a way to communicate and share, but as time goes by, its becoming a way for vendors to collect information about us to offer us products which are supposed to be what we want, according to our behavior on the network. It's also way for governments to monitor us, and a way for scam artists and criminals to collect information about us for their malicious intents.

Using the Dark web allows people to communicate, buy, connect and work privately and anonymously.

At least that's the idea. As with all technologies or environments, the less ethical among us utilize the advantages regarding anonymity and privacy that the Dark web provides, for their own ends.

Privacy can be defined as a state in which a person (or a corporate entity) can hide information about themselves from others. This can be done for various reasons, which ultimately doesn't matter. The idea is that, it's possible, or at least should be. This is becoming enforced by laws, such as GDPR, or any number of privacy acts and laws

Anonymity, can be described as hiding a person's true identity from others without hiding or censoring their activities.

As I've mentioned previously, the Internet has affected these terms, and lowered the level of both, for us.

Malicious hackers, companies and governments all collect information about us.

This harms our privacy. Few people understand how much.

Without privacy online, your information (personal or business) can be accessed and used, by the three types I listed previously (malicious hackers, companies, and governments).

Take advertising companies, for example. They collect information to be able to target us according to our preferences, search history, and other parameters, causing the effect we see, while surfing the Internet—receiving ads for products or services which we either searched for, took an interest in, or in some cases, accidentally clicked a link.

Governments collect this information to profile us and see if any person or group is a dissident, and to prevent crime or acts of terrorism. No matter what the reason is, they are invading our privacy.

It's important to understand that anonymity and privacy aren't the same.

You could be anonymous, but still not private, or vice versa. For most of us, our identity is our most precious asset, and many people prefer to have separate identities online, to ensure anonymity.

For some, anonymity is important to be able to voice their opinions without fear of retribution. For others, it's a matter of in which country they're located, and for others it depends on what their profession is.

Bottom line, we want to protect our information, be it medical, financial or personal. If a malicious hacker gains access to this information, we are at risk of theft, blackmail, impersonation, fraud, or any number of attacks that could harm us, in many ways.

Freedom of expression or speech is a right that must be exercised by all cultures and people

To preserve or maintain our online privacy and anonymity, we can use various tools, such as VPN's, Tor Browser, and by doing this, browse the Dark Web.

So how do we work in the Dark Web, while also maintaining our privacy and anonymity?

First, let's talk about what can be done on the Dark Web, focusing mainly on the legitimate uses.

Transacting on the Dark Web

To buy or sell on Dark Web markets, you need to understand a little about cryptocurrency. You've all probably heard about Bitcoin, which is the most well known one, but there are many others.

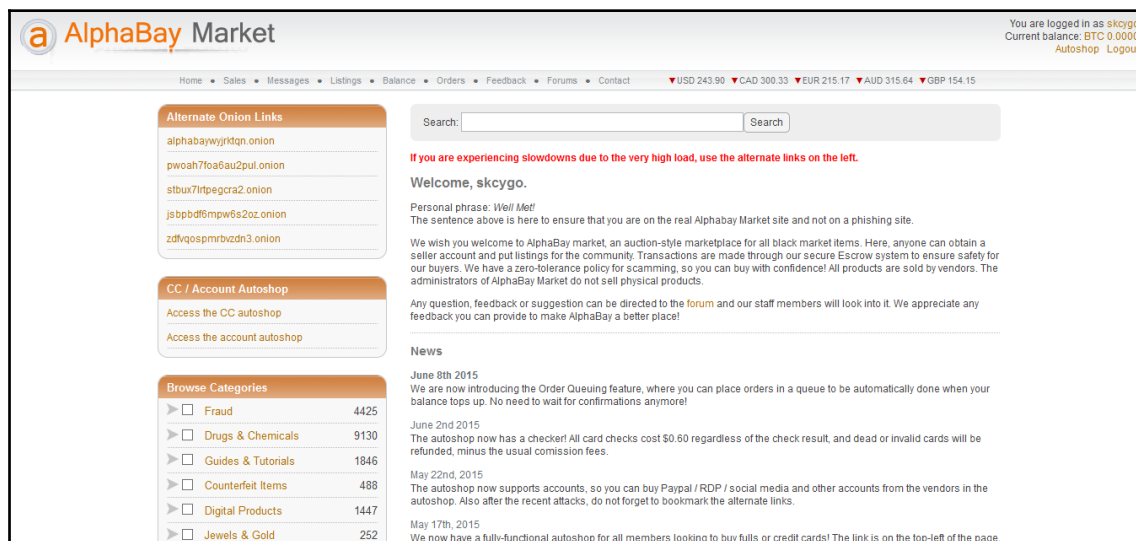
There are various ways to obtain Bitcoin or any other cryptocurrency, like purchasing or mining.

One of the important topics, transacting with cryptocurrency, is to maintain privacy. This is done by obfuscating the origin of bitcoins in a bitcoin wallet and the identity/location of the receiver.

This is usually performed by a 3rd party application/service, where the process can take between minutes to hours. Be careful when you look for one of these services, as there are scams in that market, usually due to the fact that they cost money, and provide vectors for scammers to steal our money.

Fraudulent sites pretend to be obfuscating services (also known as **tumblers**) and collect the money from unsuspecting users. The money will never reach the end target.

Always verify the service you want to work with for this (and in general), and use reputable services, which have existed for a qualified amount of time. Some Dark Web markets (AlphaBay, for example), offer these services for a small fee.



Secure transaction methods

There are three main cryptocurrency transaction methods:

Finalize Early (FE), **Escrow** and **Multiple Signature Escrow (multisig)**.

- **Finalize Early:** It is a payment method, in which a vendor requires receipt of payment before dispatching the purchased goods. The risk is on the buyer's end, but it also expedites the transaction due to little or no risk on the vendor's side (this method is the least secure for the buyer).
- **Escrow:** It is a payment method in which a Dark Web market will generate a bitcoin address to which the buyer transfers the payment. The market holds the buyer's money and pays the vendor only after the buyer marks the order as complete. It is moderately secured.

- **Multiple Signature Escrow:** It is also called multisig, this payment method generates multiple keys for the bitcoin transaction and payment release process. The multisig can be either 2 out of 2 or 2 out of 3, where 2 of 3 provides the most security for three keys - the market's key, the vendor's key and the buyer's key. The keys are:
 - **2-of-2 Multisig:** Market public key, vendor public key
 - **2-of-3 Multisig:** Market public key, vendor public key + customer public key

After receiving the goods, the buyer signs off on the transaction using his/her key, and then the market uses their key and releases the funds to the vendor.

If there are any issues, lack of communication, or if the buyer doesn't approve receipt of goods, the market can mediate the transaction and use its key which is highly secure.

Another part of financial transactions on the Dark Web are blockchains. As I've mentioned in a [Chapter 9, What Goes on in the Dark Web - Case Studies](#), blockchain is a public ledger in which all virtual transactions are indexed and recorded. Hackers can create **orphaned blocks**, through which they can attempt to take complete control of the blockchain ledger by manipulating the blocks in the ledger. There was a comparatively known attack, called the **51% attack**.

Always try to use the most secure option when performing transactions on the Dark Web.

I mentioned that there are several ways to obtain Bitcoin. One is buying Bitcoin from confirmed vendors, the other is Bitcoin Mining. This is done by individuals or groups, using dedicated hardware, which compiles a few hundred transactions from the blockchain ledger and then turns them into a mathematical problem.

Solving these problems results in new Bitcoin for the **miners**, referred to as **block reward** and verification of the Bitcoin payment network.

Bitcoin, or any other cryptocurrency (or even traditional currency) is always at risk from scams or frauds. One of the frauds that I've heard about, is related to "Bitcoin mining hardware".

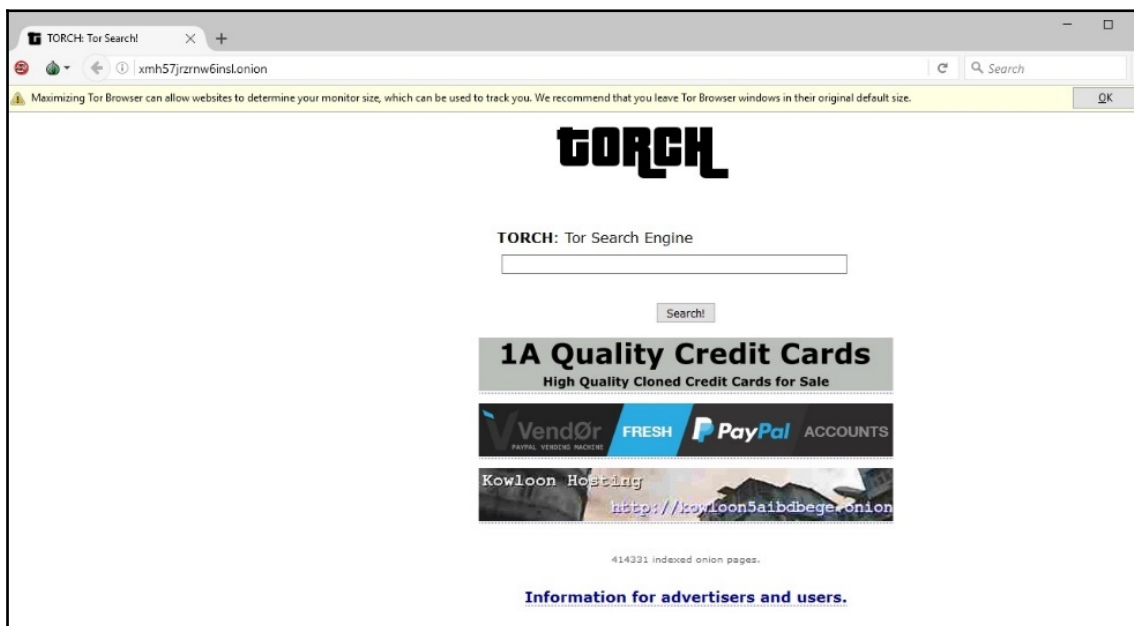
Scammers pose as legitimate hardware manufacturers, specializing in Bitcoin mining hardware, and collect money from people to develop or manufacture *new and special* Bitcoin mining systems, naturally never returning on investment and vanishing with the money.

Here are a few things to keep in mind while browsing the Dark Web:

- So if you want to make purchases on the Dark Web markets, remember—vet the market site first. Make sure it's not a scam.
- Second—never use your debit/credit card on a Dark Web site, never use Paypal, and if you purchase Bitcoin, do it from a legitimate seller who offers escrow services, or mine for Bitcoin. It's not that fast, or simple, but is feasible.
- Another common use for the Dark Web is browsing, and searching for content that either costs money on the Surface Web or that you can't find the information due to its sensitive or illicit nature.
- Always exercise common sense while browsing the Dark Web. Beware if people act too friendly, or if something seems too good to be true. Remember that people might try to take advantage of your fears of the Dark Web, when most of your fears aren't true, but are based on stories.
- Always use Tor Browser and preferably a VPN, before browsing to a Dark Web site, additionally, after finishing this book, you'll be able to decide which operating system to use when you connect to the Dark Web (Do Not use Windows).
- One of them, **Tails**, boots your machine from a USB flash drive, which helps the privacy and security of the user. This is good since nothing will remain on the computer when you reboot.

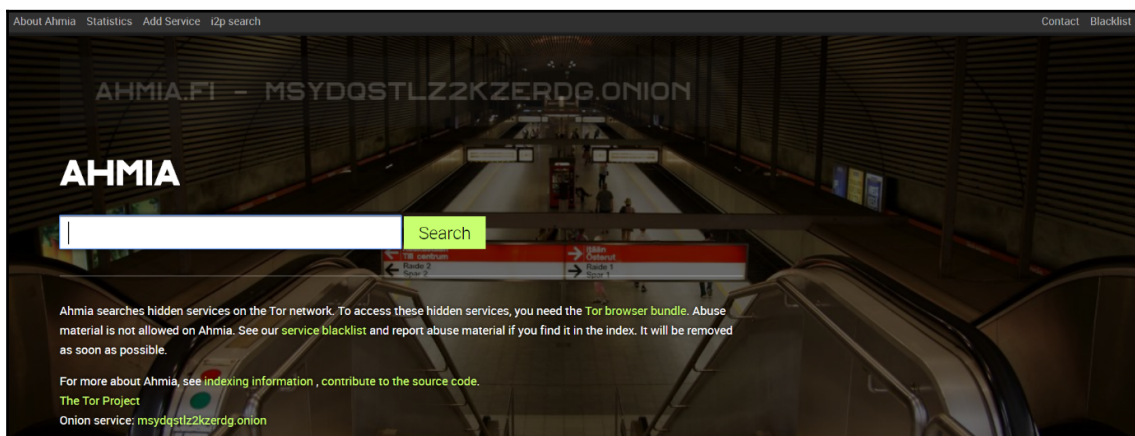
As I will discuss in Chapter 5, *Accessing the Dark Web with Tor Browser*, you can browse to the Dark Web version of Facebook, which was created to provide access to Facebook, in countries where it's blocked on the Surface Web. You can join online clubs and gaming groups, and basically do almost everything you might do on the Surface Web, just more cautiously.

Searching for information is not always as easy as Googling. But you can use Dark Web search engines, or rather indexes which will take you to the relevant sites, for example **Torch**:



TORCH search engine

Ahmia, is another Dark Web search engine , which blacklists any inappropriate or invalid data:

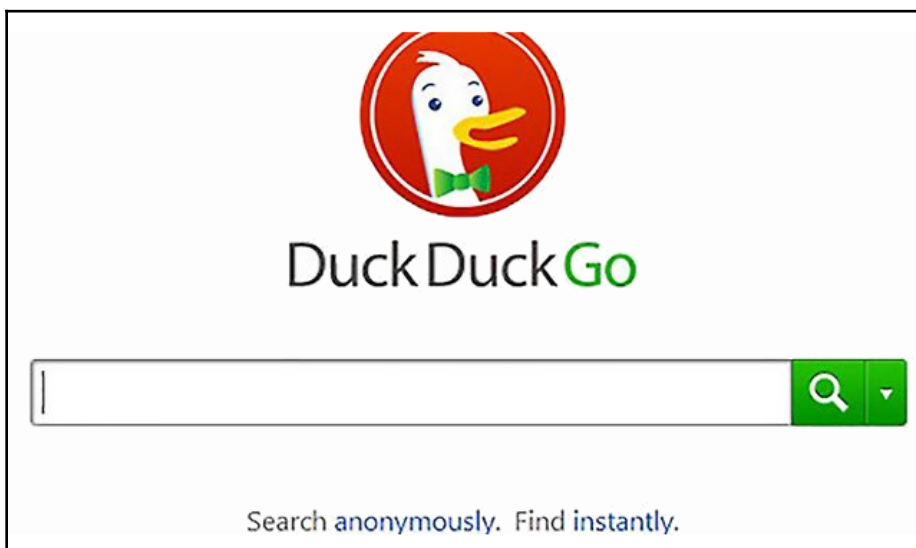


In the next screenshot, you'll be able to see another Dark Web search engine—**notEvil**.



notEvil search engine of Dark Web

DuckDuckGo is one of the most famous search engines, also used for searching on the Surface Web, since it doesn't retain search history or any other user activity.



Tor Links is a source for dark web links. Tor Links is user-friendly and organized. Drugs, digital goods, erotic, gambling, hacking, forums, media and more can be found here.

TorLinks | .onion Link List

Commercial Links

[Financial Services](#)[Services](#)[Drugs](#)[Physical Goods](#)[Digital Goods](#)[Erotic](#)[Gambling](#)

Non-Commercial Links

[Services](#)[Hacking](#)[Warez](#)[Erotic](#)[Forums](#)[Media](#)[Political](#)[Others](#)[Non-English](#)

TorLinks is a moderated replacement for The Hidden Wiki, and serves as a link or url list of Tor hidden services. Feel free to copy this deep web link list directory to your website to make others aware of the darknet. We regularly update the tor onion sites on this site.

Financial Services

[EasyCoin](#) | EasyCoin Bitcoin Wallet, now with free Bitcoin Mixer!
[WeBuyBitcoins](#) | Sell your Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and more
[HQR](#) | High quality euro bills replicas / counterfeits
[USD Counterfeits](#) | High quality USD counterfeits
[OnionWallet](#) | Anonymous Bitcoin Wallet and Bitcoin Laundry

^

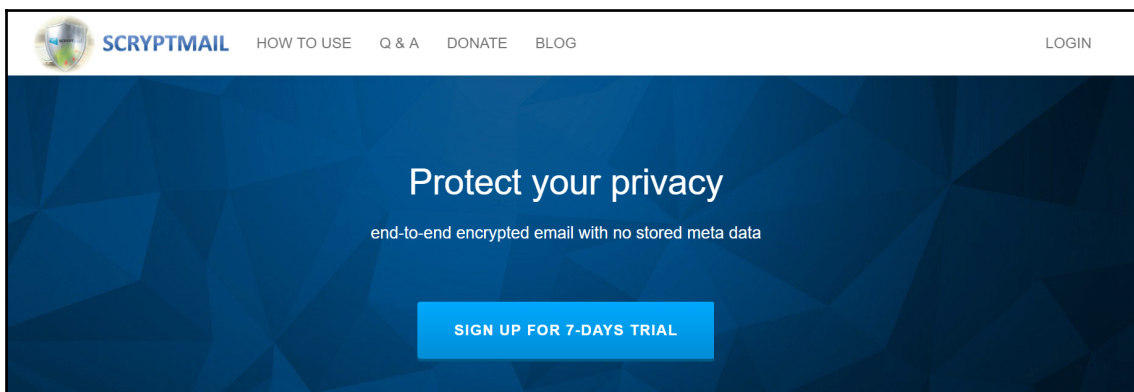
Services

Commercial Links

Commercial Links

The same as on the Surface Web there are multiple anonymous mail services. Some of them are:

- **Scriptmail.** It is free for 7 days and can be accessed on the Surface Web as well:



- **Bitmessage Mail Gateway:** It has Auto responder, Auto forwarder, broadcasting, two auto signatures and many more. Also, it is completely free.

[Register](#) | [Setup Guide](#) | [FAQ](#) | [E-Mail access](#) | [E-Mail settings](#) | [Terms and conditions](#) | [TOR access](#)

Bitmessage Mail Gateway

This is a service to connect Bitmessage with E-Mail without the need of any software. It allows you to use the Bitmessage network the same way you use E-Mail today.

Key Features

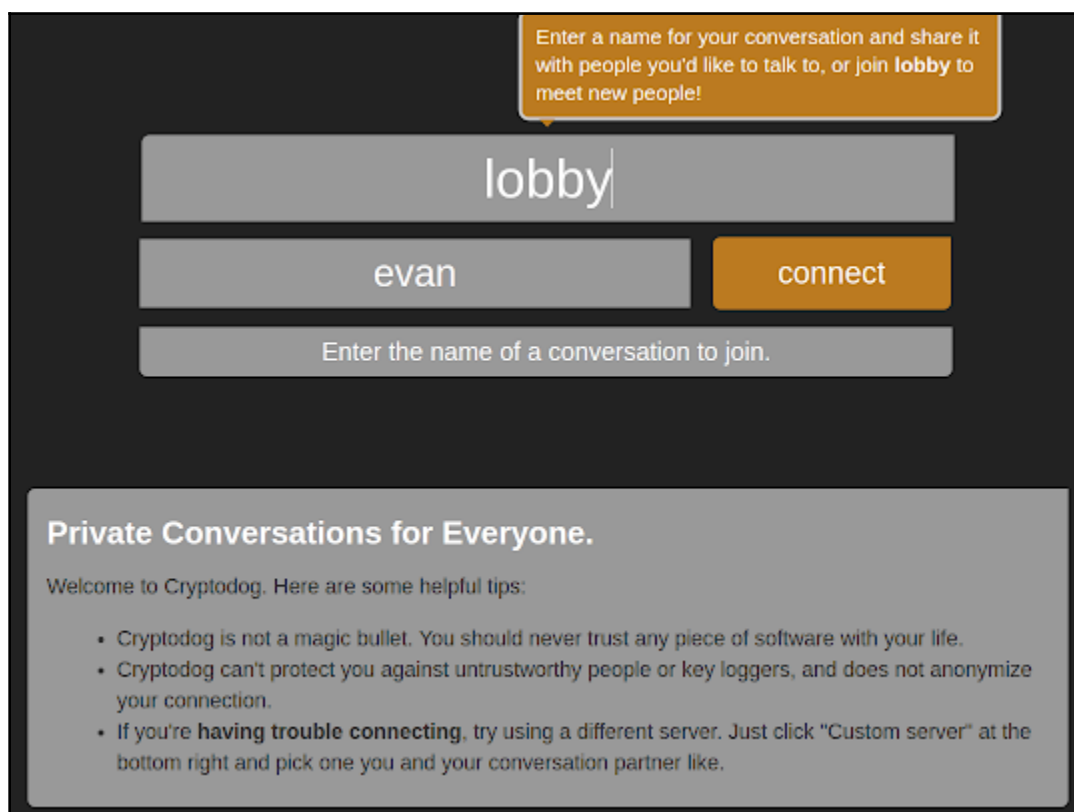
- It's completely free
- No advertisements anywhere
- No tracking with Google Analytics or other services at all
- Send and receive E-Mails from/to Bitmessage addresses
- Send and receive E-Mails from/to other E-Mail addresses
- Personal Bitmessage address
- Supports broadcasting
- Use the E-Mail client you are satisfied with and all its features (address book, spam filter, folders, rules, etc).
- Instant delivery (no [POW](#)) if your contact has an @bitmessage.ch address too.
- Server supports IMAP, POP3 and SMTP
- Easy readable alias address
- No Proxy or TOR required but TOR hidden service available (see [FAQ](#))
- Webmail Access from everywhere.
- Two webmail systems, one optimized for bitmessage compatibility, one for all E-Mail features (attachments, MIME, ...)
- Auto responder if you are away or want to set up a mailing list.
- Auto forwarder to an external address.
- Two auto signatures (Plain Text and HTML).
- Rules for automatic message filtering.

Deep web emails - Onion Mail

Onion Mail is another working anonymous email service provider at hidden web.

To create a new Onion Mail account, you need to click on **Download** option and then you will notice another window with a message **To create a new OnionMail account click HERE**. For more info about Onion Mail features and services, please visit Tor URL: (<http://it.louh1bgypgkts7.onion/>).

CryptoDog is a private chat server on the Dark Web:

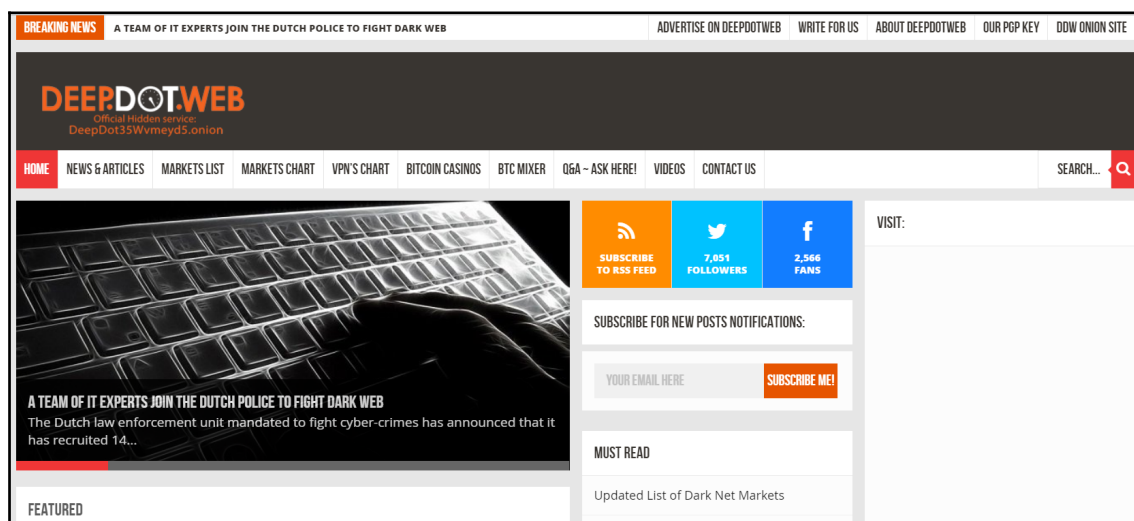


The screenshot displays the Cryptodog web interface. At the top, an orange callout box contains the text: "Enter a name for your conversation and share it with people you'd like to talk to, or join **lobby** to meet new people!". Below this, there is a large grey input field containing the word "lobby". Underneath the input field, the name "evan" is displayed in a smaller grey box, and to its right is an orange button labeled "connect". Below these elements is another grey input field with the placeholder text "Enter the name of a conversation to join.". At the bottom of the interface, a grey box contains the heading "Private Conversations for Everyone." followed by a welcome message and a list of three bullet points: "Cryptodog is not a magic bullet. You should never trust any piece of software with your life.", "Cryptodog can't protect you against untrustworthy people or key loggers, and does not anonymize your connection.", and "If you're **having trouble connecting**, try using a different server. Just click 'Custom server' at the bottom right and pick one you and your conversation partner like."

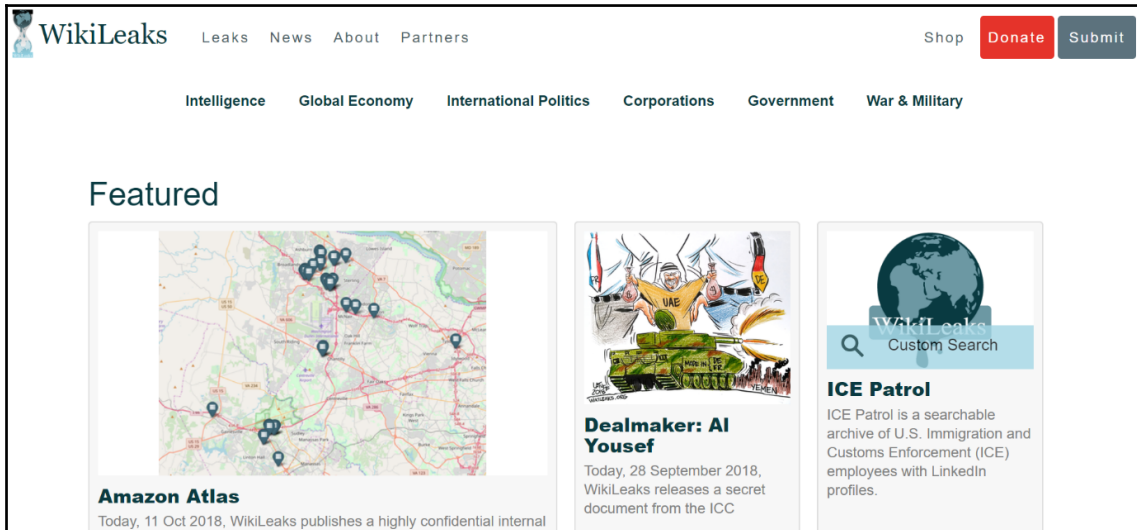
There are also many forums sites on the Dark Web, for example:

- Anonymous Forum
- Pedo Support Community
- Glazy2
- 8Chan
- Nnptchan
- HiddenChan

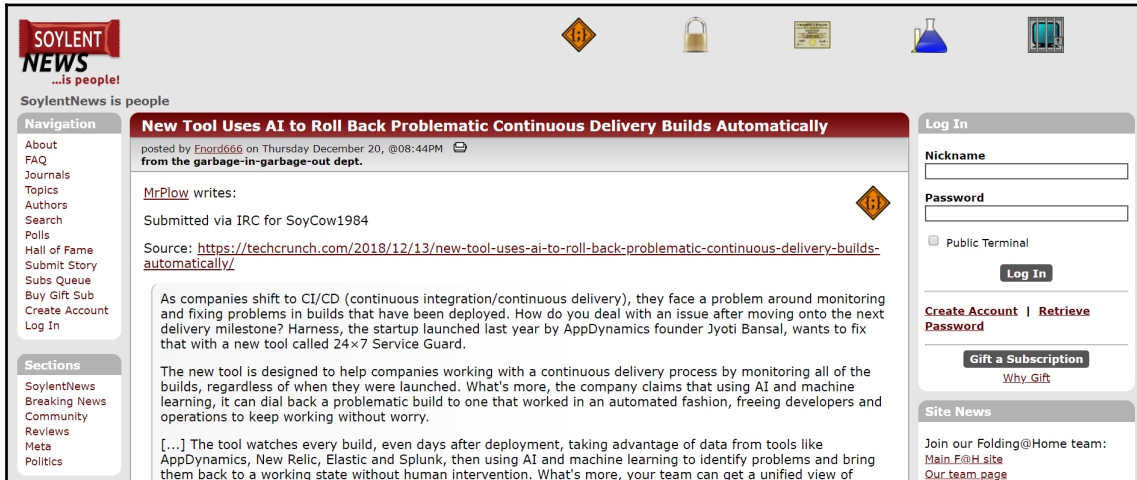
DeepDotWeb is a blog which covers the latest deep web news and other useful tutorials like how to buy drugs online, PGP tutorials, how to access dark web links, and more:



WikiLeaks is the infamous news leak site:



SoylentNews has content regarding multiple topics:



BitStore and Mobile Store sell mobile phones and related products.

Electronion or Electron shop are sites which offer electronic gadgets for sale.

Summary

The Dark Web has many uses. Some of them are benign and some are malevolent.

Part of the goal of this book is to expose you to them, so you will be better prepared and will be able to avoid problems or prevent them.

The important thing to remember is that you just need to be careful, take the precautions I will tell you about, and *keep your eyes open*.

Questions

1. Please describe what Privacy and Anonymity are.
2. What are the 3 main cryptocurrency transaction methods?
3. Please list 3 Dark Web search websites.
4. What uses are there for the Dark Web?
 1. Browsing
 2. Email
 3. Blogging
 4. Forums
 5. Financial Transacting
 6. Almost everything you might do on the Surface Web (including all the above)

Further reading

The following resources might be interesting if you'd like to delve deeper into the topics included this chapter:

- <https://www.thedarkweblinks.com/>
- <https://computer.howstuffworks.com/internet/basics/how-the-deep-web-works.htm>