
dgplug Summer Training Documentation

Release 0.1

Kushal Das

Aug 30, 2021

Contents

1	FAQ	3
1.1	What are the topics covered?	4
1.2	How do I subscribe to the mailing list?	4
1.3	What are the requisites for the training?	4
1.4	How do I get the logs?	4
1.5	How long does a session run?	4
1.6	How long is the summer training?	4
1.7	Will the session details be sent to the mailing list?	4
1.8	In case I miss a class, how do I catch up?	4
1.9	Do we need to learn something beforehand for this training?	4
1.10	How many sessions happen in a day?	5
1.11	Will the time be the same for all the sessions?	5
1.12	If I have to leave class early, should I announce it mid class?	5
1.13	Is there any calendar available for the sessions?	5
1.14	How should I behave in the channel and during sessions?	5
1.15	How can I make the most of this training?	5
2	Before you start	7
2.1	How to ask for help?	7
2.2	There is no magic mirror!	7
2.3	Learn touch typing	8
2.4	History of Free and Open Source Software	8
2.5	Download Tor browser	8
3	Watch The Internet's Own Boy	9
4	Watch Coded Bias	11
5	Communication guidelines	13
5.1	Be nice to everyone	13
5.2	Do not assume pronouns of people	13
5.3	Different mediums of online communication	13
6	Communication	15
6.1	Clients	15
6.2	How to use IRC?	15
6.3	Register your nickname	15

6.4	Rules to follow	15
7	Do not write HTML emails	17
7.1	How to write plain text email in gmail?	18
8	Mailing list	19
8.1	Rules for the sessions	20
8.2	How to ask a question?	20
8.3	More logs to read	20
9	What is IRC?	21
9.1	What is a channel?	21
9.2	IRC clients	21
9.3	hexchat	22
9.4	How to install?	22
9.5	Configurations Steps	22
9.6	IRC on the Web	29
9.7	Step 1. The Browser	29
9.8	Step 2. A username for IRC.	31
9.9	Step 3. Connecting to the DGPLUG channel.	37
9.10	Nick Ghosting	41
10	Tor Project	43
10.1	Why should you use Tor?	43
10.2	How to install and run Tor Browser?	43
10.3	For Windows users	45
10.4	How does Tor actually work?	45
10.5	Getting more help	45
11	Privacy	47
12	Assessing Your Risks	49
12.1	What do I have inside my home that is worth protecting?	49
12.2	Who do I want to protect it from?	49
12.3	How likely is it that I will need to protect it?	50
12.4	How bad are the consequences if I fail?	50
13	Good practices	53
13.1	Keep your machine updated	53
13.2	Use strong and unique passwords	53
13.3	Use password managers	55
13.4	Do not keep the computer unlocked	55
13.5	Cover up your webcam	55
13.6	Take regular backups	55
13.7	Enable 2 factor authentication (2FA)	56
13.8	Encrypt all USB drives	56
13.9	Do not download and install random software from internet	56
13.10	Do not plug random USB devices into your computer	56
13.11	Use the following browser plugins for better privacy	57
13.12	Do not trust private browsing mode to save your privacy	57
13.13	Use Tor for almost everything	57
13.14	About communication tools on phone	57
13.15	Do not click on random links in emails or from anywhere else	57
13.16	Do not install random certificate on the browser	58
13.17	SURVEILLANCE SELF-DEFENSE	58

14 Talks from around the world	61
15 Blogging	63
15.1 1. Why do we need a blog? Why do we need to write?	63
15.2 2. Blogs, how do you set one up?	65
15.3 3. Tactical Advice	65
15.4 4. Bonus References	67
16 Book suggestions	69
16.1 General topics	69
16.2 Writing & Blogging	69
16.3 Design & Presentations	70
16.4 General programming	70
16.5 Productivity	71
17 Indices and tables	73

Contents:

Table of Contents

- *FAQ*
 - *What are the topics covered?*
 - *How do I subscribe to the mailing list?*
 - *What are the requisites for the training?*
 - *How do I get the logs?*
 - *How long does a session run?*
 - *How long is the summer training?*
 - *Will the session details be sent to the mailing list?*
 - *In case I miss a class, how do I catch up?*
 - *Do we need to learn something beforehand for this training?*
 - *How many sessions happen in a day?*
 - *Will the time be the same for all the sessions?*
 - *If I have to leave class early, should I announce it mid class?*
 - *Is there any calendar available for the sessions?*
 - *How should I behave in the channel and during sessions?*
 - *How can I make the most of this training?*

The questions are not in any particular order.

1.1 What are the topics covered?

This [page](#) contains details about the topics covered in the training.

1.2 How do I subscribe to the mailing list?

Go to the [mailing list](#) page, put in your name and email id and click subscribe. Go to your inbox, open the email that you receive from the list, click on the link there and confirm.

1.3 What are the requisites for the training?

- A fast Internet connection
- Any modern Linux distribution. If you only have Windows, you can install it in a VM (say using Virtualbox).

1.4 How do I get the logs?

Find all the old logs at <http://dgplug.org/jirclogs/>

1.5 How long does a session run?

It depends on that particular class. Generally 1-1.5 hours but some sessions went upto 3 hours. (Though long sessions happen rarely.)

1.6 How long is the summer training?

About three months.

1.7 Will the session details be sent to the mailing list?

Yes, we do send the details based on the sessions. Remember to keep an eye on the mailing list.

1.8 In case I miss a class, how do I catch up?

Read the logs if available, or ask for the logs from a friend. Most things taught, will have detailed docs available.

1.9 Do we need to learn something beforehand for this training?

Not really, if you follow the sessions properly you can learn while the training is going on.

1.10 How many sessions happen in a day?

Generally just one; rarely there might be more than one session in a day.

1.11 Will the time be the same for all the sessions?

Nope, it may change, depending on each session.

1.12 If I have to leave class early, should I announce it mid class?

Yes, just inform so and leave.

1.13 Is there any calendar available for the sessions?

In 2018 we have introduced a new calendar for the summer training. You can view it [on web](#) or subscribe to it using your favorite calendar application.

1.14 How should I behave in the channel and during sessions?

- In the channel we value a kind and polite tone. Don't be rude or offensive, you risk getting kicked.
- If no session is going on, feel free to ask questions and chat with the other participants. During sessions, do not speak unless called upon.
- If you're joining late when a session is (or could be) going on, don't disturb and try to catch up. If you have a question, raise your hand by typing "!" and wait for your turn to speak.
- Having guest speakers in the channel, we want to treat them as guests. Before firing questions at them, let them speak first.

1.15 How can I make the most of this training?

This summertraining can be a great source of information and provide you with a broad and solid fundament to build your developer skills upon. However, there is much more for you to discover. We are a community that supports each other. We advocate hackerism and openness and would love to welcome you as active participants among us. Talk to other people in the channel and you will most likely find like-minded persons and make some good new friends.

You should respect the following points:

- Log files do not replace attendance during sessions. The training lives from active participation.
- Try to be online in the channel as much as possible. If you come online for sessions only, you will miss many interesting conversations and don't get in contact with other people in the channel.
- You can ask any question in the channel. However, always make sure that you have tried to find the answer yourself before, using your favourite search engine or wiki or man pages, etc. We follow the motto "Learn yourself, teach others".

- Learning something requires commitment and enthusiasm. These are much valued characteristics that will earn our respect.

CHAPTER 2

Before you start

The motto of [dgplug](#) is “Learn yourself and teach others”. The summer training effort is a huge part of this. We try to learn together and help each other. Before you jump into this, there are a few small things one should know.

But, even before you read the rest the document to learn more, first please watch [this talk](#) from the ever amazing [Ian Coldwater](#). Take your time, listen to them.

2.1 How to ask for help?

There will be many times in a day when you will need some help, may be to solve a problem, or to learn a new thing. Before you go and ask for help, you should first search for a solution. Most of the times, you will find the answer yourself. We suggest everyone to use [DuckDuckGo](#) search engine. This particular search engine does not track you, and focused to protect your privacy.

If you open the site for the first time, it will show you ways you can enable it as the default search engine in your browser. That should be the first thing to do. Go ahead, and enable DuckDuckGo as the default search engine.

To know more why should you use DuckDuckGo, read [their privacy page](#).

2.2 There is no magic mirror!

If you just come online and ask help by saying “I have an error.”, no one will be able to help you. Because, we need to see the exact error you can see in your computer. Best way to ask for help is by providing as much information as possible along with the question. If the error message is more than 2 lines, then one should use a pastebin server (like [Fedora modernpaste service](#)) and paste the whole error message there, and then only provide the URL to the pastebin in the question.

2.3 Learn touch typing

[Touch typing](#) is one of the most important thing to learn before you jump into programming or commands to control a server. Typing errors are the most common cause behind the errors we get in computers. Typing efficiently and fast will help you through out the life.

Here is a [blog post](#) to find out more about the topic.

2.4 History of Free and Open Source Software

Read [this post](#) to learn about the history, then also read [this log](#) to hear from Jim Blandy about his experience. Free Software movement is the reason why we have this community standing together. So, make sure to go through the history first.

2.5 Download Tor browser

The next important step is to [download Tor Browser](#). To start using it, follow [these steps](#). You may have a lot of questions about *Why should we use Tor?*, through out the summer training we will have many discussions on this. But, to understand the basics, have a look at this [page](#).

Please read the [Tor Project](#) chapter to learn in details.

CHAPTER 3

Watch The Internet's Own Boy

Take 2 hours of time and [watch this documentary](#).

Now spend some time and think about it.

CHAPTER 4

Watch Coded Bias

Next, you should watch [Coded Bias](#) documentary. It is available on Netflix.

Communication guidelines

Communication is one of the most important tool in any contributor's toolbox. The Free & Open Source Software communities grew over the years, and now we have various mediums to communicate over Internet. People are spread across the world in different time zones, the cultures and primary languages are different among us.

5.1 Be nice to everyone

The most important point to start this guide, always be nice to everyone over Internet. Do not use any improper words, or attack people. Everyone has their own view point, and own opinion. That may not be the same of yours, but that should not be the reason to start a heated argument over chat/meeting/ mailing list. People are opinionated, to solve some complex problem people will try to force their ideas to everyone. But, the language should always remain civil.

5.2 Do not assume pronouns of people

Do not try to assume which pronoun to use while talking to someone. It is much nicer if you use gender neutral words (or the names) in any type of communication. [This guide](#) has more details which one should read.

5.3 Different mediums of online communication

- Direct emails
- Mailing lists
- Chatting applications (IRC, Gitter, Google Chat, Slack)

[This session](#) from Shakthi Kannan has more details about how to communicate. Please go through it next.

We use IRC as our primary communication during summer training and it also a main communication medium for many FOSS projects.

6.1 Clients

- [HexChat](#)
- [webchat](#)

6.2 How to use IRC?

Please read the *[What is IRC?](#)* chapter to learn in details.

6.3 Register your nickname

Remember to register your nickname, you can follow [this guide](#).

6.4 Rules to follow

Be nice to others.

Always type full English words, no sms speak in any FOSS communications. That means no more 'u' or 'r', instead type 'you' or 'are'.

Though are few short forms which are acceptable in IRC.

Short Form	Full Form
brb	Be right back
iirc	If I remember correctly

For more [Abbreviations Commonly Used on IRC](#).

CHAPTER 7

Do not write HTML emails

Please avoid sending HTML emails, in private emails, or to any mailing list. dgplug mailing list will automatically delete any HTML email sent to the list.

We are sure you want to why is it bad? We will discuss more about it during the training.

For now, we give you [this tweet](#).



matt blaze ✓

@mattblaze

Follow



I've long thought HTML email is the work of the devil, and now we have proof I was right. But did you people listen? You never listen.

9:30 AM - 14 May 2018

170 Retweets 564 Likes



35

170

564

7.1 How to write plain text email in gmail?

You can mark outgoing emails as plain text emails in the gmail web frontend.

CHAPTER 8

Mailing list

Please join in our [mailing list](#). Remember not to do top post but only reply inline. To avoid top post use E-mail client (Thunderbird, Evolution).

- Top post reply:

```
Hello,  
  
Please refer to <http://dgplug.org/irclogs/2014/session01-welcomeandcommunication.  
→txt>  
for yesterday's training logs.  
  
The timing of the today's class is 06:30 P.M. (IST).  
  
Bar  
  
-- Foo<foo at gmail.com> wrote:  
> i have missed the yesterday's training class.  
> Where can i get the yesterday class's log?  
> What is the timing of the today's class?
```

- Inline reply:

```
Hello,  
  
-- Foo<foo at gmail.com> wrote:  
> i have missed the yesterday's training class.  
> Where can i get the yesterday class's log?  
  
Please refer to <http://dgplug.org/irclogs/2014/session01-welcomeandcommunication.  
→txt>  
for yesterday's training logs.  
  
> What is the timing of the today's class?
```

(continues on next page)

(continued from previous page)

```
The timing of the today's class is 06:30 P.M. (IST).
```

```
Bar
```

8.1 Rules for the sessions

- Do not speak when the session is going on.
- If you have a question type ! and wait for your turn.
- Try to come online 5 minutes before the session starts.
- Address people by their IRC nick.
- Do not use sir and madam.
- Do not use SMS language, write full English words.

8.2 How to ask a question?

First read [this document](#). Remember to search in DuckDuckGo and then only ask.

8.3 More logs to read

- [Log 1](#)
- [Log 2](#)

CHAPTER 9

What is IRC?

Internet Relay Chat (IRC) is an application protocol to do text based communication. It was created in 1988 and still being used as one of the primary communication medium for many people around the world, including various Free and Open Source software projects.



The above is the first ever IRC server (original image is from [Wikimedia Commons](#) taken by Urpo Lankinen).

We use IRC as our primary communication medium because it works with low bandwidth. You don't need super fast internet connection to attend the summer training sessions. Also, later when you will try to contact other communities, you will find most of them are active on IRC.

9.1 What is a channel?

Every IRC server has various virtual groups or rooms where people can communicate with each other. These are known as channels. The channel names start with # sign. For example, **#dgplug** is the channel name on the Libera Chat server for our training.

9.2 IRC clients

There are various IRC clients, for our sessions you can use **hexchat** client on your computer.

9.3 hexchat

hexchat is a popular Internet Relay Chat (IRC) client. It has a choice of a tabbed document interface or tree interface, support for multiple servers and is highly configurable.

- [hexchat](#)

9.4 How to install?

For Fedora:

```
# dnf install hexchat
```

For Ubuntu:

```
# apt-get install hexchat
```

For windows please download hexchat from their [site](#).

9.5 Configurations Steps

Launching **Hexchat** for the first time, will open the network selection window where you have to need to do the following

1. Put in a nickname that is fairly unique, in the Nick name box.
2. And an alternative in the second choice box.
3. Fill in the username field too (For convenience's sake, keep it the same as your nickname)
4. Click the New Network name in the list below and rename it to Libera or Libera Chat.

Your window should look something like this.

Then click the edit button on the right (in the pic above), to edit and configure the server setting to `irc.libera.chat/+6697` like you see in the pic below ... (also make sure that the ssl option is ticked)

Click close and then you'll be back at the network selection window. With Libera highlighted, hit the connect button and you should be connected to the Libera Chat IRC network. Hexchat will ask you to connect to a channel. Select the I'll join a channel later option and hit ok.

Now that we've connected to IRC, we need to register our nickname to make sure someone else not using it. We need to type this command `/msg NickServ REGISTER YourPassword youremail@example.com` in the tiny box at the bottom where we type in our messages and commands. Here YourPassword is some long password of your choosing (*not* your email account password) and `youremail@example.com` needs to be replaced with your email address

We've done this in the image below. (The email and password we've typed is greyed out. You'll see it more clearly if you click the image to see a larger view. Folks reading on a cell phone, you'll have to really zoom in.)

If all goes well the Libera Chat server, should respond with something like this

Now if we hop over to our email, we should get a email like the one below.

We copy the command from the email (the whole `/msg NickServ VERIFY ...` line) and paste it into our Hexchat window and hit enter. Libera Chat should then confirm all is well like so ...

Network List - HexChat [X]

User Information

Nick name:

Second choice:

Third choice:

User name:

Networks

2600net
2ch
AccessIRC
AfterNET
Aitvaras

☐ Skip network list on startup ☐ Show favorites only

Edit Libera - HexChat ✕

irc.libera.chat/+6697

Add
Remove
Edit

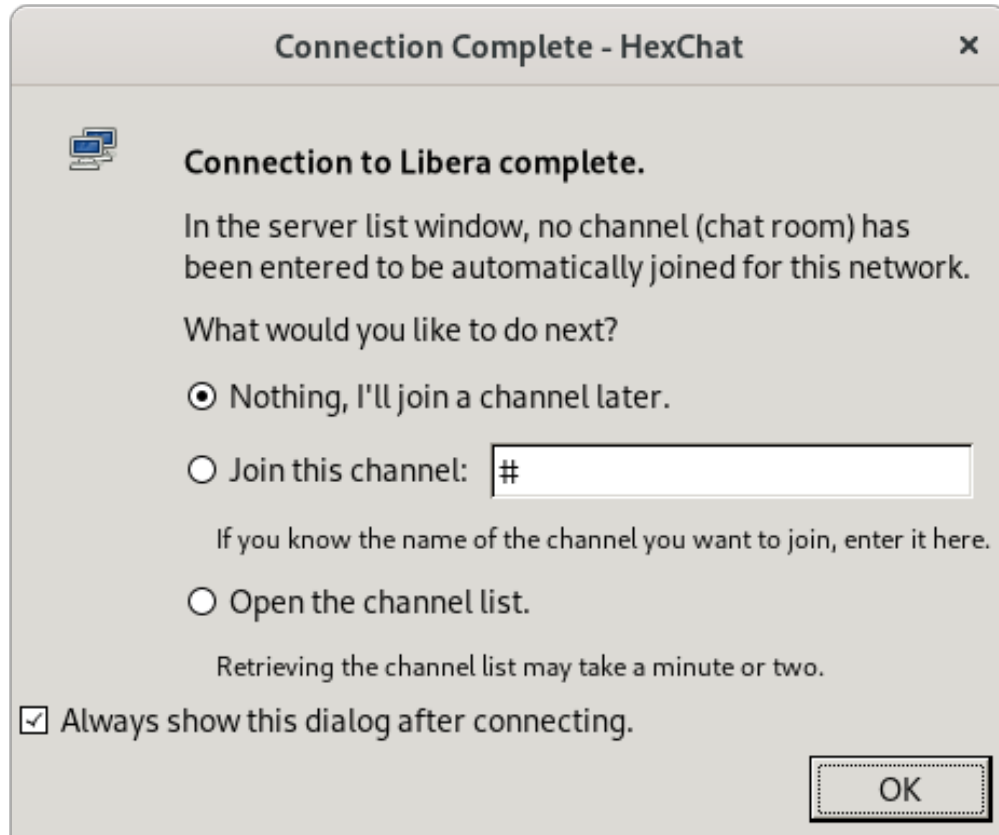
Servers | Autojoin channels | Connect commands

☐ Connect to selected server only
☐ Connect to this network automatically
☐ Bypass proxy server
☒ Use SSL for all the servers on this network
☐ Accept invalid SSL certificates
☒ Use global user information

Nick name:
Second choice:
Real name:
User name:

Login method: Default ▼
Password:
Character set: UTF-8 (Unicode) ▼

Close



Now that our nickname is registered, we can always use this same nick by authenticating with NickServ by issuing the following command:

```
/msg nickserv identify your_password
```

Manual authentication to NickServ in this fashion, can be quickly get tedious though.

With HexChat, we can speed this up / automate this away, by setting up SASL authentication.

Open the network selection window with *Ctrl+S* and select the network to edit. (Libera in our case)

In the edit window, shown below, change the login method to SASL and fill in your password.

Quit Hexchat and launch it again and we'll get the familiar join a channel prompt.

This time we can choose the "Join this channel:" option and type in `#dgplug` for the channel and click ok. (We can also untick the "Always show this dialogue after connection ..." prompt if we so choose.)

If all goes well, we should be in the **#dgplug** channel, all ready to chat and learn :)

Activities

HexChat

May 31 14:41

mjb-at-libera @ Libera - HexChat

HexChat View Server Settings Window Help

Libera.Chat

[14:38:43] * Connected. Now logging in.

[14:38:44] * *** Checking Ident

[14:38:44] * *** Looking up your hostname...

[14:38:45] * *** Found your hostname:

[14:38:48] * *** No Ident response

[14:38:48] * Capabilities supported: account-notify away-notify chghost extended-join multi-prefix sasl=PLAIN,ECDSA-NIST256P-CHALLENGE,EXTERNAL tls account-tag cap-notify echo-message solanum.chat/g solanum.chat/realhost

[14:38:48] * Capabilities requested: account-notify away-notify chghost extended-join multi-prefix cap-notify

[14:38:49] * Capabilities acknowledged: account-notify away-notify chghost extended-join multi-prefix cap-notify

[14:38:49] * Welcome to the Libera.Chat Internet Relay Chat Network mjb-at-libera

[14:38:49] * Your host is zinc.libera.chat[195.148.124.80/6697], running version solanum-1.0-dev

[14:38:49] * This server was created Sat May 29 2021 at 16:11:45 UTC

[14:38:49] * zinc.libera.chat solanum-1.0-dev DGQRSZaghilopsuwz CFILMPQsbcefgijklmnopqrstuvz bkloveqjfi

[14:38:49] * WHOX CALLERID=g SAFELIST ELIST=CTU MONITOR=100 ETRACE FNC KNOCK CHANTYPES=# EXCEPTS INVEX

[14:38:49] * CHANLIMIT=#:250 PREFIX=(ov)@+ MAXLIST=bqeI:100 MODES=4 NETWORK=Libera.Chat STATUSMSG=@+ CASEMAPPING

[14:38:49] * NICKLEN=16 MAXNICKLEN=16 CHANNELLEN=50 TOPICLEN=390 DEAF=D :are supported by this server

[14:38:49] * TARGMAX=NAMES:1,LIST:1,KICK:1,WHOIS:1,PRIVMSG:4,NOTICE:4,ACCEPT:1,MONITOR:1,EXTBAN=\$,ajrxz CLIENTVER=

[14:38:49] * supported by this server

[14:38:49] * There are 57 users and 24256 invisible on 22 servers

[14:38:49] * 36 :IRC Operators online

[14:38:49] * 11 :unknown connection(s)

[14:38:49] * 16911 :channels formed

[14:38:49] * I have 1735 clients and 1 servers

[14:38:49] * 1735 1737 :Current local users 1735, max 1737

[14:38:49] * 24313 24317 :Current global users 24313, max 24317

[14:38:49] * Highest connection count: 1738 (1737 clients) (11292 connections received)

[14:38:49] * - zinc.libera.chat Message of the Day -

[14:38:49] * - Welcome to Libera Chat, the IRC network for free & open-source software

[14:38:49] * - and peer directed projects.

[14:38:49] * -

[14:38:49] * - Use of Libera Chat is governed by our network policies.

[14:38:49] * -

[14:38:49] * - Please visit us in #libera for questions and support.

[14:38:49] * -

[14:38:49] * - Website and documentation: https://libera.chat

[14:38:49] * - Webchat: https://web.libera.chat

[14:38:49] * - Network policies: https://libera.chat/policies

[14:38:49] * - Email: support@libera.chat

[14:38:49] * End of /MOTD command.

[14:38:49] * mjb-at-libera sets mode +R on mjb-at-libera

[14:38:49] * mjb-at-libera sets mode +Z on mjb-at-libera

[14:38:49] * mjb-at-libera sets mode +i on mjb-at-libera

mjb-at-libera /msg NickServ REGISTER

[14:41:09] -NickServ- An email containing nickname activation instructions has been sent to @

[14:41:09] -NickServ- Please check the address if you don't receive it. If it is incorrect, DROP then REGISTER a

[14:41:09] -NickServ- If you do not complete registration within one day, your nickname will expire.

[14:41:09] -NickServ- mjb-at-libera is now registered to @.com.

mjb-at-libera

26

Chapter 9. What is IRC?

Libera.Chat Account Registration Inbox x



Libera.Chat Network Services <noreply.support@libera.chat>

to me ▾

mjb-at-libera,

In order to complete your account registration, you must type the following command on IRC:

```
/msg NickServ VERIFY REGISTER mjb-at-libera HtOghK8uoszM55hC
```

Thank you for registering your account on the Libera.Chat IRC network!

--

This e-mail was sent due to a command from mjb-at-libera [redacted] at Mon, 31 May 2021 09:11:09 +0000. If this message is unsolicited, please contact support@libera.chat with a full copy.

```
[14:41:09] -NickServ- mjb-at-libera is now registered to [redacted]@[redacted].com.
[14:43:01] >NickServ< VERIFY REGISTER mjb-at-libera HtOghK8uoszM55hC
[14:43:02] -NickServ- mjb-at-libera has now been verified.
[14:43:02] -NickServ- Thank you for verifying your e-mail address! You have taken steps in ensuring that your
registrations are not exploited.
```

mjb-at-libera [redacted]

Edit Libera - HexChat ✕

irc.libera.chat/+6697

Add
Remove
Edit

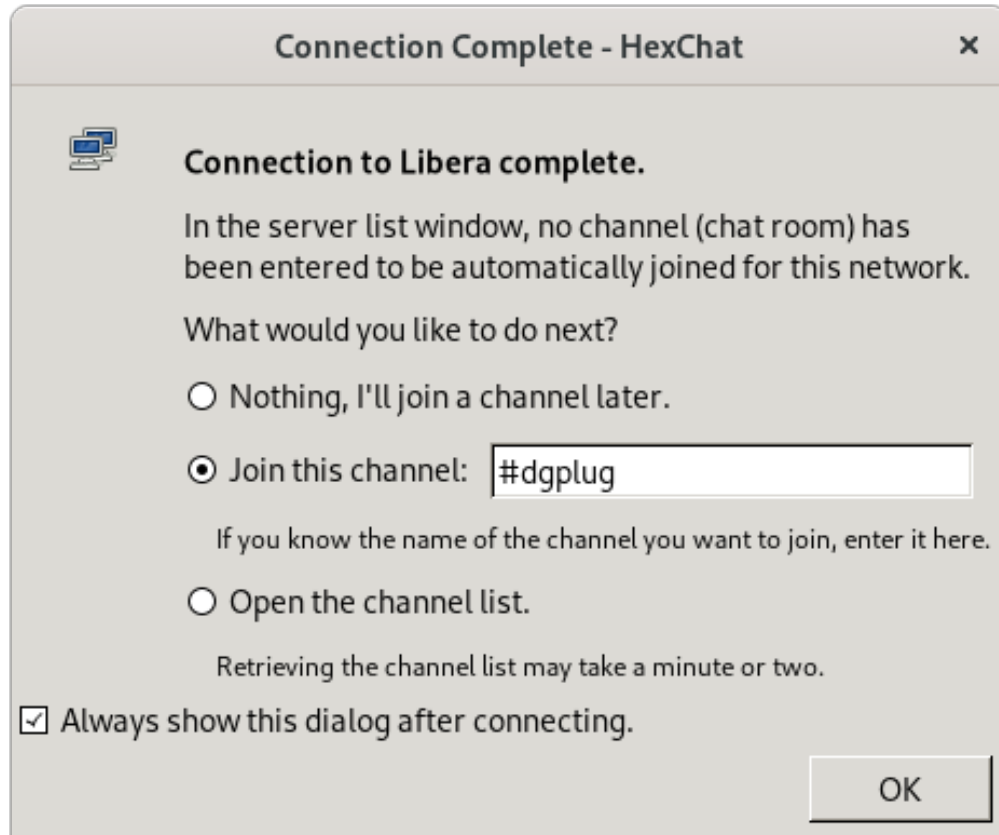
Servers Autojoin channels Connect commands

☐ Connect to selected server only
☐ Connect to this network automatically
☐ Bypass proxy server
☐ Use SSL for all the servers on this network
☐ Accept invalid SSL certificates
☒ Use global user information

Nick name:
Second choice:
Real name:
User name:

Login method: SASL (username + password) ▼
Password:
Character set: UTF-8 (Unicode) ▼

Close



9.6 IRC on the Web

While a client (xchat, hexchat, etc), on any platform, is the best way to experience IRC on a daily basis, you can in fact use your web browser to connect to IRC!

While it might not be as comfortable as a native client, irc via a browser is actually quite full featured.

It depends on you knowing commands though, so [this page on the IRC beginner website](#) will come in real handy.

So let's start at the very beginning.

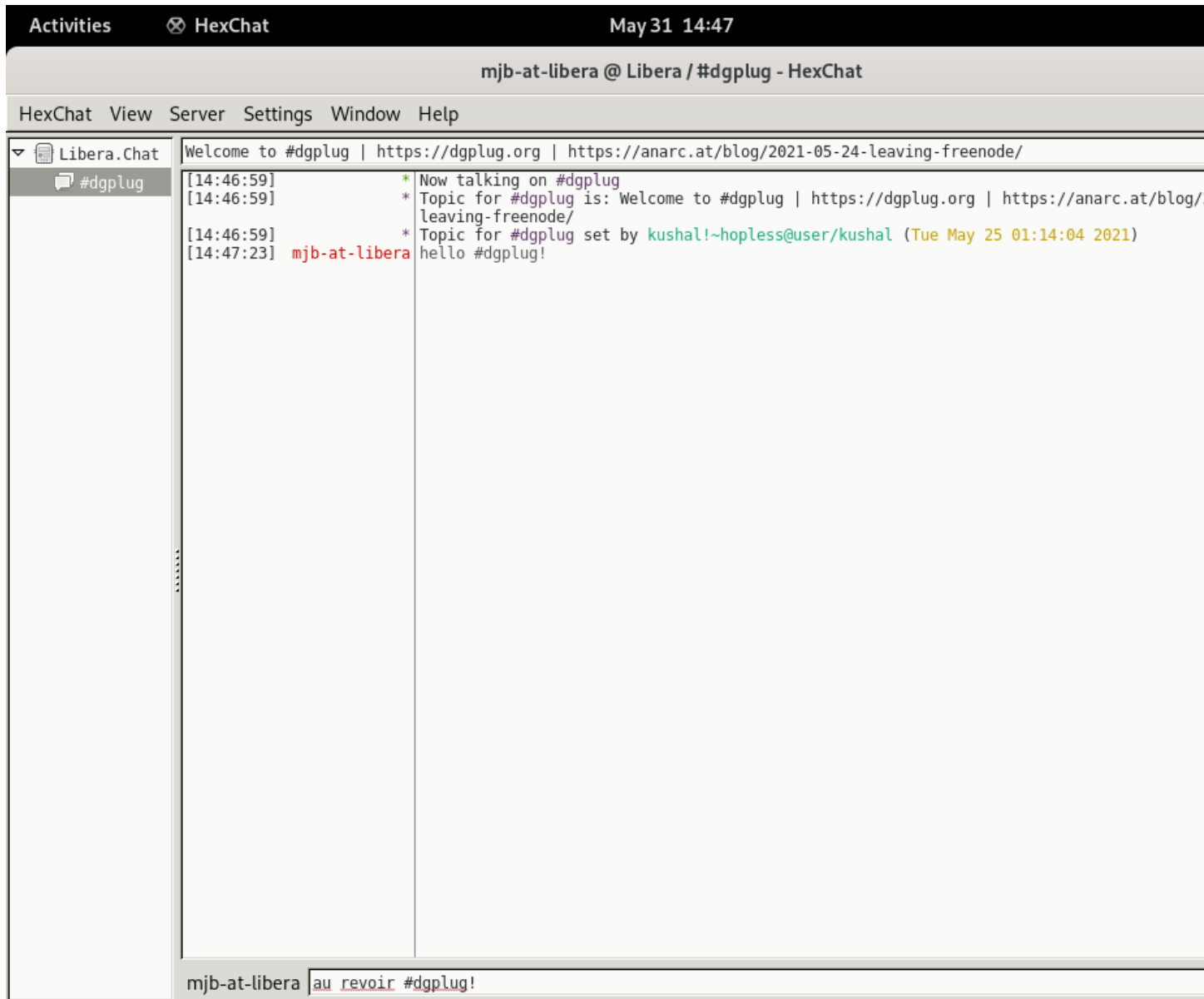
Here's what we'd need for our summer sessions.

1. We need a browser
2. We need an username that stays the same, throughout sessions
3. We need to login to the #dgplug channel on [Libera Chat](#) with that username

9.7 Step 1. The Browser

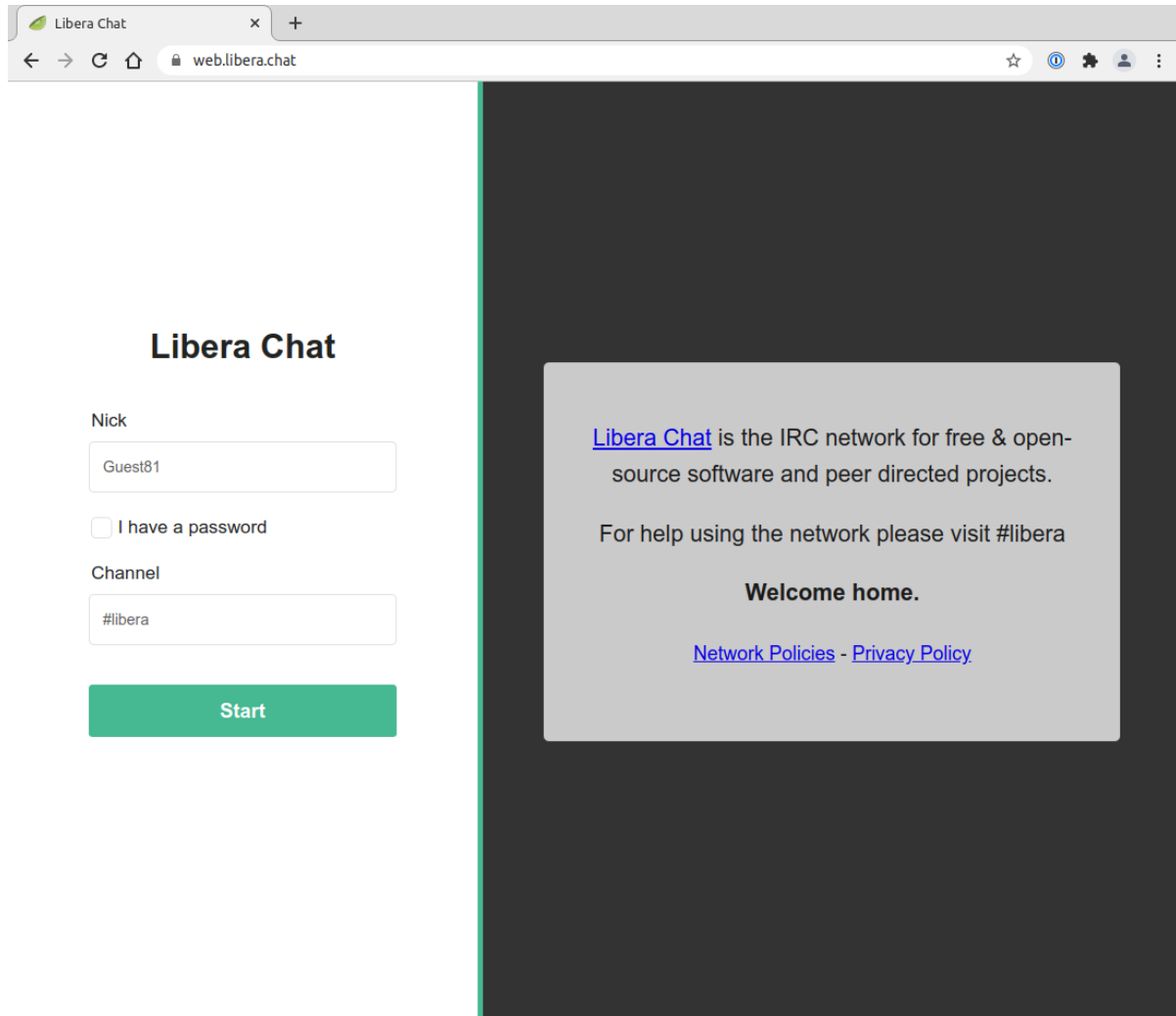
Congratulations!

You've already have one and are successfully connected, if you're reading this :)



9.8 Step 2. A username for IRC.

Let's mosey over to the [Libera Chat](https://web.libera.chat) website.



The screenshot shows a web browser window with the address bar displaying "web.libera.chat". The page has a dark background. On the left, there is a white login form titled "Libera Chat". The form includes a "Nick" field with the text "Guest81", a checkbox labeled "I have a password", a "Channel" field with the text "#libera", and a green "Start" button. On the right, a light gray box contains a welcome message: "Libera Chat is the IRC network for free & open-source software and peer directed projects. For help using the network please visit #libera. Welcome home. Network Policies - Privacy Policy".

Login with the nickname you want, like I've done here.

I've chosen `mariojason` for a nick.

Clear the channel of the default channel that says `#libera`, so that it's blank

Click Start.

Libera Chat

Nick

mariojason

☐ I have a password

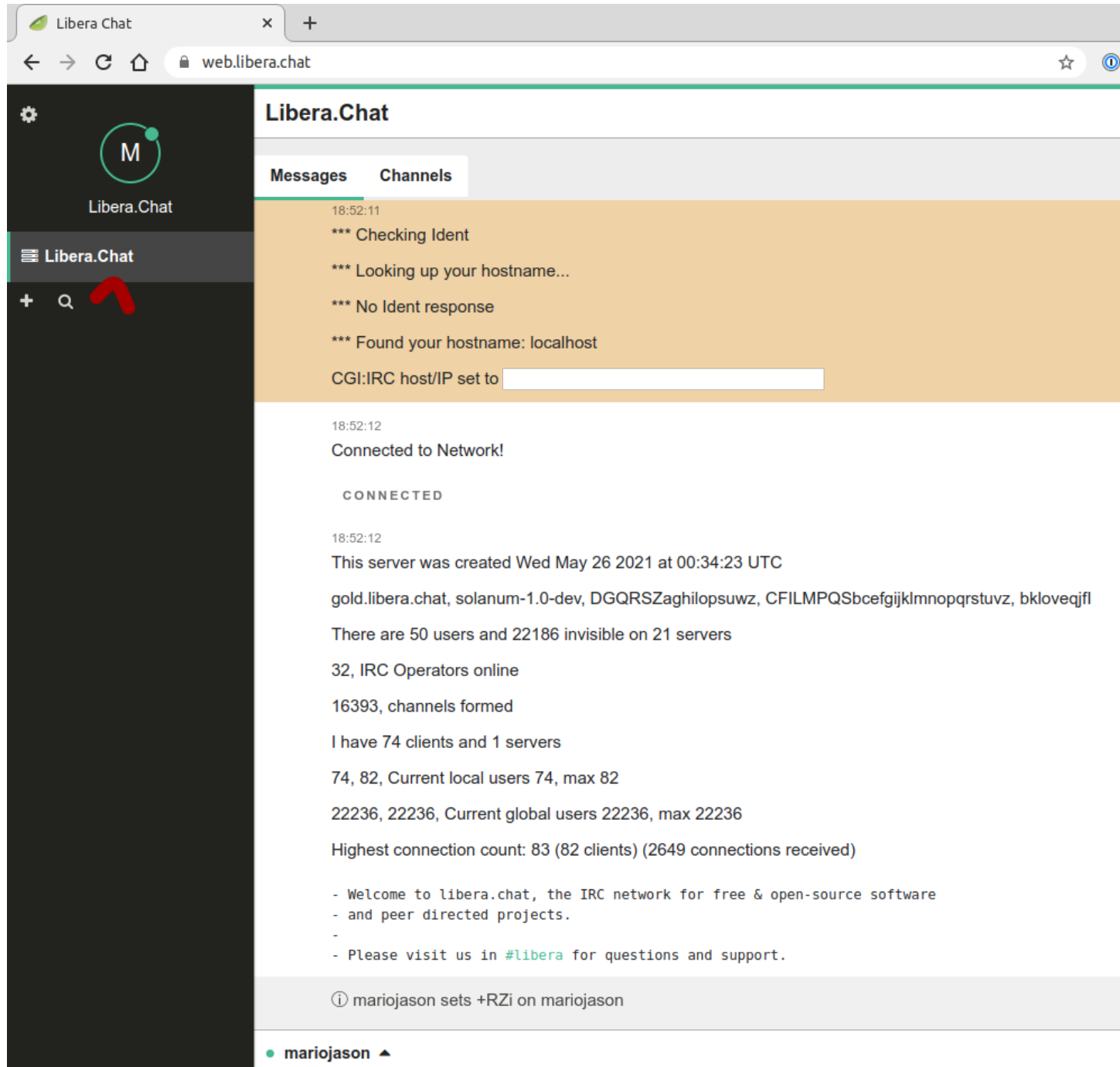
Channel

|

Start

And you should enter the world of irc!

There'll be a lot of stuff that'll end with a screen like this.



You'll obviously have figured out that the little white box at the bottom, next to your nickname is where you type in your messages and commands.

You can type `/quit` to quit your connection for example. (Don't do this yet)

Also note the tabs on the left, specially the one that you are currently on, the one that says "Libera.Chat" (pointed to with red) at the top left of your window.

You'll want to click this tab before typing in sensitive IRC commands (as you will do shortly).

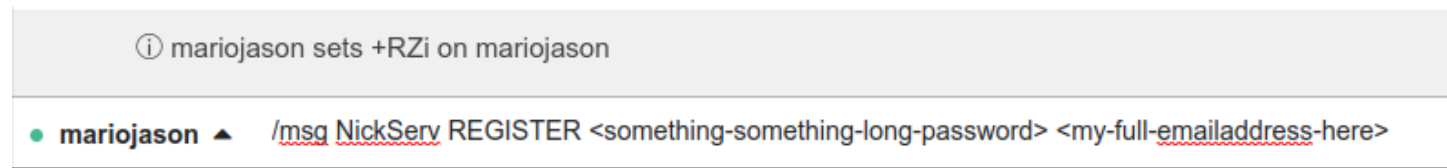
You'll see more tabs, as you join channels later and you'll use the tabs to switch between them.

You in with your username? Good.

Now let's register it so that we can always have the same one.

Type the command `/msg NickServ REGISTER <password> <email>`, where password will be some complicated password of yours while email is where you put in your email address

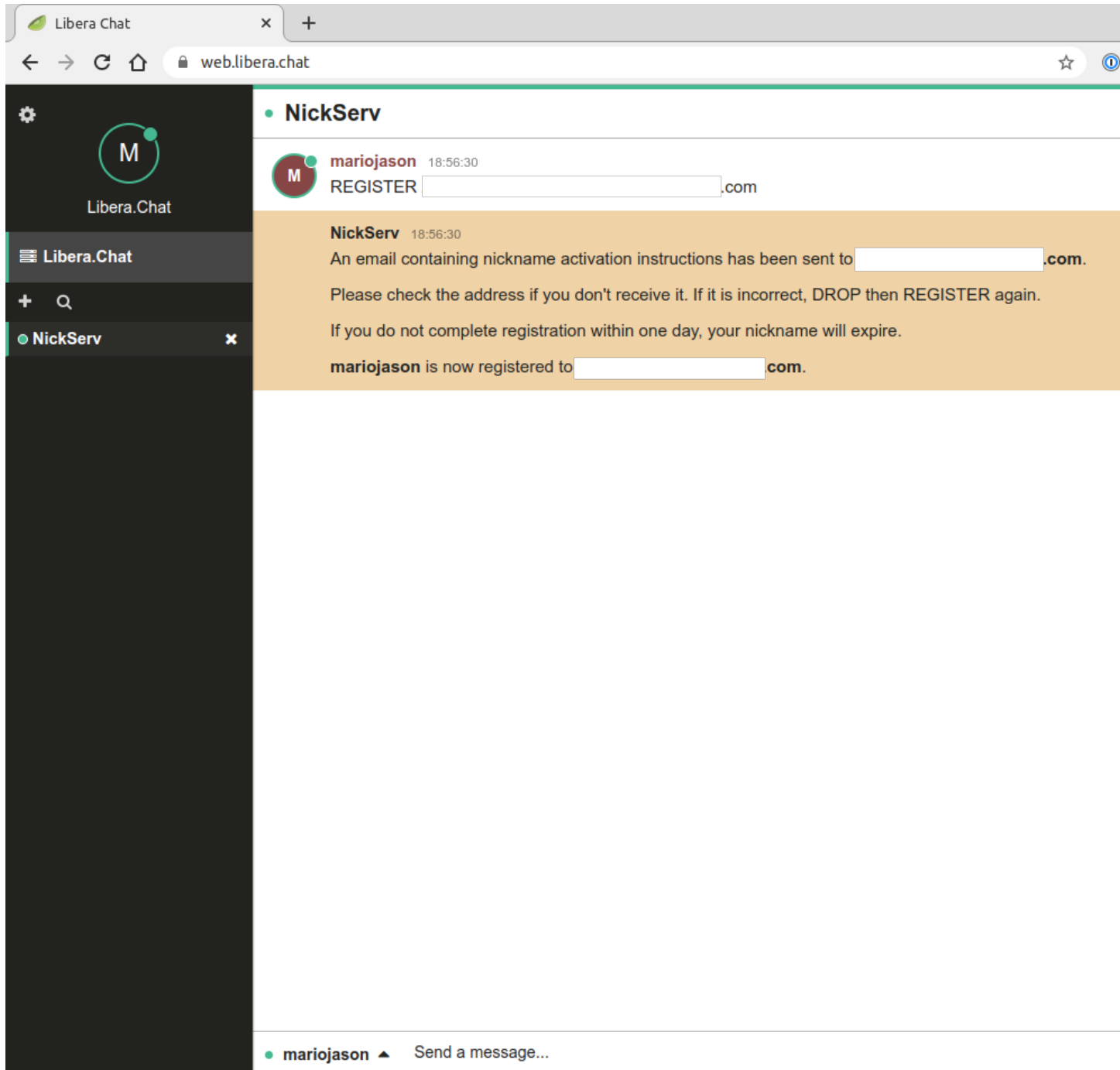
You can see me doing it below



If all works well, Nickserv will reply saying that activation instructions have been sent to your email id, like so (click the NickServ tab on the left to read) ...

So hop over and check your mail. This is what you should expect to see.

Let's copy the `/msg` line and go back to the irc page and paste it in the chat bar like so ...



Libera.Chat Account Registration Inbox x



Libera.Chat Network Services <noreply.support@libera.chat>

to mariojason ▾

mariojason,

In order to complete your account registration, you must type the following command on IRC:

```
/msg NickServ VERIFY REGISTER mariojason rZPrCl9i47fUnyFV
```

Thank you for registering your account on the Libera.Chat IRC network!

--

This e-mail was sent due to a command from mariojason[~]
at Fri, 28 May 2021 13:26:30 +0000. If this message is unsolicited, please contact support@libera.ch
with a full copy.



A screenshot of a chat window. On the left, there is a green circle next to the name 'mariojason' followed by a small upward-pointing triangle. To the right of this, the text '/msg NickServ VERIFY REGISTER mariojason rZPrCI9i47fUnyFV' is displayed. The text is underlined with a red dashed line.

And voila! You should be verified!

Now that we're done registering our nickname, quit the connection by typing in the `/quit` command and let's move to ...

9.9 Step 3. Connecting to the DGPLUG channel.

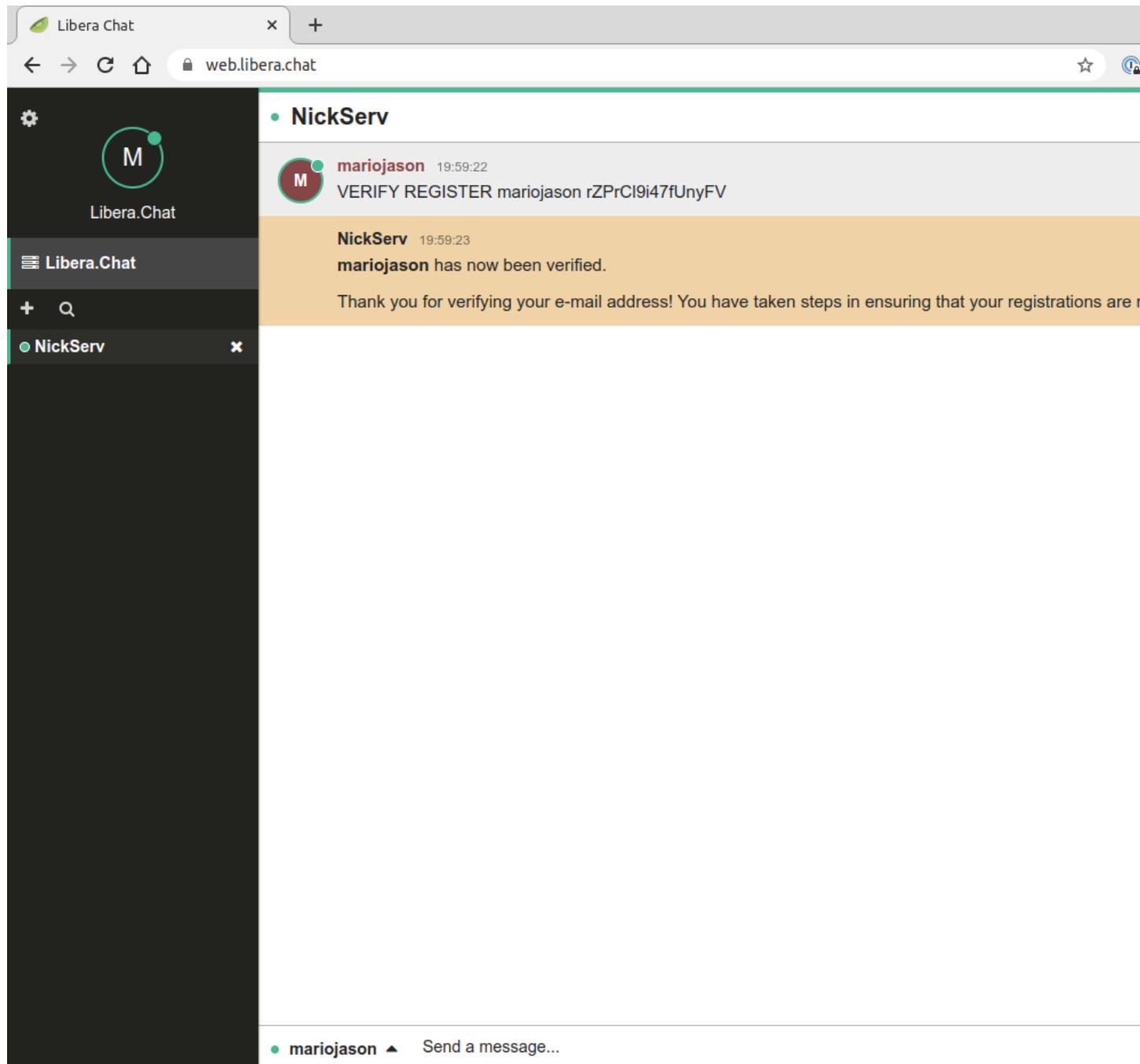
Now we're back to [where we started](#).

Only this time, fill in all the details.

1. Put in your nickname
2. Make sure the *I have a password* box is checked
3. Put in your password in the box that appears for you to type in.
4. Change the channel name to `#dgplug`

And hit Start!

You should login and you should be switched to a new tab with the `#dgplug` channel.



The screenshot shows a web browser window with the address bar displaying "web.libera.chat". The page title is "Libera Chat". On the left side, there is a login form with the following fields and options:

- Nick:** A text input field containing "mariojason".
- I have a password:** A checkbox that is checked.
- Password:** A text input field with masked characters (dots) and a toggle icon for visibility.
- Channel:** A text input field containing "#dgplug".
- Start:** A green button labeled "Start".

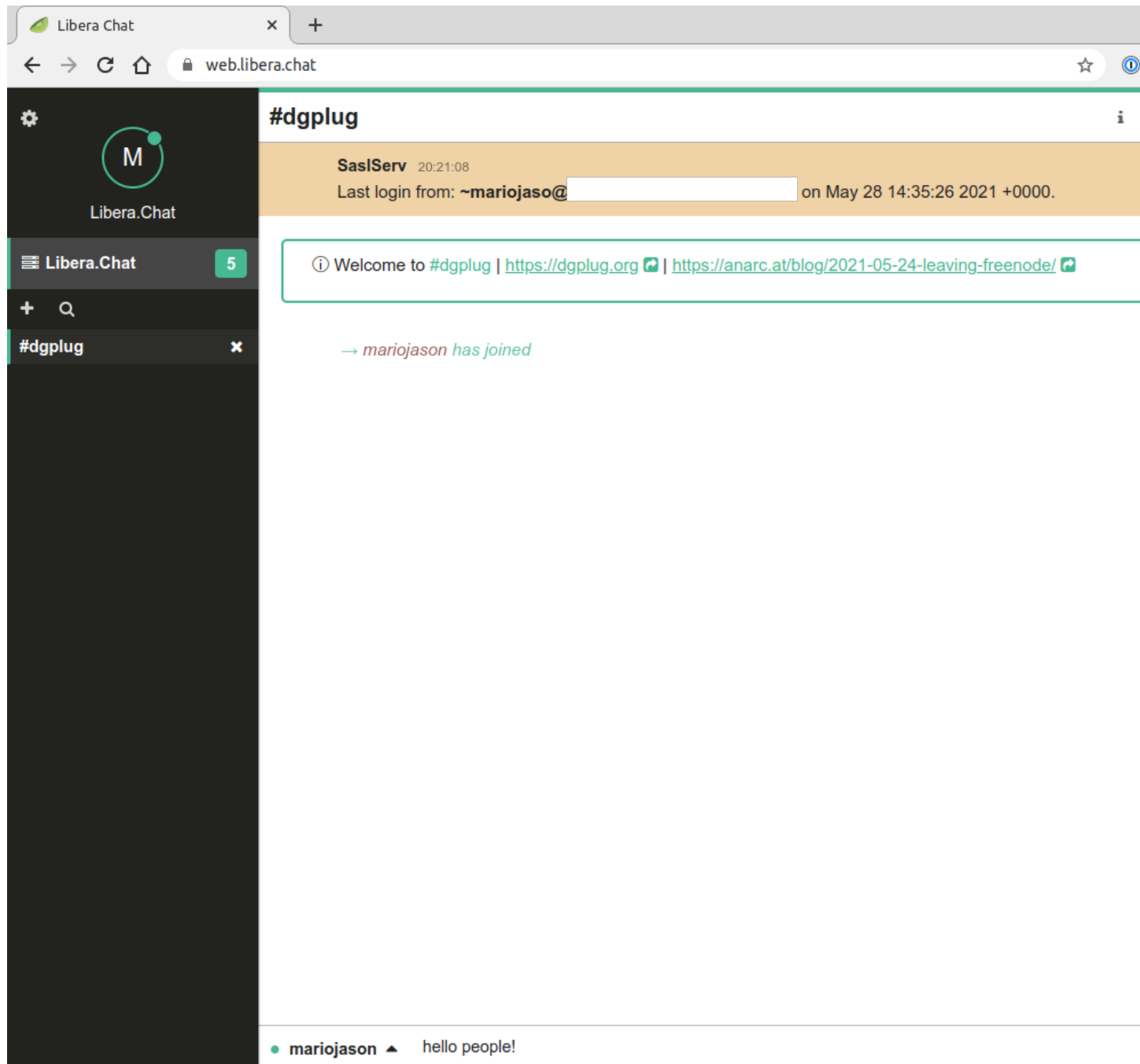
On the right side, there is a large dark gray area containing a light gray box with the following text:

[Libera Chat](#) is the IRC network for free & open-source software and peer directed projects.

For help using the network please visit #libera

Welcome home.

[Network Policies](#) - [Privacy Policy](#)



There! You're in! Welcome! Enjoy your time in the channel :)

9.10 Nick Ghosting

If for some reason, your nick lingers on after you are disconnected either due to a bad connection, or due to a [netsplit](#), you will be unable to use your nick again since it already is on the server. To remove the nick from the server, we need to **ghost** it. To do this, make sure you are authenticated to NickServ and execute the following command:

```
/msg nickserv ghost your_nick_name your_password
```


What is Tor? Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

The [Tor Project](#) is the most suggested project when it comes to protect privacy and anonymity. We suggest dgplug participants to download the Tor Browser, and start using it for regular Internet access from the beginning.

10.1 Why should you use Tor?

Watch this [youtube video](#).

Warning: Always download Tor Browser from the Tor Project website, do not download or use it from any other random website.

10.2 How to install and run Tor Browser?

Visit the [download page](#) and then download the *tar* file, and also the signature file. Please verify the download before you start using it, the steps for the same are given in [this page](#).

Note: You can open the image in a new tab to view it in proper scale.

The above graphics shows the steps, you can execute the desktop file to start the browser.

```
./start-tor-browser.desktop
```



You will see the above window when Tor Browser starts, just click on the **Connect** button, and then it will connect to the Tor network. For the first time the connection will take some time, afterwards it will be much faster.

10.3 For Windows users

Download the Tor installer from www.torproject.org and follow the steps as shown below.

10.4 How does Tor actually work?

Read this [overview page](#) to learn how does Tor actually works.

10.5 Getting more help

Please visit the new [supper stie](#) for any other query. You can also any question in our #dgplug channel too.

CHAPTER 11

Privacy

Before we talk about this issue, we think you should learn more about what is going on in the modern connected world. Please go through the following links first.

- [Nothing to Hide](#)
- [The House That Spied on Me](#)
- [Goodbye Big Five.](#)

Next round, watch the following talks:

- [Why privacy matters](#)
- [Edward Snowden Interview on Apple vs. FBI, Privacy, the NSA, and More](#)

CHAPTER 12

Assessing Your Risks

Note: This chapter is originally from [SURVEILLANCE SELF-DEFENSE](#) guide by EFF under the [Creative Commons Attribution License](#).

Trying to protect all your data from everyone all the time is impractical and exhausting. But, do not fear! Security is a process, and through thoughtful planning, you can assess what's right for you. Security isn't about the tools you use or the software you download. It begins with understanding the unique threats you face and how you can counter those threats.

In computer security, a threat is a potential event that could undermine your efforts to defend your data. You can counter the threats you face by determining what you need to protect and from whom you need to protect it. This process is called "threat modeling."

This guide will teach you how to threat model, or how to assess your risks for your digital information and how to determine what solutions are best for you.

What might threat modeling look like? Let's say you want to keep your house and possessions safe, here are a few questions you might ask:

12.1 What do I have inside my home that is worth protecting?

Assets could include: jewelry, electronics, financial documents, passports, or photos

12.2 Who do I want to protect it from?

Adversaries could include: burglars, roommates, or guests

12.3 How likely is it that I will need to protect it?

Does my neighborhood have a history of burglaries? How trustworthy are my roommates/guests? What are the capabilities of my adversaries? What are the risks I should consider?

12.4 How bad are the consequences if I fail?

Do I have anything in my house that I cannot replace? Do I have the time or money to replace these things? Do I have insurance that covers goods stolen from my home? How much trouble am I willing to go through to prevent these consequences?

Am I willing to buy a safe for sensitive documents? Can I afford to buy a high-quality lock? Do I have time to open a security box at my local bank and keep my valuables there?

Once you have asked yourself these questions, you are in a position to assess what measures to take. If your possessions are valuable, but the risk of a break-in is low, then you may not want to invest too much money in a lock. But, if the risk is high, you'll want to get the best lock on the market, and consider adding a security system.

Building a threat model will help you to understand threats that are unique to you and to evaluate your assets, your adversaries, and your adversaries' capabilities, along with the likelihood of risks you face.

12.4.1 What is threat modeling and where do I start?

Threat modeling helps you identify threats to the things you value and determine from whom you need to protect them. When building a threat model, answer these five questions:

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

Let's take a closer look at each of these questions.

12.4.2 What do I want to protect?

An **asset** is something you value and want to protect. In the context of digital security, an asset is usually some kind of information. For example, your emails, contact lists, instant messages, location, and files are all possible assets. Your devices may also be assets.

Make a list of your assets: data that you keep, where it's kept, who has access to it, and what stops others from accessing it.

12.4.3 Who do I want to protect it from?

To answer this question, it's important to identify who might want to target you or your information. A person or entity that poses a threat to your assets is an **adversary**. Examples of potential adversaries are your boss, your former partner, your business competition, your government, or a hacker on a public network.

Make a list of your adversaries, or those who might want to get ahold of your assets. Your list may include individuals, a government agency, or corporations.

Warning: Depending on who your adversaries are, under some circumstances this list might be something you want to destroy after you're done threat modeling.

12.4.4 How bad are the consequences if I fail?

There are many ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data.

The motives of adversaries differ widely, as do their attacks. A government trying to prevent the spread of a video showing police violence may be content to simply delete or reduce the availability of that video. In contrast, a political opponent may wish to gain access to secret content and publish that content without you knowing.

Threat modeling involves understanding how bad the consequences could be if an adversary successfully attacks one of your assets. To determine this, you should consider the capability of your adversary. For example, your mobile phone provider has access to all your phone records and thus has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted communications. Your government might have stronger capabilities.

Write down what your adversary might want to do with your private data.

12.4.5 How likely is it that I will need to protect it?

Risk is the likelihood that a particular threat against a particular asset will actually occur. It goes hand-in-hand with capability. While your mobile phone provider has the capability to access all of your data, the risk of them posting your private data online to harm your reputation is low.

It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in Stockholm (where they are not).

Conducting a risk analysis is both a personal and a subjective process; not everyone has the same priorities or views threats in the same way. Many people find certain threats unacceptable no matter what the risk, because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

Write down which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about.

12.4.6 How much trouble am I willing to go through to try to prevent potential consequences?

Answering this question requires conducting the risk analysis. Not everyone has the same priorities or views threats in the same way.

For example, an attorney representing a client in a national security case would probably be willing to go to greater lengths to protect communications about that case, such as using encrypted email, than a mother who regularly emails her daughter funny cat videos.

Write down what options you have available to you to help mitigate your unique threats. Note if you have any financial constraints, technical constraints, or social constraints.

12.4.7 Threat modeling as a regular practice

Keep in mind your threat model can change as your situation changes. Thus, conducting frequent threat modeling assessments is good practice.

Note: Create your own threat model based on your own unique situation. Then mark your calendar for a date in the future. This will prompt you to review your threat model and check back in to assess whether it's still relevant to your situation.

CHAPTER 13

Good practices

Here are a few suggestions on good practices while using computers daily life. In this guide we mentioned a few major habits or tools., and then we also provide links to documents to learn more about those habits or tools.

Note: You should read the previous chapter first, and then only start reading this chapter.

Warning: But, always remember, no technology can help user errors. So, think before you click any link or execute any random command.

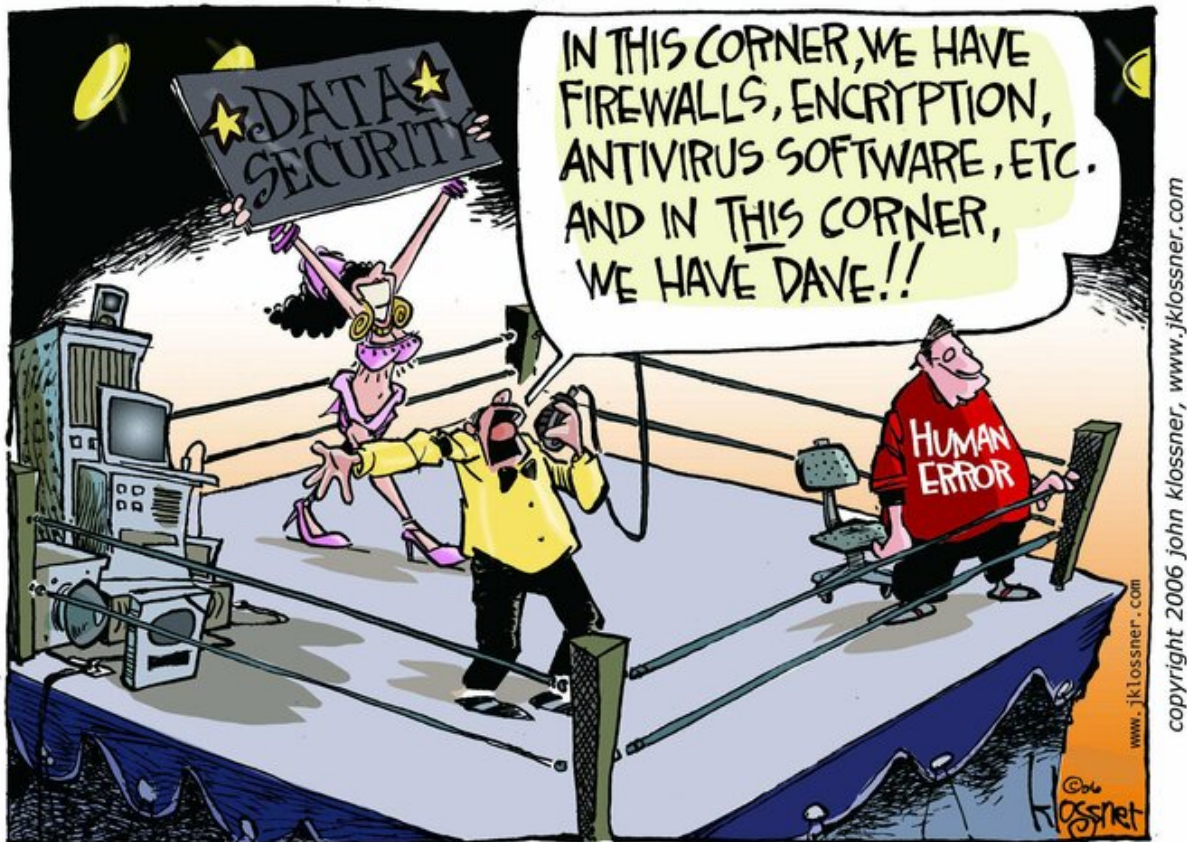
13.1 Keep your machine updated

Always keep all the software updated. There are always new security updates available, and we should install them as soon as possible. This is true not only for normal computers, but, also for mobile phones and any other modern smart home internet things.

If you don't update your computer regularly, or else an attacker can find out the vulnerabilities in older version of the software or in the older version of the operating system you are running and attack your computer. Remember your threat model, think about what all things can go wrong if someone gets access your computer because of older vulnerable software.

13.2 Use strong and unique passwords

We should use unique passwords in different places. Otherwise, if someone can get hold of one of your password, they can break into other sites/places with the same password. We suggest using [diceware](#) to generate all of your passwords. To learn more, please read [this blog post](#).



13.3 Use password managers

Password managers will help you to store all of those long passphrases in one place. Learn from the guide about [password managers](#). KeePassXC is a good option on desktop.

Bitwarden is a good starting option for newbies. Many of us also use 1Password as password manager.

13.4 Do not keep the computer unlocked

If you are not in front of the computer, then always lock the screen. Do not keep the computer unlocked, let it be inside your house, or in your hostel, or in anywhere else. This is again an habit, and it takes time to make this habit. Having the computer always password protected will make sure that any person can not directly access your computer even if you are not front of the computer for few minutes.

The following is an [incident](#) where a child typed things in to the Twitter account of the US Strategic Command.



US Strategic Command ✓ @... · 31m :
;l;;gmlxzssaw

1,557 6,664 8,549



US Strategic Command ✓ @U... · 1m :
Apologizes for any confusion. Please
disregard this post.

110 107 400

13.5 Cover up your webcam

Over the last few years it became very well known that big agencies and criminals can access people's webcams and record without anyone knowing. Covering up your laptop webcam will protect you at one level against these criminal activities. Here is [story](#) which talks about how the FBI director also puts up a tape on his laptop's webcam.

13.6 Take regular backups

One should always backup their computer, and if possible more than one backup copy. For example, you should at least backup your ssh keys, gpg keys, and all other important configs in couple of **encrypted usb drives**.

Note: Learn how to encrypt your USB drives below

13.7 Enable 2 factor authentication (2FA)

Enable 2 factor authentication in all the websites or applications (if they allow it). This will provide a second layer of security incase someone finds your password.

If possible also stay away from SMS based 2 factor authentication. Instead, use the mobile applications like **FreeOTP**, **Google Authenticator**, **Authy**. These generates time based tokens which can be used as 2FA.

To learn more, read [the guide](#) on 2FA.

To know more which all sites provides 2 factor authentication, visit <https://twofactorauth.org>.

13.8 Encrypt all USB drives

While installing Linux in your system, you can encrypt the whole drive. This will help in case your laptop is stolen or taken away by someone. This also means try to keep your laptop in shutdown state most of the time, so that to boot the system, one will have to provide the encryption password.

- For mac follow this [guide](#).

Note: Use [Veracrypt](#) to encrypt all removable drives. Follow [this guide](#) to learn the usage.

The same goes to the all USB devices you use. We have much bigger chance to misplace or forget about small USB devices. [How to encrypt USB devices using LUKS](#) has all the details you need to know to encrypt or decrypt any USB device.

Once again this is tied to your threat model, if you share or copy any kind of sensitive documents (or example personal photos, or bank documents, or vital other documents), having them in an encrypted device will help in case the drive gets lost, or stolen.

13.9 Do not download and install random software from internet

Do not download software from any random site and install them on your computer. They may have malware or virus in them, which can attack not only your computer, but also all the computers in the network. The same goes about any software which says to execute some random shell script from internet.

On the other hand, one should always check different applications installed in a computer, and remove the applications which we are not using regularly. This will reduce the attack surface.

13.10 Do not plug random USB devices into your computer

If you ever find any random USB device in the parking lot, or on footpath, or in college, do not plug that into your computer. This is one easiest way people spread malware and systems get compromised. The same goes for [any USB device handed over in a conference](<https://www.bbc.com/news/technology-43128073>) or by booths at the street side.

13.11 Use the following browser plugins for better privacy

- [HTTPS Everywhere!](#)
- [Privacy Badger](#)
- [Disconnect.me](#)

Install the above mentioned plugins in your favorite browser. They are available for both Firefox and Google Chrome browsers.

13.12 Do not trust private browsing mode to save your privacy

Read this [document](#).

13.13 Use Tor for almost everything

Start using Tor browser for daily life. Read the previous chapter on Tor Project to know more. You may want to split your browsing between different browsers. For example, you can use one of the browsers (Firefox or Google Chrome) for your email and github accounts, one for all banking purpose. And then use Tor for the rest.

If you start using Tor Browser for social media sites like Facebook or Twitter, or reading different news websites, it will be difficult for anyone to track your browsing history. Tor Project [published a blog](#) post explaining this in details.

Your local ISP will know that you are using Tor, but, they will not have any clue about what all sites you are visiting. Visit [the EFF site](#) to understand who all can see which part while you are using Tor.

One strategy can be using more than one browser, say using Google Chrome for your gmail or youtube accounts, and then use Firefox for banking and other important tasks. Then you can move all of your other browsing in the Tor Browser.

13.14 About communication tools on phone

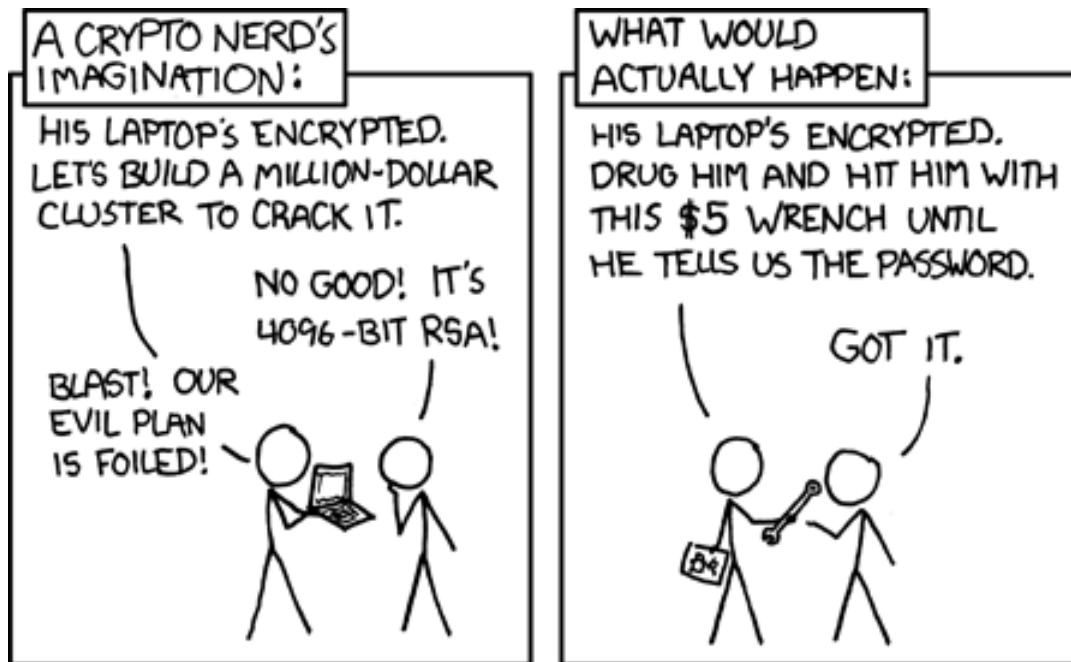
Do not use *Telegram* or even have it installed on your phone. You can use [Signal](#) for any kind end-to-end encrypted communication from your phone (it is available for your Linux desktop too). Martin again wrote another [amazing guide](#) for Signal.

Also always remember that end-to-end encryption does not mean no one can ever read your messages, the other person can lose the phone or someone may steal your phone. Some times some friend may just want to check those amazing photos on your phone, and then click on the Signal app and read all the messages there.

(Original work: <https://www.xkcd.com/538/>)

13.15 Do not click on random links in emails or from anywhere else

Many people are attacked by simple phishing attacks where someone sends a random link (which looks like a normal known website URL). They many times also provides downloads and ask the victims to download and open those attachments in the victim's computer.



To avoid from any such phishing attacks, make sure that don't click on any URL in emails or random websites. Also, always think about any email attachments, before downloading or opening those files. The same goes to any PDFs you receive over email.

<https://www.youtube.com/watch?v=iJcQNgVtH8Y>

13.16 Do not install random certificate on the browser

Do not trust any random certificate from internet. Only trust the certificates come as bundled with the browser. For example, in [this tweet](#) one government agency asked people to install a certificate from Root Certifying Authority of India. But, the same is [already blacklisted](#) for issuing fake certificates.

13.17 SURVEILLANCE SELF-DEFENSE

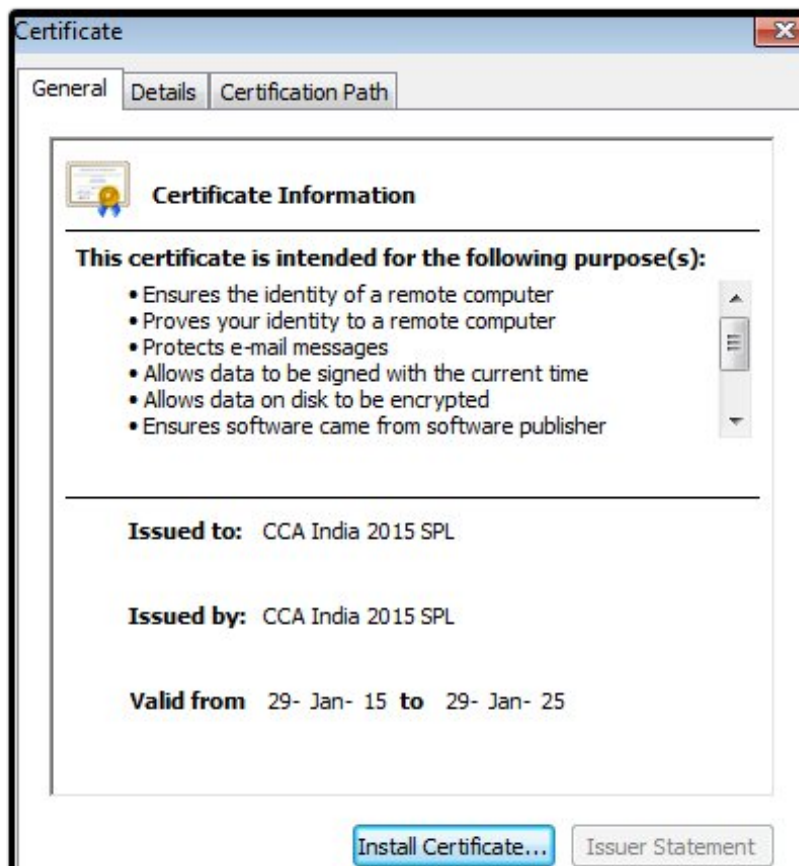
Now read [SURVEILLANCE SELF-DEFENSE](#), you will get a chance to know things in much more detailed level.

**NCIIPC India** ✓

@NCIIPC

[Follow](#)

Viewers of @NCIIPC web portal are getting security error in certain browsers due to unrecognized root certificate of Root Certifying Authority of India (#RCAI). Follow user manual for installation of required root certificate to avoid such warning [nciipc.gov.in/documents/User ...](http://nciipc.gov.in/documents/User...)



8:32 AM - 27 Apr 2018

CHAPTER 14

Talks from around the world

Below are a few talks on OPSEC from different conferences around the world.

- [DEF CON 22 Blinding The Surveillance State](#)
- [#HITB2012KUL D1T3 - The Grugq - OPSEC: Because Jail is for wuftpd](#)
- [We're Not Equally Vulnerable to Surveillance | Chris Soghoian at MozFest](#)
- [DEF CON 22 - Robert Rowley - Detecting and Defending Against a Surveillance State](#)
- [OPSEC for security researchers](#)

This is short three part series on writing and blogging.

Follow this advice, and you'll be better than half of the programmer blogs out there!

15.1 1. Why do we need a blog? Why do we need to write?

15.1.1 Your blog should be your home on the web¹.

While it's all fine and dandy to have your github profile and your medium presence and your twitter thingamajig, always remember that you don't [control those services](#).

Neither is there any assurance, [that they will last](#).

You'll find a lots of links here to [Seth Godin](#), [Brent Simmons](#), [Dave Winer](#)² and our very own [Kushal Das](#).

Why?

Because they have blogs.

They controlled their message.

They started early and never stopped. [Seth](#), [Dave](#), & [Brent](#) have been writing online since the mid to late 90s; [Kushal](#), since the early oughts.

15.1.2 Your blog is the easiest way of controlling your message.

Think you can host videos the way you want to? Not unless you're Mr.Moneybags.

How about audio? Well, imagine the setup and the time and effort.

All you need to blog is consistency, a computer and an internet connection.

Can be online? Can blog!

¹ Now that you're learning here, it will be :)

² Inventor of RSS, Blogging & Podcasting and the longest running blog on the net

And as you grow, you can scale your blog to all levels of crazy & fanciness. (if you so choose)

15.1.3 Blogs make it easy for people to reach out to you.

You can share all you know. Your thoughts, your opinions, your own way of serving the world.

Stick to it long enough and the world will beat a path to your door.

For a long, long while (nearly a decade) Seth was the first result when you searched Google for the word blog.

With a reach like this, do you think any of our heroes have trouble finding new projects or things to do?

15.1.4 Blogs are measure of growth.

I think this is Kushal's [second post](#), (he was a college kid) on his blog in 2004.

Today junies came to the hostel. Now it sems that we r being ragged by our management. Carrersangi's work will be started after 16th of this month.

Today (2018), nearly eighteen years later Kushal speaks of moving on, and [touching new heights with his career and defending online rights in India](#).

Reading his blog through the years, shows you a clear through line as he made his way in the world, what he learnt, where he went, what he did and how he got to where he is.

Reading [Dave's](#) blog shows how he rolled his way from xml to [rss](#) to [blogs](#) to [podcasting](#) to [outlining tools](#) over the years. There's a [neat summary](#) at Brent's page.

This could be you too ...

And while all those are good and valid external reasons, my favorite reasons to have a blog, to write regularly, are the *internal ones*.

15.1.5 Writing sharpens your mind.

- You start writing.
- You write a lot of puff.
- You get into the habit of writing.
- You gain discipline.
- You gain mental clarity.
- You think critically
- You gain deep understanding of your thoughts as you put pen to paper (or keys to screen)
- You learn how to communicate those thoughts in a manner that is assertive, yet open to feedback
- Your learn to get to the heart of the idea.

And these are the reasons, the real reasons, you ought to learn to write.

[Seth Godin](#) concises it better than I ever could.

If no one reads your post, does it exist? *What do most people get out of blogging? After all, most blogs are virtually unread by outsiders. . .*

The act of writing a blog changes people, especially business people. The first thing it does is change posture. Once you realize that no HAS to read your blog, that you can't MAKE them read your blog, you

approach writing with humility and view readers with gratitude. The second thing it does is force you to be clear. If you write something that's confusing or in shorthand, you fail.

Respectful and clear. *That's a lot to get out of something that doesn't take much time.*

15.2 2. Blogs, how do you set one up?

This is the simplest section of all.

You could, of course, if so inclined, do your research and figure out what you want amongst the 3 major platforms and 7–10 minor ones. Paid, free, hosted, self hosted, Github pages ... hours of fun :)

Or if all of this sounds intimidating and scary, simply go sign up for a free account and start up a [blog at Write.as](#).

The important thing right now, is to actually get something up and running with minimal fuss, so that you can **start writing regularly**.

You can always move to something you want later.

[Click here to get started.](#)

15.3 3. Tactical Advice

In order to have a good blog, in order to write well ...

1. You must want to write.
2. You must make the time to write.
3. **You must write. A lot.**
4. Write on a schedule.
5. **Consistency is key.** In fact, in the beginning, consistency matters more than quality. Have a rhythm. Once a day, twice a week, every other day. And then show up. Stick to the rhythm.

That's it. Everything below is just frosting on the cake.

15.3.1 Structuring and writing a post.

1. Make a template to write to. Use it over and over. Here's a simple one. Search for more. Make your own. It's just an aid, so that you don't have to scratch your head wondering *how* to write, when all you want to do is write ...
 - a. Title
 - b. Short introduction
 - c. Write what you wanted to write
 - Write about What

- Write about Why
 - Write about How
 - Write about When
 - d. Give an example
 - e. Summarise and conclude
2. Get to being creative.
 - a. Write like you've solved the biggest problem in the world
 - b. Create obstacles and then solve them.
 3. Use titles and subtitles.
 - a. Make the post scannable (a reader should get the gist, just reading the sections and subsections)
 - b. Try to flow from one section to the next
 - c. There's reason daily soaps cut in the middle of a scene
 - d. Emphasize items of importance
 4. Use paragraphs
 - a. Do short lines
 - b. Make them punchy!

15.3.2 General writing suggestions

- As you grow, niche down. (general suggestion for a professional blog). Go from a something you're learning about, to something you become an authority on.
- Yes, other people have written about what you have. But no one has *your* voice. So if you feel like writing about it, **write about it**.
- Use grammar and punctuation well.
- **Use a grammar checker.**

Warning: Note of caution. If you'll be using Grammarly, only use the Grammarly website. Don't install the browser extension. (Those can let someone, snoop into everything you type or do in your browser.)

- Use a [Style Guide](#).
- Get to know them well.
- Know these are only conventions. Break them at will :)

And in the end, while it is your blog, don't let it be about you.

It's about [your journey](#).

The obstacles you faced.

How you overcame them and how **you seek to help others** with the the wisdom and experience you've now gained.

Some author in the past shared this good advice in an interview ...

What advice would you give to aspiring writers trying to decide their next move?

Do aspiring writers need any more advice?

Alright, you asked so I should answer.

Here's all I got:

Read more than you write, live more than you read.

15.4 4. Bonus References

Just as I was done with this little section, Seth Godin released an episode about blogging on his podcast.

And obviously, he does a much better job than me, explaining the whys and wherefores of blogging.

You can find [the episode](#) and [the entire transcript](#) here.

I also write and share inspiring and tactical posts on writing on [my blog](#).

CHAPTER 16

Book suggestions

Books are marked as [S] as for starters.

16.1 General topics

- Hackers: Heroes of the Computer Revolution [S]
- Hackers & Painters: Big Ideas from the Computer Age. Paul Graham. [S]
- Linux and the Unix Philosophy. Mike Gancarz. [S]
- Free as in Freedom. Richard Stallman. ([https://en.wikisource.org/wiki/Free_as_in_Freedom_\(2002\)\)](https://en.wikisource.org/wiki/Free_as_in_Freedom_(2002))) [S]
- Open Sources, Chris DiBona & Sam Ockman (free to read here - <https://www.oreilly.com/openbook/opensources/book/index.html>)
- The Architecture of Open Source Applications. (<http://aosabook.org/en/index.html>) [S]
- Ghost in the Wires
- Mother American Night

16.2 Writing & Blogging

- On Writing, Stephen King[S]
- Bird by Bird, Anne Lamott
- On Writing Well, William Zinsser
- English Composition and Grammar. John E. Warriner. [S]
- Good English: How to Write It. G. H. Valins. [S]
- The Elements of Style. Willam Strunk Jr. and E. B. White. [S]

16.3 Design & Presentations

- The Non-Designer's Design Book, Robin Williams[S]
- The Non-Designer's Presentation Book, Robin Williams (for creating)
- Presentation Zen, Garr Reynolds (for creating)
- Confessions of a Public Speaker, Scott Berkun (for delivering)
- Don't Make Me Think, Steve Krug
- Visualize This. Nathan Yau.

16.4 General programming

- i want 2 do project. tell me wat 2 do (<http://www.shakthimaan.com/what-to-do.html>) [S]
- Men of Mathematics, E. T. Bell.
- Programming Pearls. Jon Bentley.
- Functional Thinking. Neal Ford.
- A Discipline of Programming. Edsger W. Dijkstra.
- The Passionate Programmer. Chad Fowler. [S]
- 97 Things Every Programmer Should Know. Kevlin Henney. [S]
- How to Prove It. A Structured Approach. Daniel J. Velleman. [S]
- Programming Language Pragmatics. Michael L. Scott.
- Thinking Mathematically. J Mason, L Burton, K Stacey.
- Patterns of Software: Tales from the Software Community. Richard P. Gabriel
- Program Construction. Roland Backhouse.
- Small Memory Software. Charles Weir, James Noble.
- Beautiful Code. Leading Programmers Explain How They Think. Andy Oram, Greg Wilson. [S]
- Beautiful Testing. Tim Riley, Adam Goucher. [S]
- Beautiful Data. Toby Segaran, Jeff Hammerbacher. [S]
- Discrete Mathematics using a Computer. John O'Donnell, Cordelia Hall. [S]
- Discrete Mathematics for Computing. Peter Grossman. [S]
- C Interfaces and Implementations: Techniques for Creating Reusable Software. David R. Hanson.
- Expert C Programming. Peter van der Linden.
- The Pragmatic Programmer: From Journeyman to Master. Andrew Hunt. David Thomas. [S]
- Agile Software Development: The Cooperative Game. Alistair Cockburn. [S]
- Refactoring: Improving the Design of Existing Code. Martin Fowler, Kent Beck et. al.
- The Mythical Man-Month [S]

16.5 Productivity

- The 7 Habits of Highly Effective People. Stephen R. Covey. [S]
- How to Get More Done: Seven Days to Achieving More. Fergus O' Connell. [S]
- How to Win Friends and Influence People. Dale Carnegie. [S]
- Beautiful Teams. Andrew Stellman, Jennifer Greene. [S]
- Mastery, Robert Greene
- Deep Work, Cal Newport
- The War of Art, Steven Pressfield
- Do the Work, Steven Pressfield
- Tuesdays with Morrie. [S]

To learn about commands of a GNU/Linux system, start reading [Linux command line for you and me](#) book.

CHAPTER 17

Indices and tables

- `genindex`
- `modindex`
- `search`