I seek refuge in Allah from Shaytan, the accursed,

> "And prepare against them whatever you are able of power and of steeds of war by which you may terrify the enemy of Allah and your enemy and others besides them whom you do not know [but] whom Allah knows. And whatever you spend in the cause of Allah will be fully repaid to you, and you will not be wronged."

[8:60]
In the name of Allah, the indiscriminately merciful, the acutely merciful,
All glory and thanks is to Allah, the cherisher of all of existence,
And, verily, may peace and blessings be upon our leader Muhammad, his family, his companions, and all those that follow upon their path a great peace until the day of judgement.

As for what follows,

Remaining Anonymous Online

The question of online anonymity is an important one in this day and age. The advent of technology has made the internet ubiquitous and necessary to daily life. However, we see that the tyrants have invested in methods by which they can monitor every single particle of data that goes across the web. Every picture, phone call, text message, or any other form of anything uploaded or downloaded is monitored by these agencies. This prompts several questions, why do they monitor? Do we need to avoid their monitoring? How?

Since this is intended to be a rather brief paper, I won't discuss these questions in depth besides the final one. Short answers will suffice the two former questions. The intelligence agencies specifically monitor the internet with the intention of dismantling anti-colonial narratives and attacking those who postulate them. Whether Muslim, radical socialist, anarchist, or anti-government activist, they want you. They want to know what you send, when you send it, to whom you send it to, why, and how to use it against you. They monitor your social media. Even if you never use your real name, post a picture, or leave any hints, they can track your IP address, know your identity, and jail you for a few online posts. They search for keywords such as "kafir" in order to find specific individuals. These agencies are notorious for even harassing youth around the ages of fourteen to sixteen for their beliefs and rather reckless online posting.

Do we really need to avoid this? How much danger is there? For one living in South Africa or in Sham, there may not be much danger directly. You do not need to conceal your identity from any immediate threat that would be able to reach you through your internet usage. The need to avoid these agencies is exaggerated in those living in Western countries, from Finland to

the West coast of the United States. Here, kafir intelligence agencies are particularly interested in entrapping young Muslims. Sometimes, they will pretend to be sincere brothers or sisters and invite Muslims to marriage or hijrah, sometimes both, and when they coerce them, they jail them for trying to join terrorist organizations. It is clear these are amongst the foulest of Allah's creation. They want to find ikhwan who discuss these things because they know the true Islamic narrative is dangerous to their flamboyant way of life, wherein they hoard wealth from the poor and slaughter the weak. The United States government, the government of the United Kingdom, France, and elsewhere, want to jail you. They want you to suffer. And they aren't playing games.

Before I delve into how exactly this is done, I will dismiss a minor issue. Is it lying to trick the kufar into thinking we live in different locations than we actually do, through words or otherwise, even if other Muslims may hear or see this?

The ennobled messenger of Allah, sal'Allah'u alaiyhu wa' ala alaiyhi wa sahbihi salam tasleeman katheera ila yawm al din, said, in a rigorously authenticated narration,

> “War is deceit.”

[al-Bukhari: 3029]

The people we are fooling are ones who have an open war with Allah, his messenger, our khilafah, and just about every sincere Muslim on this planet. You are engaging in war tactics so that you can spread the true dawah and discuss matters of jihad, to uncover news about your mujahid brothers, to dismiss lies. You are entering into a sort of psychological warfare with them, they do not take it lightly, and we do not take it lightly. Therefore, we can trick them and it is totally permissible.

Ghost VPN

VPN stands for Virtual Private Network. Essentially, when one accesses a website through normal means, on their computer, they give that website their IP address. From this, the persons' address may be deduced. You may have wondered how Google knows what language to present to you without you ever having chosen it. That's how. Google knows your country, but the government agencies of the world know your home address and your entire name. That's where VPNs come in. If you use a VPN, instead of your IP telling them your real location, it will pick another location. Whether Italy, France, the Czech Republic, or in a remote location in the wilderness. If the agencies attempt to track you, their search will lead them to a dead end.

Ghost VPN is a popular program along these veins, but it is certainly not the only one. Many are available, and you can use whatever you feel most comfortable with. It is a program that you start, then you would begin to browse websites you don't want the government seeing you use, such as Twitter.

What are the adab of using a VPN? Never. Ever. Login with your real name or any such identifiers. Do not check your private Facebook with your full name. Do not check your private email. Or your bank account. Why not? This will show them that the person who is in Ireland is also logging into a Facebook account used by Salma Ahmad al-Sudaniyyah. And now they know your name, can find your address, and when you login to that Facebook off of a VPN, they know your home address. Turn on the VPN when no other internet browsers are open. Do what you need to do. Turn it off once done. Simple.

One can download and install this off of Google search.
https://www.cyberghostvpn.com/en_us

TOR

Whereas Ghost VPN was a program, TOR is an internet browser similar to Google Chrome, Firefox, and Internet Explorer. TOR uses the same line of thinking, however, instead of simply placing you in one location, it sends you internet signal through nodes, or servers, across dozens of countries. That way, any searches will come up inconclusive. TOR is a world ahead of Ghost VPN in terms of security and is the fundamental basic I recommend everyone to have. The same adab follow, no personal information on TOR whatsoever. One can choose to use Ghost VPN and TOR at the same time for additional security.

This can be found and downloaded in the TOR Browser Bundle, available online.
https://www.torproject.org/projects/torbrowser.html.en

Encrypted Email

Now that one has a VPN, and TOR, he needs a new email. You can't use that same email that reveals your home address. I personally recommend to turn on Ghost VPN whilst all other browsers are closed, turn on TOR, and go to bitmessage.ch. Follow the instructions there. Bitmessage is a peer-to-peer email service, meaning they don't save any of your emails anywhere, unlike GMail which saves every email. The only person who gets your email is that other person. Emails are also sent to random peoples' inboxes, but they are not given the keys to see or decode them. This is done to confuse any spies who wish to uncover who sent what email to who. The contents of the email, the sender, and receiver are all hidden. Your email address will look something like, DA94RDGBH0SFDSG0484802@bitmessage.ch, when first making it. Simply go to the alias page, bitmessage alias, and create a nickname. You cannot login with this nickname, so it is important to save the original address, but it will end up looking like AmreekiWitness@bitmessage.ch instead of letters and numbers. This can be used to access social media. Login to your encrypted email at, bitmessage.ch/webmail .

TAILS OS

We have discuss a program, Ghost VPN, a web browser, TOR, and now we will discuss an operating system, TAILS. The same way some people use Windows 7, Windows XP, Apple OS, or Linux, TAILS is an operating system. It is built from the ground up for the utmost privacy and security, in person, and online. It runs on a flash drive, and is a bit difficult to set up, but worth it. One boots their computer from a flashdrive, instead of when it normally boots

from a hard-drive, and this allows one to access TAILS once installed. It has multiple desktops, can turn off instantly, TOR pre-installed, amongst a plethora of security features. To use a VPN and TAILS is one of the most bleeding edge forms of internet security. The same adab as before apply.
Download here: https://tails.boum.org/

Social Media

One might be asking themselves if they can continue using their old social media on these. The answer is yes, but I do not recommend it whatsoever. If one feels they post things in which they would need this security, which is most Muslims upon haqq who are active online, then they should make a disclaimer saying something similar to,
"I recant all opinions deemed dangerous or violent expressed on this page. This page was run for educational and analytic purposes only, to study the radical Muslim community for recreational purposes. I invite all those who follow this page to leave such corrupt ideology. I am not affiliated with any groups or organizations deemed terrorist or dangerous otherwise by any Western government or union of governments. I am a law abiding citizen in every regard."
And then proceed to delete all other tweets/posts on the page and after leaving this up for a few minutes, simply delete the page. Make no indication that you have done this based on instructions. You are in a war with these people, we have discussed this earlier. Now, once you are on either TOR with a VPN, TOR, and/or TAILS OS, make a new bitmessage email. Make an alias. Sign-up for Twitter on TOR. Do not post pictures or any indication of who you are explicitly. If you feel the need to alter your writing style a bit, if you were a popular page, do so. You can make subtle indications that this is so and so, however, nothing that can be proven in a court of law. Allah'u must'a'n, may we never see inside one of those rooms for such a purpose.

Instant Messaging

There are two forms of instant messaging that can be used. One is on Google chrome, known as Cryptocat. Simply turn off all other tabs, enter into Ghost VPN, and then use Cryptocat. The other exists on PC, Linux, and Android devices, and is known as ChatSecure. It is run through TOR and messages are encrypted. Searching online will give one all the information they need.
I hope I have not written too much and that this does not bore anyone, but this is an introduction to the matter of online security. There is much I did not discuss, and perhaps some omitted that I should have. I ask Allah to accept this from me for his sake, and not for the sake of anyone else, I ask Allah to give us barakah, I ask Him, the one who hears the call of the caller, to hear our call. I ask Allah to never allow us to comitt haram online. I ask him to hasten our venturing to the lands of jihad and hijrah, the lands in which there is no worry about people spying on private matters, in which the justice of Allah is supreme over the paranoia of men.
Ameen, Ameen, Ameen.

BarakAllah feekum, ash-hadul la ilaha il Allah, wa ash hadu anna Muhammadar Rasul'Allah. And the last of our call is al-hamdulilahi rahb al-alamin.