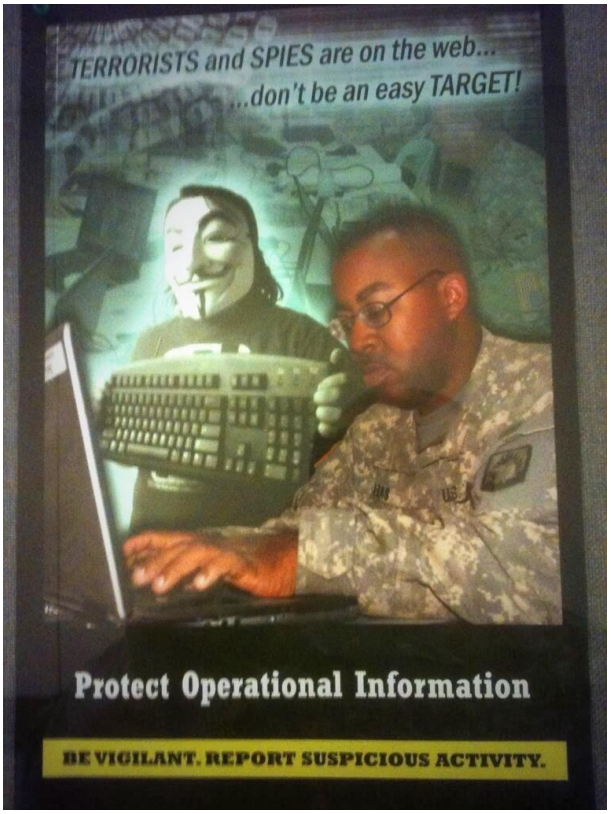


INTRODUCTION TO SECURITY SYSTEMS

Passwords, Email, Encryption, and More

ABSTRACT

As the world becomes more and more digitized, the possibilities for surveillance by the government, companies, or a malicious third party individual increase dramatically. It is only with knowledge of security protocols and the tools to make use of them that one can survive in the brave new world.

Peter Heft

Table of Contents

Contents

Part 1. Introduction

In light of revelations about the NSA's role in illegal domestic surveillance (x), and this terrifyingly hilarious photo inside a US army base coverphoto, downloads of anonymity programs and browsers such as Tor (The Onion Router) have skyrocketed as people become more aware of what the government is doing and what "privacy" actually means. In fact, usage of Tor is up by over 100% and the so called "Dark Web" has risen to the Scroll to bottom spotlight. This surge, however, has been met with a downside - a false sense of security. The aim of this post will be to share the methods I use to keep information private and methods that one could use to attempt to remain anonymous on the internet. (Later posts may, if the need arises, be centered around specific security aspects)

Now this being said, there are a few disclaimers:

1. The most obvious - I choose to share information about me on the designated page ***not*** because I do not know how to be secure, but because I am willing to share this much. I am also willing to stand by my convictions, thus I sign my name. That being said, incognito personas are fun and I maintain a few.
2. ***There is rarely, if ever, total security.*** Someone wiser than I once said "a false sense of security is worse than being unsure"[1]. The point of this post is to give you the tools to try to be secure.
3. These are just the tools I use, if you want to complain, use the comments section or, as will be linked to throughout the post, read some other article.
4. Finally, I am no expert in the academic sense of the word, rather, I am an enthusiast who wants to learn and share what he has learned. As such, don't take my explanations with the same rigor as you would Jacob Appelbaum or Bruce Schneier.

Part 2. Passwords and Managers

There is much discussion regarding password entropy and what makes for a good password. You have xkcd's analysis of password strength in issue 936 (fig. 2) arguing that random words as opposed to letters, numbers, and symbols make ***better*** passwords on the one hand, and Webroot's exact opposite analysis on the other hand. But before we discuss specifics, there is one rule that must be followed...***DO NOT USE THE SAME PASSWORD FOR EVERY ACCOUNT. EVER.***

This should be extremely intuitive but it isn't, thus I will provide an analogy. You install the same lock on your house, storage unit, car, and safe and you make one copy of the key. Now what happens if an adversary gets ahold of said key? They have access to your house, storage unit, car, and safe. Bam. Just don't do it.

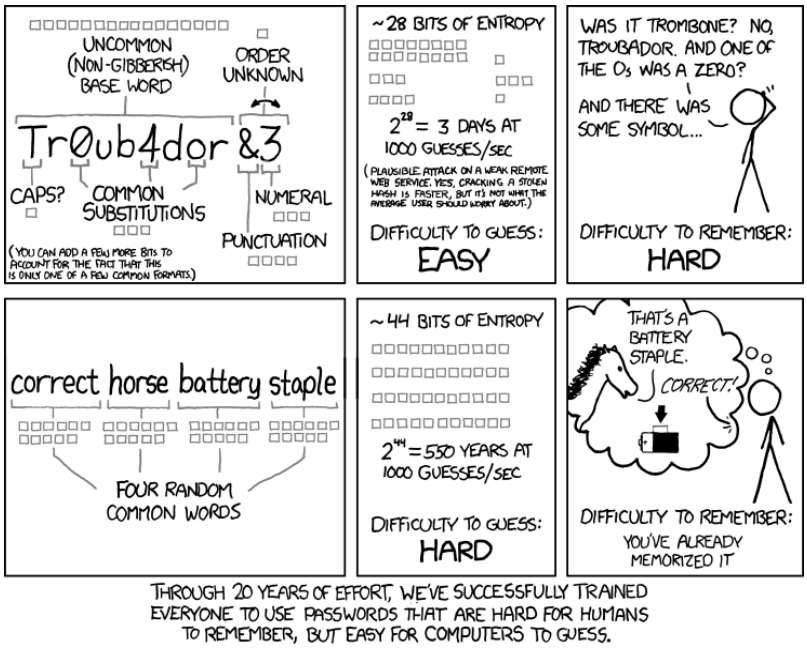


Fig. 2

But now that that's settled, let's talk more specifically. Personally, I subscribe to the Webroot model, that is, randomizing passwords. The reason for this is this is simple: words that are in the dictionary are subject to, able to be cracked by, a brute force attack much easier[2][3]. Hell, there are even forum threads dedicated to which dictionary is the best to pool words from! Now some of you may be thinking, "well I use a multi-word pass***phrase***!". Sorry, but the evidence indicates that that too, is not as secure as you think[4][5][6].

In contrast, the data suggest that randomized passwords are actually the strongest and will help in furthering the security of your accounts[7][8][9]. Additionally, this LifeHacker article directly explains everything above again, if I didn't convince you.

But all this begs the question...how in hell is one supposed to remember randomized passwords?? Well that's were a good password manager comes in! (And consequently, that is what the rest of this section will be on)

So what is a password manager? A password manager is, at it's core, a file that holds all your login information for any and all accounts that you store in it. For example, it may have your Facebook login credentials (*username, password, any notes).* Now for the security conscious individual, skepticism is natural here. Using a password manager raises two important questions:

1. How do we know this manager is secure and doesn't have a backdoor?
2. Why put all your eggs in one basket?

Before I tell you which manager I use and why, I will let LifeHacker answer question number two (note: their password manager is a different one than I use but the same principle still applies *my emphasis added*):

> Isn't this "all your eggs in one basket" stuff?
>
> Yes, it is, but it's a basket that is very well thought out and ***very firmly secured***. Someone would have to firstly obtain the file containing all the passwords exposed and secondly have your master password either disclosed, guessed or brute force attacked, none of which should happen if you choose one securely.
>
> Whilst having all your account details exposed at once is undoubtedly a very bad thing, ***the risk is infinitesimal*** compared to the chances of having it breached via website.
>
> Of course the other risk is that an as yet unknown vulnerability is found with the 1Password software. Certainly what we'd call a zero-day vulnerability (one that is not yet known), is possible. In fact there was one found in LastPass just last month and to their credit, they plugged that hole in no more than a few hours. And that's the point with professional products of this nature; their entire being is centred on offering a secure solution and if a vulnerability is found, you can be pretty damn sure it's going to be squashed very quickly.[10]

Now LifeHacker mentions their preferred password manager, 1Password. I do not use this program for a few reasons, first, it seems to be originally targeted toward Mac users (I use a PC), second, the program I use, I will argue, is far superior, and third, 1Password seems to not be open-source (there are a ton of benefits to open-source software that I won't get into now).

The program I use, and would highly recommend, is an open-source program called KeePass. KeePass stores all of your passwords and login information in an encrypted file that can ***ONLY*** be opened if you know the master password. This means that you just need to remember one password, the master. (Oh, and it has a built in random password generator)

Now we get to the first question, the security of the manager. I won't repeat everything that's on KeePass' security page but I will mention some of the more important security features (you can

read more in depth on their page). KeePass features a 256bit keysize AES* or Twofish** block cipher to encrypt the database, secure desktop mode to prevent against keyloggers, and encrypted process data which means that a memory dump would not reveal the master password. Additionally, it's completely open-source which means anyone can review the code and check to see if there are any backdoors and, guess what(?), none.

If you're still not convinced, I think the awards speak for themselves (these are a few):

- KeePass is the recommended password manager in the BSI CyberSecurity Recommendations BSI-E-CS 001/003 1.4 German by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik).

- Rated **Outstanding** and received **Download Pick** award of CNET Download.com.
- KeePass is on the **Best Windows Software** list on MakeUseOf.

So just in case anyone can't find the download page, here it is.

At the end, there will be a how-to guide on KeePass (among the other pieces of software mentioned, if a full how-to is needed).

Part 3. Browsers and Add-ons

This section will be about the browser set up I use to maximize privacy while still maintaining usability (note: This section will ignore Tor and VPNs, those are for another section).

Now let's all be honest here Mozilla's Firefox is objectively the best browser for security, flexibility, and customizability. Now that that's over with, let's talk more importantly, addons.

- The first add-on everyone should have is called **Adblock Plus.** It's a free add-on that, as the name implies, blocks advertisements from websites. While it's not perfect, there's a reason it's number one on Mozilla's most popular list. Just navigate here and click "+Add to Firefox".
- Next we have **DoNotTrackMe.** This free add-on sends messages to websites that you don't want to be tracked as well as blocking tracking attempts by third parties. To get it, head here and click the green button. (Alternatively, this can be replaced with **Ghostery** which is functionally the same, yet it does have a better UI. To get that, head here)
- The next one comes right from our friends at the Electronic Frontier Foundation and it's called **HTTPS Everywhere.** This is probably my favorite add-on and with good reason: it forces your connections to websites to be routed through the encrypted HTTPS protocol as opposed to HTTP. There are tons of reasons why HTTPS is good but basically all you need to know is that, if used properly, it encrypts the data going to the site as well as verifies the integrity/security of the site. To get this add-on, head over to the EFF page here and click the "Install in Firefox" button.
- Next is another one of my favorites, **Web of Trust.** Web of Trust is a pretty fantastic add-on that has saved my ass on countless occasions. Web of Trust works like a crowd-source type thing where websites are rated by users according to *trustworthiness* and *child safety*. Additionally, it allows users to comment about specific websites giving you more information. All this comes in the form of a little circle in the upper corner of the address bar that is either *green, yellow, or red.* (Green indicates it's probably safe, yellow is meh, and red is most likely un-safe) What's more, when you Google something, the same circles will show up next to the results showing you which sites are good, and which aren't. And if that wasn't enough, if you accidentally get redirected to a "red" site, it automatically stops the connection and ASKS you if you want to continue. So with Web of Trust, you don't need to worry if "awesome-free-movies-and-software.com" is a good site or not... To get this add-on, head over here and click the green button. (I can't stress this enough, this is probably the best add-on in existence, there is one downside however***)
- Next there is one called **Best Proxy Switcher.** I do not use this one because I use a VPN, but this has good reviews and is basically a proxy add-on to hide your IP address. You can get it here.
- The next one is a just there - it's called **NoScript** and it blocks Java Script from running. This can either be good (for privacy), or a pain in the ass (if you go to websites that use lots of Java). I personally don't use this one, but it's an important add-on for security. Get it here.

The next few are just some aesthetic add-ons/how I have my browser set up. You can ignore these if you like but they are just aesthetic add-ons.

- There's a nice add-on called **Profile Switcher** that allows you to switch between configured Firefox profiles. (x)
- Then there's **Omnibar.** This makes the entire address bar a search box AND address bar, much like Google Chrome. (x)
- Next is **Speed Dial.** This allows you to configure quick links to your favorite websites that are easily accessible via a new tab (Ctrl+T). (x)
- Finally, there's a love it or hate it add-on: **Tree Style Tab.** This basically takes all your tabs, and instead of having them lined horizontally, they are arranged vertically in a tree layout where each new tab opened opened within a tab creates a new "leaf". (x) Fig. 3

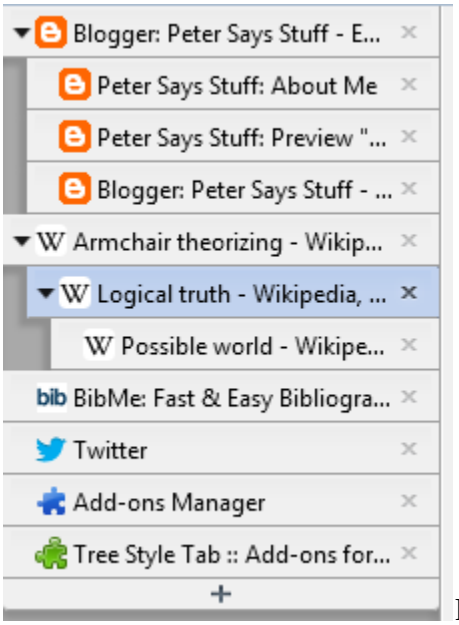


Fig. 3 - This is just a demonstration of what **Tree Style Tab** looks like. There is much much more you can do with it, but this is located on the side of my screen (I can adjust the width).

If you want more, you could read this article from LifeHacker.

Part 4. Email and Clients

So here we get into tricky waters because, since the shutdown of Lavabit, there really isn't a great "private" email provider. In fact, one author went so far as to say "[e]xpecting privacy with email providers is extremely naive". We now have three tiers, the paid/invite-request private, the free "private", and the NSA on speed-dial "private". I have no experience with the first tier thus I will only briefly touch on them.

Paid/invite-request

In this section, there are a few options to choose from. There's Riseup which "provides online communication tools for people and groups working on liberatory social change". There are two things I see with this, first, there seems to be no great verification that it's totally private nor does there seem to be information about the data purging/handing over policy (their privacy policy doesn't tell you much), and second, it's a request service which means you have to explain why you should get an account and how you fit in with a group that "believes in direct democracy, anti-sexism, anti-racism, anti-capitalism, self determination, local autonomy, ecology, and communal economics"[11].

Next there's Autistici/Inventati which, from what I can tell, operates similarly to Riseup in that you need to request an account OR you need to pay for one. When comparing these two, I'm inclined to say A/I is better.

And finally, there's Kolab. If I were to pay for a service, it would be this. The reasoning is simple, the servers are all physical in ~~Sweden~~ Switzerland(very good privacy laws) (kind reddit user sisquo corrected me, it's not Sweden), no data crawling, you can export your data, and it's open-source (to an extent). If you want more information than what I can provide, since I have not used Kolab, you should read Gizmodo's article here.

Free "Private"

This tier only includes one service because, quite frankly, this is the only one I can find that seems semi-legitimate as well as the one I have some experience with. Hushmail. Hushmail allows for PGP encrypted emails if both parties have a key, or password encrypted emails if only one does. Additionally, Hushmail supposedly keeps all the information private and doesn't reveal anything...however that has turned out to be false back in 2007.

So where does that leave us? Well, with the

NSA on Speed-Dial Providers

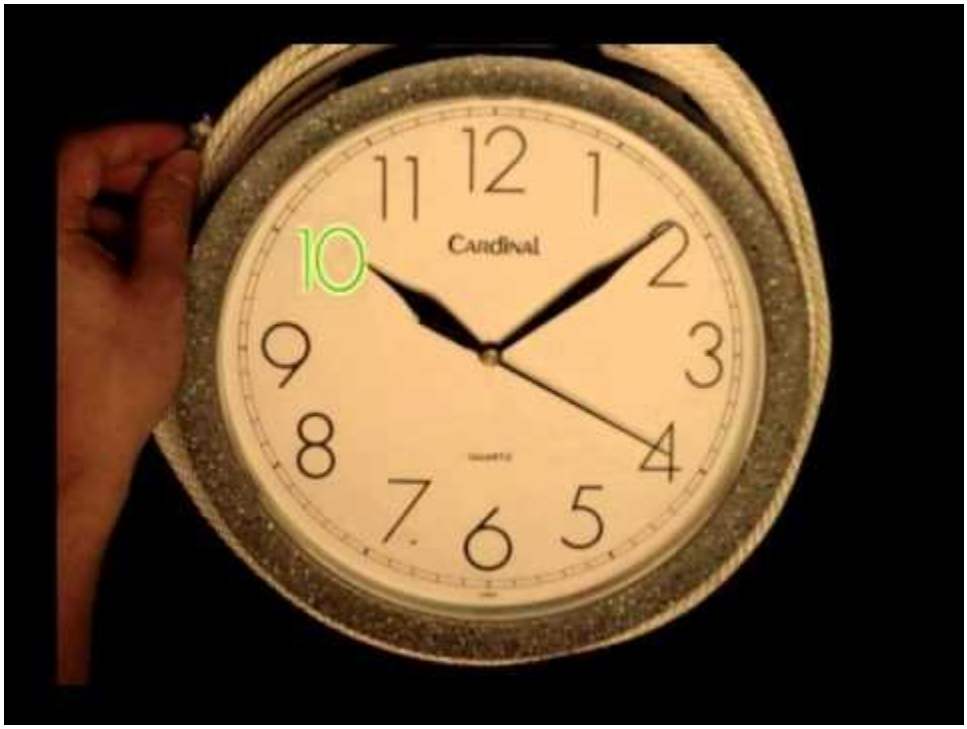
These services include GMail, Yahoo!, and Hotmail among others. Now while these are in no way secure ***as they come***, as shown time and time again, they are convenient and can be made secure[12][13][14]. Now while these are insecure "out of the box", with a good email client and some knowledge of encryption, you can maintain some semblance of security. (If you really

want to go incognito, you could use Pidgin with OTR enabled or use some good ol' fashioned IRC...but I won't be talking about that)

So what can one do about securing these seemingly insecure email systems? Well the first thing any netizen would want to do, after picking one of the aforementioned services (I use GMail), is to download an email client. A client is something that allows you access your email from your desktop as opposed to logging in to gmail.com. This has numerous benefits ranging from customizability, to ease of use, to encryption. There are a number of different clients, from eM, to Zimbra, to what I use, Mozilla's Thunderbird. (For the purpose of this and the how-to set it up and use encryption later on, I will be using Thunderbird.

So once you've picked an email provider and a client, you can scroll on down to the "how-to" section and pick up from there. I will also show how to encrypt your mail.

However, before you decide you want to encrypt your email, I suggest, at the very least, watching this video on Public Key Cryptography (specifically, the Diffie-Hellman Exchange):



(Some extra reading if you want, here is an article about other services and a forum thread)

Part 5. Data Encryption

Now this is my favorite part, because we get to be sneaky. Data encryption is an interesting game that comes in many flavors. You can either encrypt specific files, create encrypted volumes (that is, a place to store files), or encrypt entire partitions. This is how this section, and the relevant how-to, will be broken down: I will discuss the different pieces of software for each operating system (OS X, Linux, and Windows 7 and 8.1 *pro*), and then in the how-to show the creation of an encrypted volume with the software I use. An important note, the programs I will be talking about are, with the exception of full disk encryption on Windows 8.1 Pro, not the proprietary programs people throw at you.

OS X

When using a Mac, and granted I don't have much experience, there aren't a massive number of quality open-source encryption options available. The two big ones are EncFS and TrueCrypt. I have very little knowledge about EncFS, apart from some reading about Android encryption, so I cannot really comment either way, but from what it seems like, it's mainly a tool for encrypting specific files *as opposed to* encryption volumes or partitions. (If I'm wrong, please let me know)

Truecrypt on the other hand, is my program of choice and I will write more about it in the Windows section as well as the how-to. But basically, it provides the ability to create encrypted volumes (basically folders that can't be opened without the key), hidden volumes (if you want plausible deniability - read here), partition encryption, hidden partition encryption, full disk encryption, and hidden full disk encryption.

So as much as I'm a Mozilla fanboy, I'm a TrueCrypt fanboy as well.

Linux

There are significantly more options regarding encryption when it comes to Linux, but a lot of it will depend on the distribution you are using (eg. Ubuntu, Fedora, etc). That being said, there are still some programs that stay the same. There is EncFS, Cryptsetup working off LUKS, and TrueCrypt, among others. I have somewhat more experience with Linux and thus I can say that LUKS based programs seem solid, however I always err to TrueCrypt. But, if I understand correctly, Cryptsetup comes native with some Linux distributions and is obviously open-source so I'd be inclined to say it would work *more* seamlessly with Linux.

Windows 7 and 8.x

This section will be divided into three mini parts, one on Windows 7, one on Windows 8, and one on Windows 8.1 vs. 8.1 **pro**. But before that, I need to explain the distinction between full disk encryption, and volume or partition encryption. Full disk encryption is where the entire hard drive of a computer is encrypted. This means that when one turns off the computer and turns it back on (or if it goes into hibernate), one needs to re-enter a master password before ***any*** information is available. In contrast, partition or volume encryption encrypts ***part*** of the hard

drive. This means one can still boot normally, but some files cannot be accessed without mounting them by entering the master password.

Windows 7:

If you're still rocking Windows 7, kudos to you. I've come to hate Windows 8 *less*, but I still miss 7 and the hardware associated with it. (The hardware question is only really relevant if you're laptop is a year or so old) If you're using Windows 7, there are a few options instead of the proprietary programs. You have, again, EncFS, DiskCryptor, and of course, TrueCrypt, among others. The only real difference I can tell between DiskCryptor and TrueCrypt, is that the former stores passwords in a cache while mounting as well as auto-mounts encrypted flashdrives whereas TrueCrypt can be configured to do the aforementioned but it also has the hidden volume ability. So yet again, I err to TrueCrypt.

Windows 8:

If you're running plain Windows 8 (you can check this by going to Control Panel>System and Security>System or by clicking the Windows Button + "c" to get the Charms menu, hitting "settings", and then "PC Info"), there is no option for full disk encryption (there is hope). The reason for this is the way the operating system boots and the type of hardware that Windows 8 is optimized for (more info here). So for the time being, regular Windows 8 offers no option for full disk encryption, neither proprietary or open-source. That being said, one can still create encrypted volumes or encrypt large partitions, but not the entire disk ***including*** the boot sector. But Microsoft decided to be sneaky and offer the following...

Windows 8.1 PRO

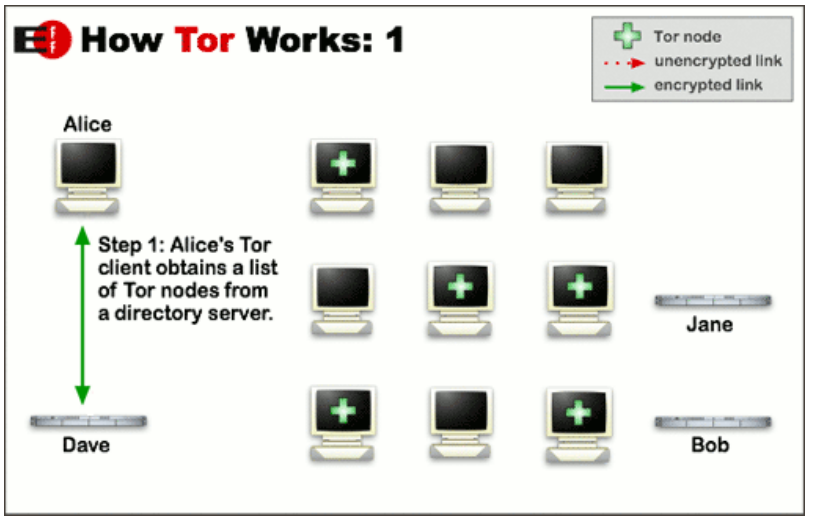
There's a free upgrade to 8.1 that is cool, except it is the same as before in that it offers no option for full disk encryption. The only way to get this is to pay, if I recall correctly, $99 to upgrade from 8.1 to 8.1 PRO. With 8.1 Pro, you then have the option to use Microsoft's Bitlocker, or Symantec's encryption. In the face of these two options, I would opt for Bitlocker for full disk encryption, and TrueCrypt for partition and volume encryption. That being said, we just have to wait. According to TrueCrypt's "Future" page, it will include "Full support for Windows 8" as well as the "Ability to encrypt Windows system partitions/drives on UEFI-based computers (GPT)"!!

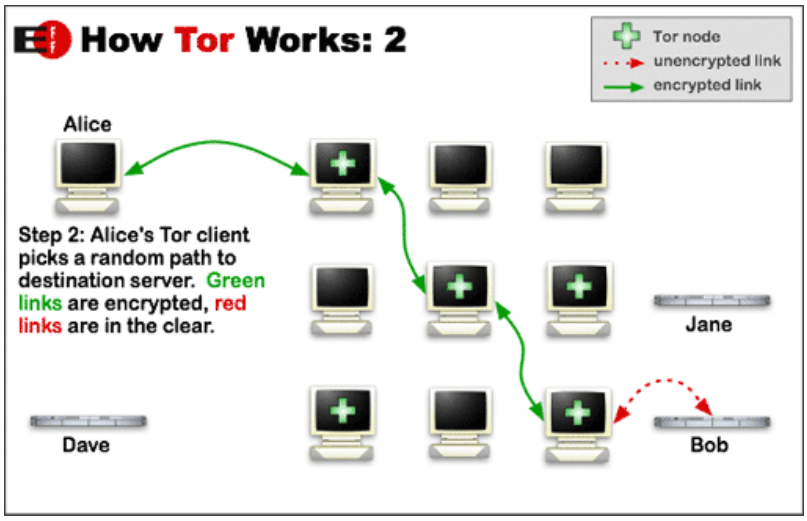
Part 6. Anonymity

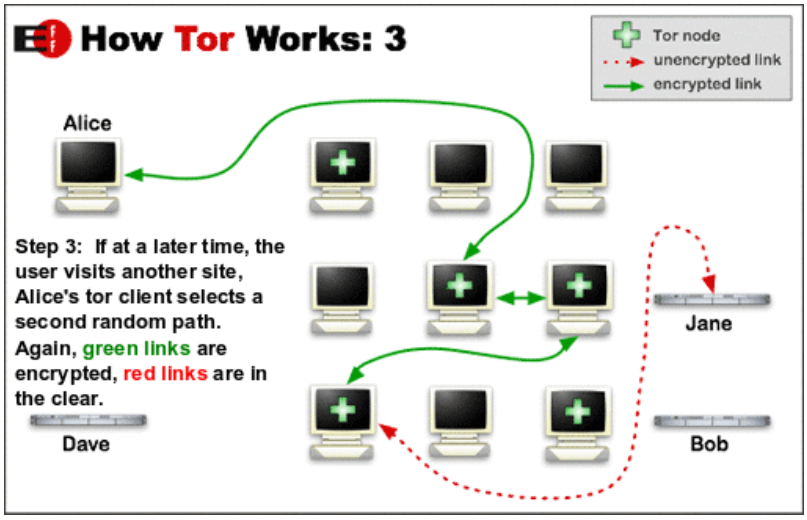
Now before I go into anything here, an important point must be made: it is very very difficult if not impossible to remain 100% anonymous on the internet. Human error mixed with potentially bad code makes the likelihood of a slip up almost certain...it's the magnitude that matters.That being said, there are tools one can use to, if used correctly, ensure near perfect anonymity. This section will be divided up into three sections as well, Tor - It makes you cry, Tails - The 007 of OS', and VPNs.

Tor - It makes you cry[15]

Tor is a world famous anonymity network that was, ironically enough, funded by the DoD back in 2002 when trying to work with so called "onion routing". Tor, if used properly, allows one to remain almost entirely anonymous (granted, there are attack methods but those are very difficult and the Tor busts have been because of human error, not police skill). The way that Tor works is, basically, by sending bits of your search that are encrypted to different computers, called relays, around the world, bouncing back and forth so the original source cannot be traced, until the data finally arrive at an exit node. At this node, the data are sent to the site in question and your results come back. The Tor Project actually explains this nicely (and better than I can) with three images shown below:



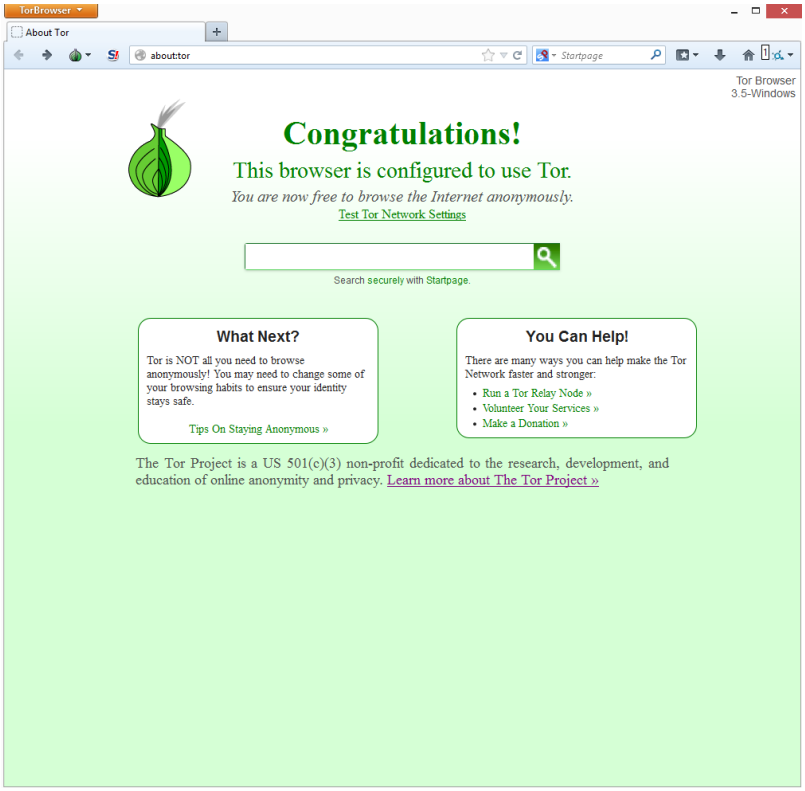




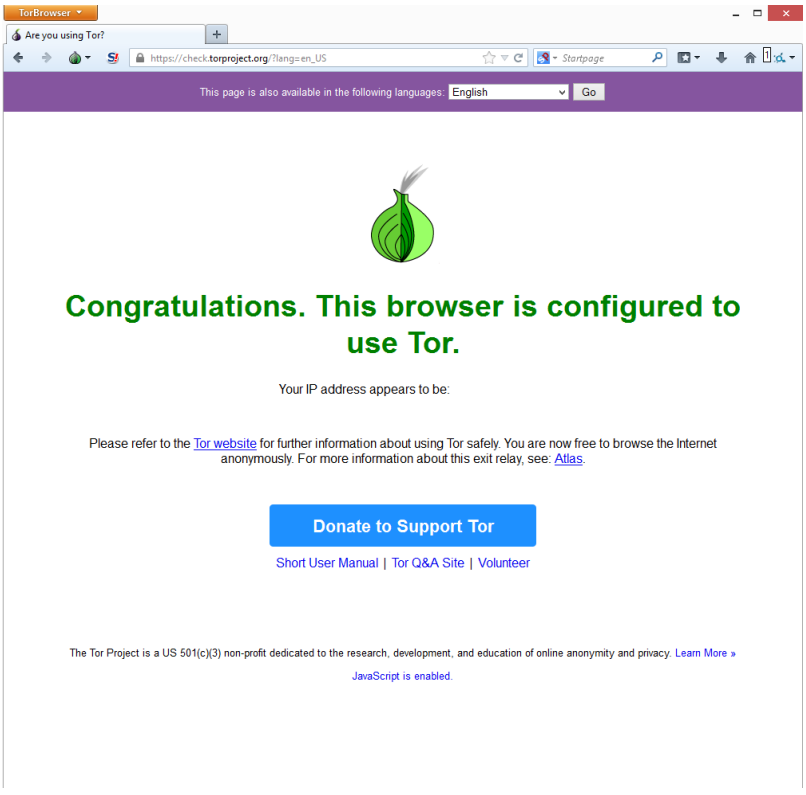
What makes Tor special is the fact that it is able to circumvent censor, access hidden sites, and most importantly, help users remain anonymous. Basically, the NSA hates Tor.

Using the Tor Browser Bundle is relatively straight forward and doesn't need a special how-to, I can explain it here. You navigate to torproject.org and click the giant button that says "Download Tor". This will take you to the Browser Bundle page located here. From here, you click the button that says "Download Tor Browser Bundle" and it begins downloading as .exe file. Once done, double click the file and it should extract itself (**note where it is extracting to**). Once extracted, navigate to the extraction directory, for me it's the desktop, and open the newly created folder called "Tor Browser". Within this file, you see an application that says "Start Tor Browser", double click this. From here, a small program called Vidalia starts and that sets up the connection and a browser opens. You will either see one of two pages indicating success (if it fails or you're not connected successfully, it will tell you).

You will either see this:



or this (IP redacted):



Once you see that, you should read up on the documentation here and familiarize yourself with the security of Tor.

Tails - The 007 of OS'

Tails, the self-described "Amnesic Incognito Live System", is an entire operating system built around the Tor work. It is a Debian based Linux system that routes all outgoing connections through Tor. As is indicated by the description, it is what's called a "live system" which means that it boots off a CD-ROM or Flashdrive and runs on your computer instead of the operating system (temporarily). When using Tails, nothing is saved to the hard drive, only to RAM, and that gets erased as Tails shuts down (or over time due to memory loss). The main issue with tails is what's called a "cold-boot" attack, but for most people's uses, this is a non-worry. If you stick around until the how-to section, I will show you how to make a Flashdrive bootable so you can run Tails anywhere.

As with Tor, it is very important to read the documentation, specifically, the "about" and "warning" pages.

VPNs

VPNs, or Virtual Private Networks, are ways to help anonymize your traffic while not sacrificing speed. VPNs work by creating an encrypted tunnel to a specific server and then from said server to a specific website. This server is often public which means many people share the same IP address (the server's) and thus you gain anonymity by blending in. For a more indepth explanation, I suggest you watch *Eli the Computer Guy's* video on VPNs over here. There are many other reasons one would want to use a VPN (such as getting away with Torrenting or bypassing filters), but the focus of this post is privacy. If you want a more extensive list, there is the following article. If still not convinced, the following one minute video is quite good.

Now most quality VPNs are not free, they cost a monthly fee that can be paid as a yearly thing, but this is usually pretty cheap. The VPN I use, and highly highly recommend, is called Private Internet Access and costs $6.95 a month, or $39.95 a year. That may seem like a lot, but it is well worth it. Private Internet Access has over 700 servers in 10 countries and is always growing which means there will be very minimal speed lose. What's more, configuring Private Internet Access to work on your iPhone or Android is easy.

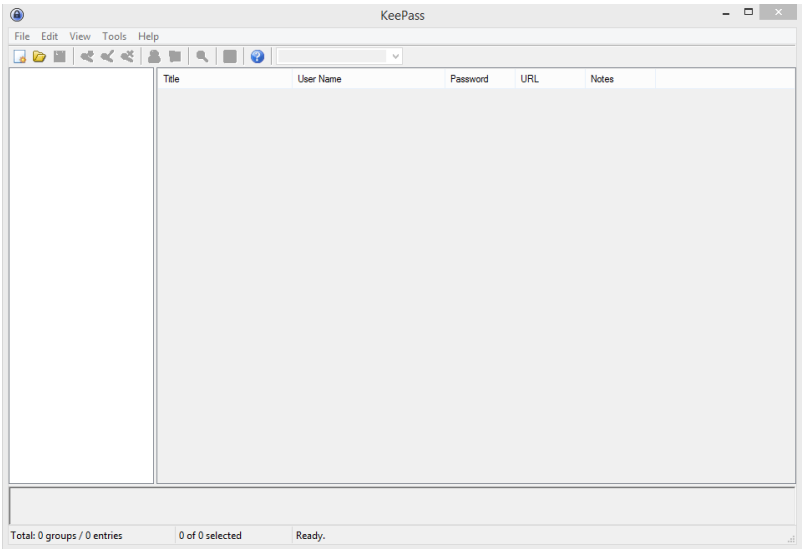
I say, shell out the money, it is well worth every penny. (There are free VPNs, but I'm skeptical of security as well as speed. If you want, you can read more here and here.)

Part 7. How-To's

So here we get to the fun part, where I have to take a ton of screenshots and write how-to guides! This section will be organized as follows: **KeePass, Thunderbird w/ PGP Encryption, TrueCrypt, and Tails.**

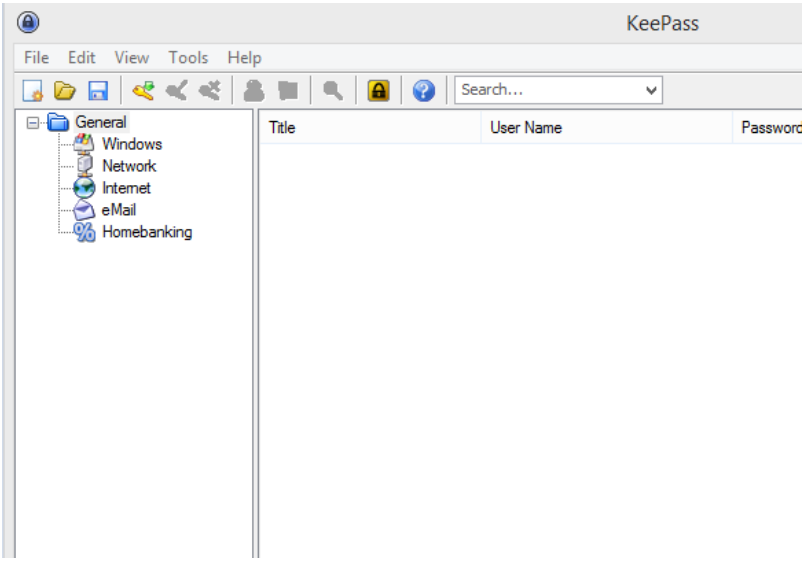
KeePass

The first step is to head over to KeePass' download page and download either edition. It will begin to download a .exe file...wait for it to finish. Once done, double click the installer and go through the normal installation steps. From here, I will show you how to create a database to manager your passwords. Once installed you will see Window that looks like this:



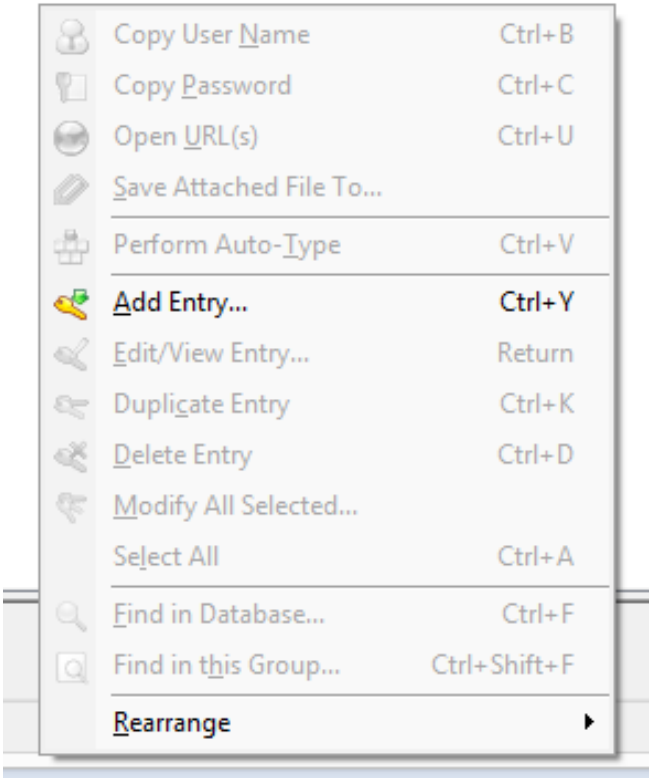
From here, you will want to click "File", the "New" (Ctrl + N). You will get a prompt to set a master password. This is really the only password you need to remember, but it also needs to be very strong. So I recommend you either use a generator like this, or think of a very good password (see references in the password section). For the sake of this tutorial, I will use the password "password". The screen looks like this:

You're asked to repeat the password, do that. Following that, you get the main hierarchy page where you can start to create folders and subfolders - this is what the default layout looks like:

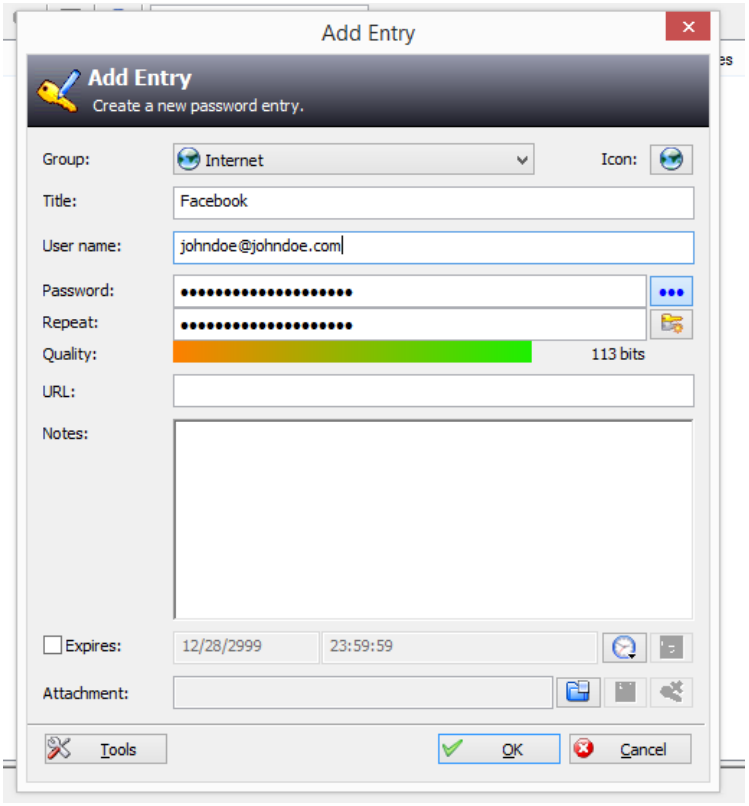


If you don't wish to use any of the premade groups, you can create your own by right clicking tree window, and pressing "Add Group" (you can also add subgroups, etc). For the purpose of this, I will just be using the premade "Internet" subgroup.

When you're ready to create an entry, click the subgroup, in this case "Internet", and then right click in the blank space, this is what you see:

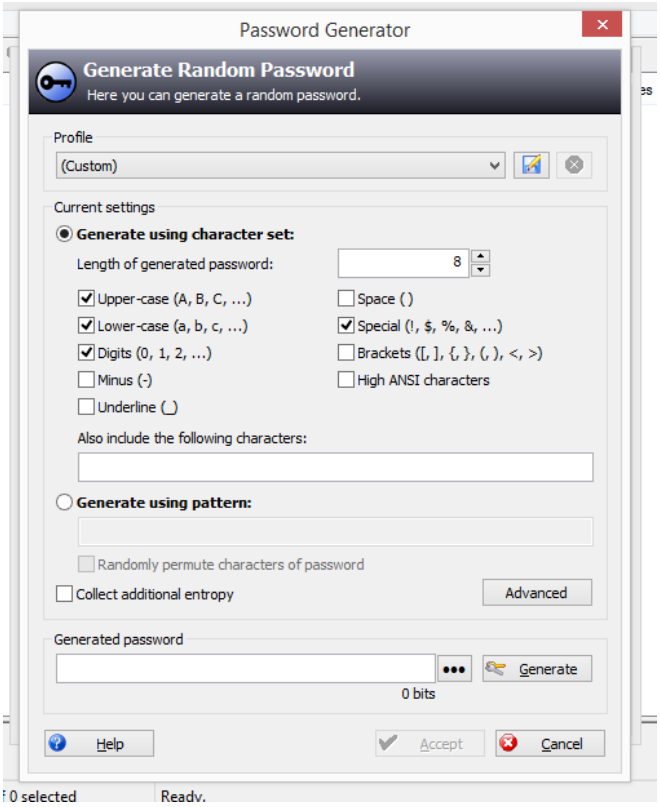


Hit "Add Entry". The Window that appears is where you place all the info needed to log in to whatever site you're creating an entry for (for the purpose of this tutorial, I will be using a fake Facebook account). The following image shows the screen with the title I entered as well as the username. You will see a long password that is bubbled, ignore that, it's a default random password that you can change:

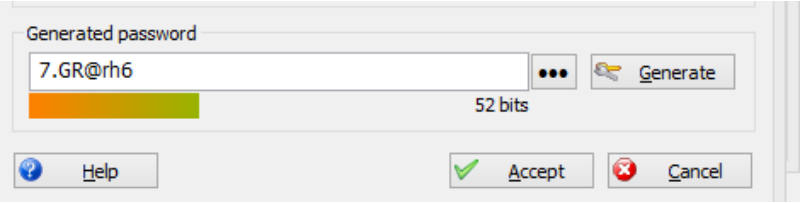


Next is the password creation step. If you click the button with three dots next to the password field, it will reveal a string of characters, in my case, it was "HPnZWgWDMscIaueZ2X8j". This is a random password that is automatically generated. You can do one of three things here: keep this random password, delete it and type your own, or use KeePass' generator. (***Obviously if you've already created an account somewhere with a specific password, delete the random one here and type the password you used when creating the account.*** For example, if johndoe@johndoe.com's Facebook password is "password", that is what he would type)

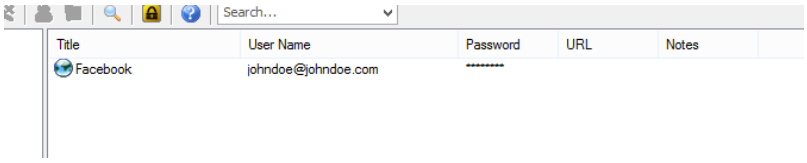
The latter is what I will show. To use the generator, click the button **right below** the dots. It takes you to the following screen:



There are a ton of options you can change here that will massively increase the security of the password, but I'll leave the more complex settings (like "Collect additional entropy") for another tutorial, the things already checked are fine. However, if you want, you can change the length. I'm keeping it at 8. Click the "Generate" button and you will see a password appear:

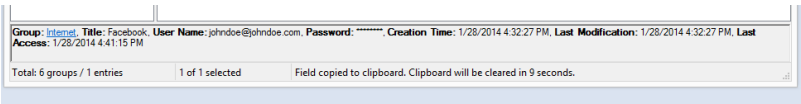


From there, click "Accept". You are then returned to the previous page and the random password that was pre-created, is replaced with the one you just made. Here, you can type any notes you want, or when you're done, click "OK". Now you should see your first entry!:



But the question is now, how do you use it?

Well, you navigate to whatever site you created it, say Facebook, and type in your username (you should have that memorized). Then, in KeePass, if you double click the password that is stared out, it copies to your clipboard ***for 10 seconds***. This means that if you hit Ctrl + V or "Paste" in the next 10 seconds, the password will be there:



Within this interval, go back to Facebook and paste the password into the login box and log in! If you run out of time, simply go back and re-do it. Alternatively, if you single press the entry in KeePass so it's highlighted, and then hit "Enter", it will open up the "Edit Entry" menu. From here, you can simply press the three dots and reveal the password. You can then copy it directly from there. Two things to note: first, **copy, not cut**, and second, this has no time limit which means that it will stay in your clipboard until you copy something else. I recommend the first way.

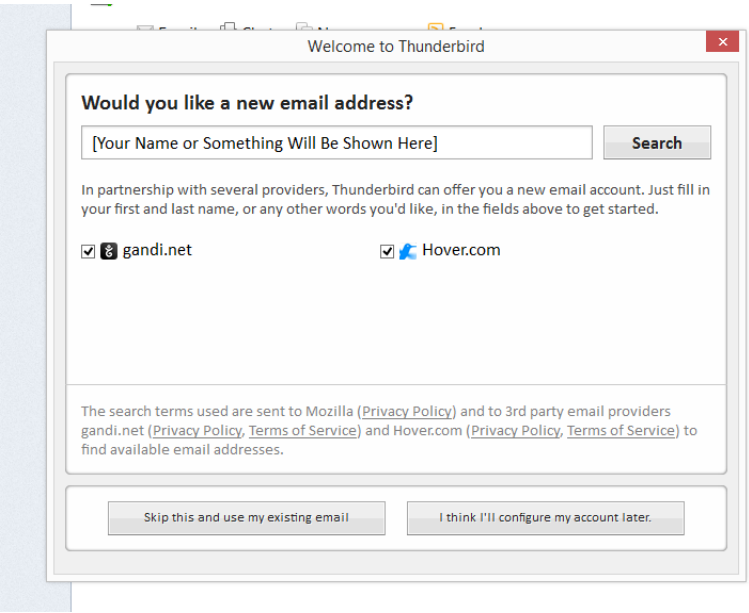
Finally, you need to actually save the file. What KeePass does it stores all these entries in a database file which means that, just like when editing a word document, you must ***always*** save. To do so, click "File" and then "Save As" and save it to your desired location.

Important note: Make sure you have a backup of the file (it's called database.kdb by default, but you can change the name)!! If you lose the file, you lose all your passwords.

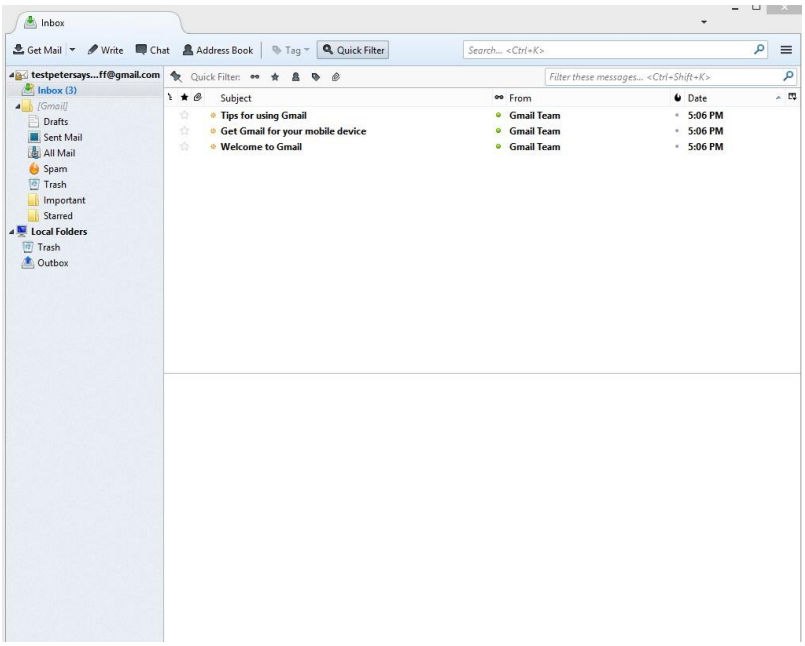
If you want to re-open the database, navigate to where you saved the file, double click it, and reenter your master password. If you enter the wrong password, nothing happens and your data are secure. Congratulations! You've just created your first KeePass database!

Thunderbird With PGP Encryption

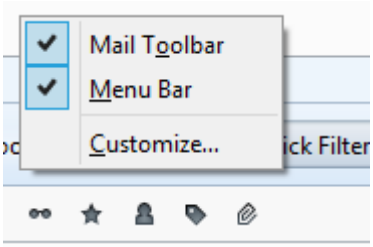
The first thing to do with Thunderbird, is navigate to the download page here and let the file download. Once it's done, double click the installer and install as normal. Once Thunderbird is successfully installed, you will want to open the program. Opening it for the first time gives you the following window:



You'll want to click the "Skip" button and use an account you already have, be it GMail, Yahoo!, etc. The next page is where you will input your login credentials. This part is very straight forward and doesn't need much explanation. Once that is done, wait for Thunderbird to sync up your mail. Once complete, you get a screen like this (this is a demonstration, not my actual account):

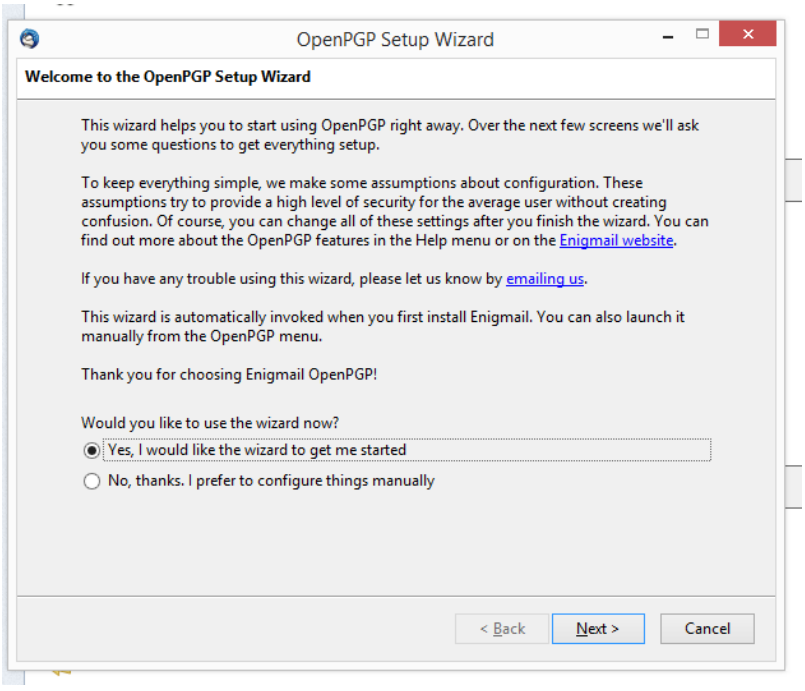


The next step is to right click the top panel and make sure "Menu Bar" is ticked:



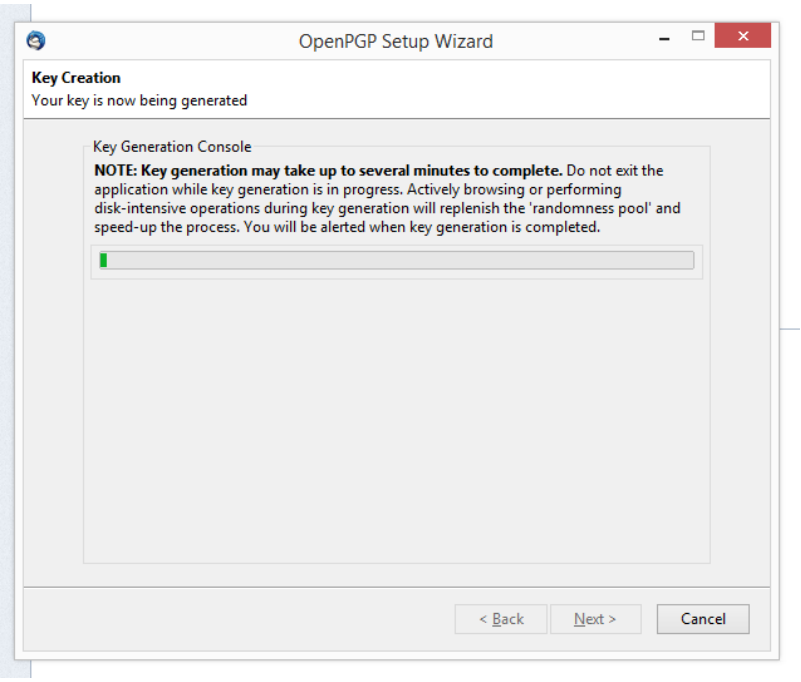
Once done, hit "Tools" and then "Add-ons". That will take you to the following:

Once there, search for **Enigmail**. Hit "Install" and then "Restart Now". Once Thunderbird reopens, you will see an OpenPGP wizard, this will let you set up your public and private key:



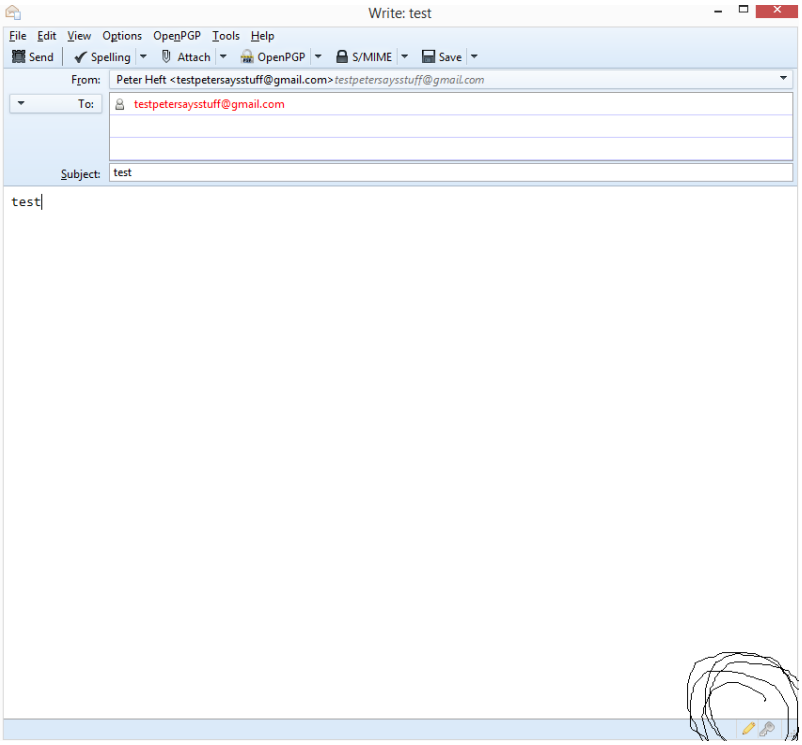
Click "Next", "Next", "Next", "Next", and then tick "I want to create a new key pair..." and hit "Next". You then get to a password screen. You should type in a password you can remember,

because this will be used to sign and encrypt all outgoing emails (if you choose). Enter it and click "Next". You should see the following window showing you it's working:

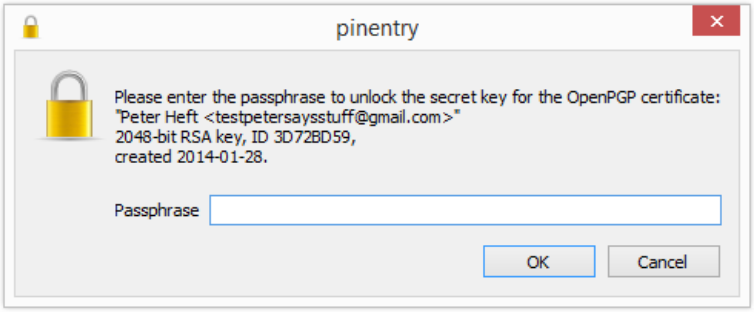


You will then get a pop-up that asks you if you want to generate a revocation certificate, do this and save it somewhere safe!

Now you have OpenPGP installed! I recommend you send an email to yourself first to test, if you do that, this is what you'll see (Notice the circle in the bottom right - the highlighted pencil indicates that you are signing the message, the un-highlighted key indicates that it won't be encrypted. You can press either and to change the status):



When you hit send, the following pops up, enter your password and all is well:



But that's only half the battle, you now have a public-private key pair, but you need to share them! (Well, just your public key) Navigate to your desktop, or search your computer, for a program called "Kleopatra" and open it. Kleopatra is a PGP key database that holds your information. This is where you will export your public key from so others can send you encrypted emails. From here, you will want to right click on the email you just used (I'm not showing screenshots because all my keys are here) and hit "export certificates". You then want to save them somewhere safe. If you open the certificate in Notepad, it starts off something similar to this:

-----BEGIN PGP PUBLIC KEY BLOCK-----

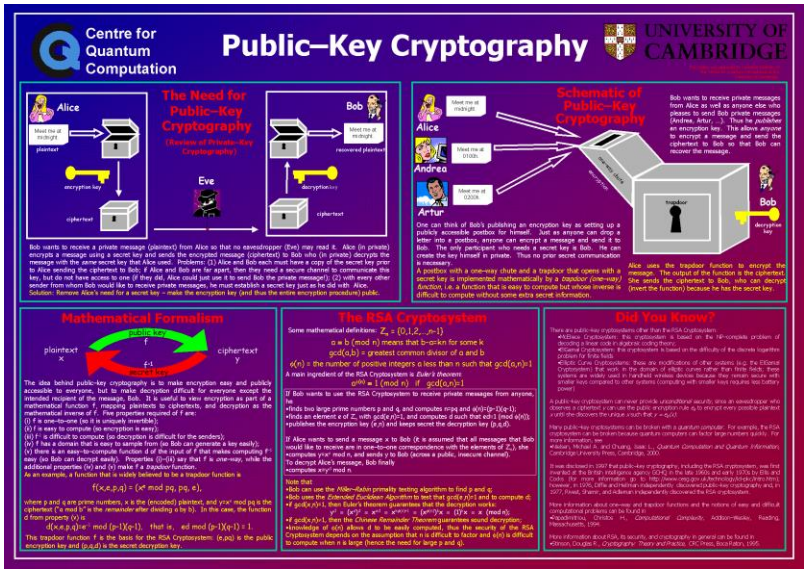
Version: GnuPG v2.0.22 (MingW32)

mQENBFLoLEoBCAC78bGpF6NFBSS6G4ZZPaX58EMNymqWyLgj4Qdi+u5eONx+0zTj

B3c5VMXCKAjiqoE6t2q+5yPvptGZci88dD2EC...

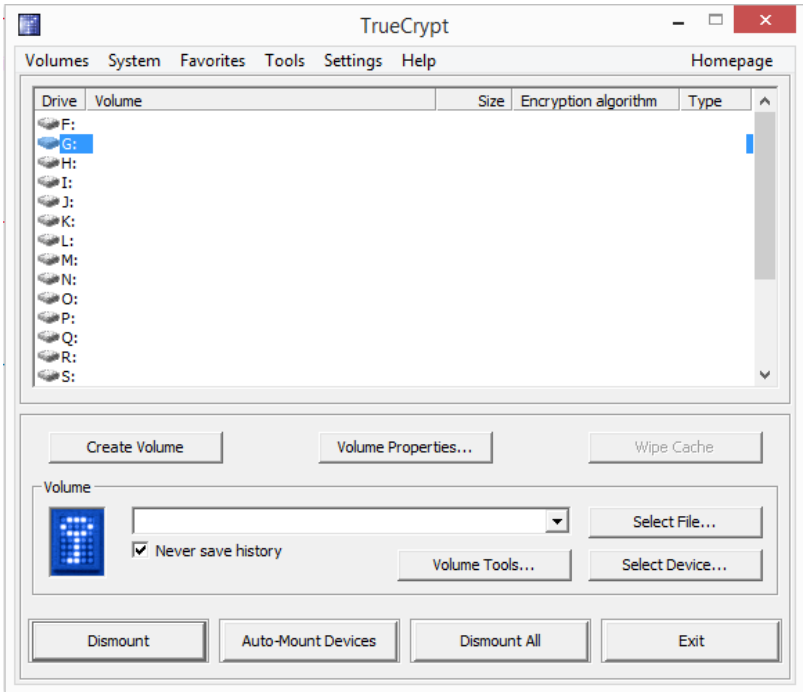
This file, as well as the text therein, is the public key you can share with anyone. People will use this public key to encrypt messages to send to you but only the private key that is set up and hidden in Kleopatra and Enigmail can be used to decrypt the emails. ***Never give out your private key!***

Congratulations, you learned how to set up an email client with basic encryption. Before you go out into the wide world however, I suggest you also do more reading here, and here. For more information on Public Key Cryptography, I suggest you read the following, or watch the video I inserted above. Additionally, the following graphic from the University of Cambridge is nice:



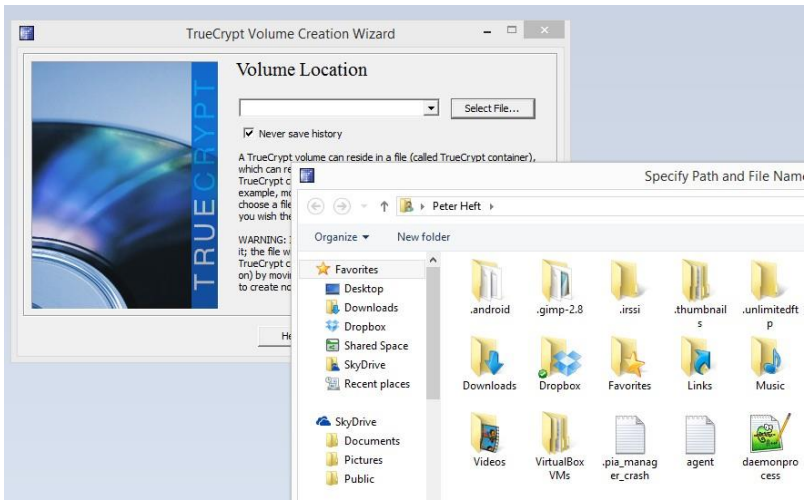
TrueCrypt

For this explanation of how to use TrueCrypt, I will just explain how to create a basic encrypted volume because that is the best for beginners. So first, navigate to the download page and download the correct version. Once downloaded, run the program and this is what you should see:

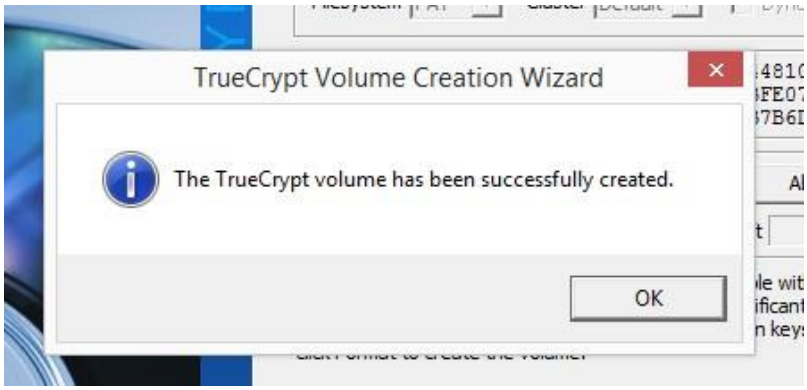


From this window, click "Volumes" and then "Create New Volume". You get the following window where you just want to click "Next":

Click "Next" again, we just want a standard volume. The next page asks you for a file. I suggest you make a file some place called "personal.txt". Once that is made, use the file manager to find what you just created and select it and click "Next" (**NOTE: DO NOT SELECT A FILE IN USE, IT WILL DELETE EVERYTHING)**:

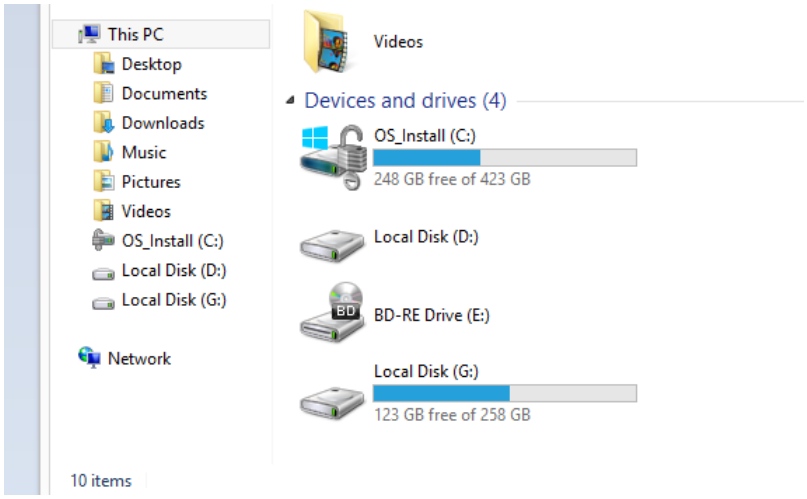


Following that, select the encryption method (I would say with AES) and click "Next", then specify the size you want the volume to be. So if you want to hold a 1gb file, make the space larger than 1gb. "Next". You get to a screen where it asks you to enter a password - enter a ***strong*** password here, this is the master password to decrypt this volume. Once that is done, click "Next" and wiggle your mouse in the window for a few seconds (this generates random numbers to use as the *salt*) and then click "format". Once it's done formatting, you get the following lovely window:



But as always, that is only half the battle. The next step is to mount the newly created volume. From TrueCrypt's main page, highlight a drive letter (eg. F:, G:, etc), click the "Select File" button, and navigate to where you saved the newly created volume and select it. Then click "Mount". Here it will ask you for your password and you should type it in and hit okay.

Once this is done, the volume is now mounted to whatever letter you assigned it. For the sake of this, it's G:. You then navigate to "This PC" and you should be able to see all your drives, including the newly created one titled "Local Disk (G:)"! (Note: My G: will be different because that is a much larger partition):

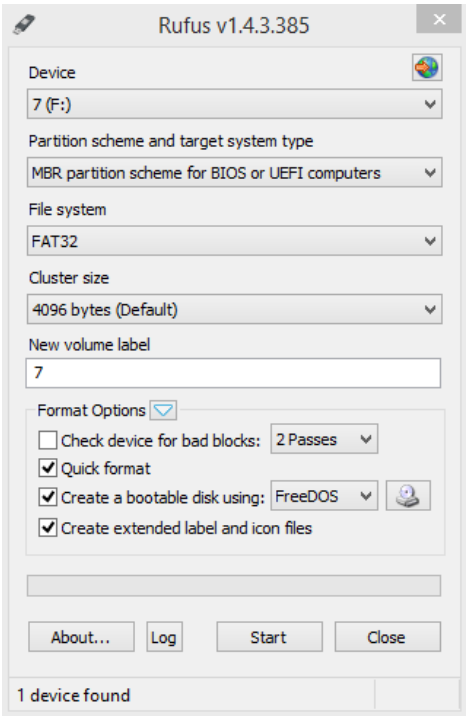


In order to dismount, go back to the TrueCrypt UI, highlight the drive letter, and hit "Dismount" and all is good. Congratulations!

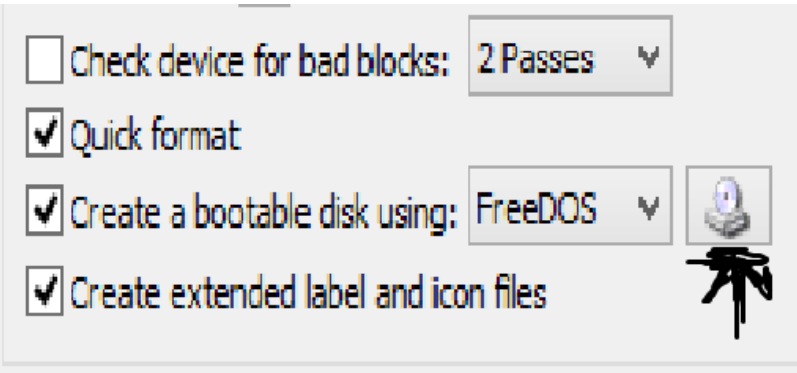
Tails

Finally, we get to Tails. Tails is going to be a bit more complicated so here is what I will do, I will explain how to make a flashdrive bootable, load it with Tails so it can boot, and then link you to a video explaining how to boot from a flashdrive. So what you need, a flashdrive, to download Tails from here, and a program called Rufus.

First, you should plugin your flashdrive and wipe it...this should be straight forward. Next, you need to open the program called Rufus, you will see the following screen:



From here, make sure the correct drive is selected (that is, make sure it's your flashdrive and not your external harddrive), and click this little button:

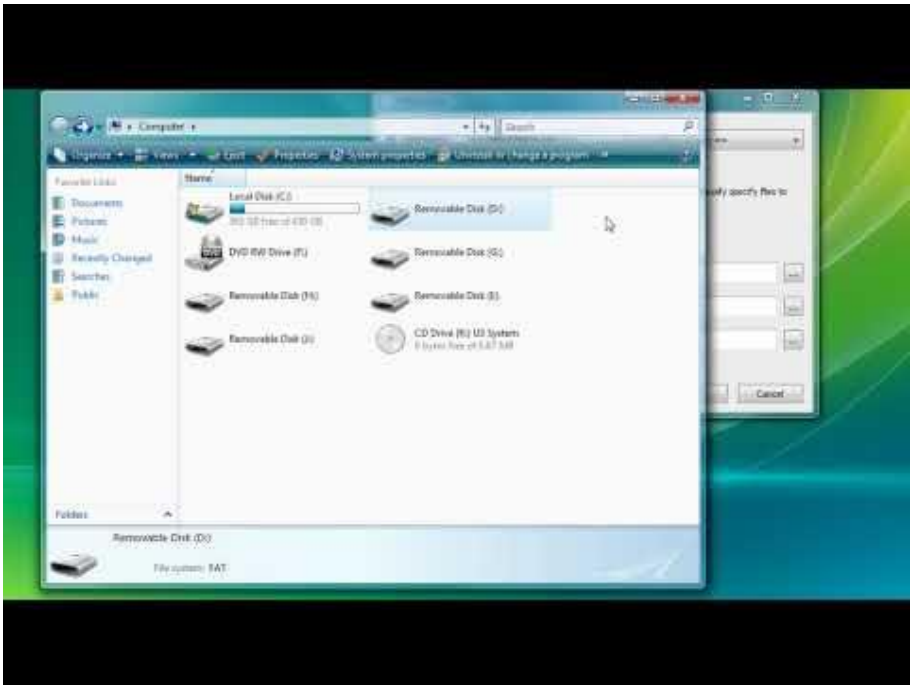


Next, navigate to where you saved the Tails .iso file and double click it. Then you will be taken back to Rufus and you should click "Start". From there, it may take a little bit, but the flashdrive is being made bootable. During this step ***do not remove it.*** Once it is done, eject the flashdrive and move on...

Now, because I don't have the time or the means to show you with images how to change the BIOS settings and boot from a flashdrive, I will leave this video, as well as some links:

Here is the link to the specific section of the video - http://youtu.be/pVCxkbZnEgA?t=4m43s.

Or if you want to hear him repeat everything I did (he does it a tad differently), watch it here:



Links here, and here, and here.

Part 8. Notes

More information:

Eff.org

Security in-a-Box

Notes:

*AES, or Advanced Encryption Standard, is the National Institute of Standards and Technology's (NIST) standard for US Government encryption. It is also the defacto encryption standard worldwide.

**Twofish is one of the standards used in OpenPGP and has, thus far, been uncrackable.

***The one drawback to WoT is that sometimes people rate based on political views. This means that actually safe websites (eg. Metapedia or Stormfront) are marked as unsafe simply because they have a far-right political view point. Additionally, not every site is rated. For example, my website (cnqzu.com) is not rated yet, but that doesn't mean it's unsafe.

Citations:

1: "Schipul - The Web Marketing Company." Schipul - The Web Marketing Company. N.p., n.d. Web. 27 Jan. 2014. <http://www.schipul.com/quotes/900/>.

2: "Breaking into Twitter accounts with a dictionary password attack." Naked Security. N.p., n.d. Web. 27 Jan. 2014. <http://nakedsecurity.sophos.com/2009/01/14/breaking-twitter-accounts-dictionary-password-attack/>.

3: "Passwords used by the Conficker worm." Naked Security. N.p., n.d. Web. 27 Jan. 2014. <http://nakedsecurity.sophos.com/2009/01/16/passwords-conficker-worm/>.

4: "Multi-word passphrases not all that secure, says Cambridge University." Naked Security. N.p., n.d. Web. 27 Jan. 2014. <http://nakedsecurity.sophos.com/2012/03/19/multi-word-passphrases/>.

5: Bonneau, Joseph. "Light Blue Touchpaper." Light Blue Touchpaper RSS. N.p., n.d. Web. 27 Jan. 2014. <http://www.lightbluetouchpaper.org/2012/03/07/some-evidence-on-multi-word-passphrases/>.

6: Bonneau, Joseph, and Ekaterina Shutova. "Linguistic properties of multi-word passphrases." JBonneau. N.p., n.d. Web. 27 Jan. 2014. <http://www.jbonneau.com/doc/BS12-USEC-passphrase_linguistics.pdf>.

7: "How Do I Create a Strong Password?." How Do I Create a Strong Password?. N.p., n.d. Web. 25 Jan. 2014. <http://www.webroot.com/us/en/home/resources/tips/getting-started/beginners-how-do-i-create-a-strong-password>.

8: "GRC | Ultra High Security Password Generator ." GRC | Ultra High Security Password Generator . N.p., n.d. Web. 27 Jan. 2014. <https://www.grc.com/passwords.htm>.

9: "Password Generator." Create Safe & Secure Passwords -. N.p., n.d. Web. 27 Jan. 2014. <https://identitysafe.norton.com/password-generator>.

10: "The Only Secure Password Is the One You Can't Remember." Lifehacker. N.p., n.d. Web. 27 Jan. 2014. <http://lifehacker.com/5785420/the-only-secure-password-is-the-one-you-cant-remember>.

11: "Request an email account." user.riseup.net. N.p., n.d. Web. 28 Jan. 2014. <https://user.riseup.net/forms/new_user/policy>.

12: "Revealed: Google and Facebook DID allow NSA access to data and were in talks to set up 'spying rooms' despite denials by Zuckerberg and Page over PRISM project." Mail Online. Associated Newspapers, 8 June 2013. Web. 28 Jan. 2014. <http://www.dailymail.co.uk/news/article-2337863/PRISM-Google-Facebook-DID-allow-NSA-access-data-talks-set-spying-rooms-despite-denials-Zuckerberg-Page-controversial-project.html>.

13: "How Google Gives Your Information to the NSA." Gizmodo. N.p., n.d. Web. 28 Jan. 2014. <http://gizmodo.com/how-google-gives-your-information-to-the-nsa-512840958>.

14: Gellman, Barton, and Ashkan Soltani. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say." Washington Post. The Washington Post, 1 Nov. 2013. Web. 27 Jan. 2014. <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>.

15: http://www.reddit.com/r/onions

ps. happy Data Privacy Day :)