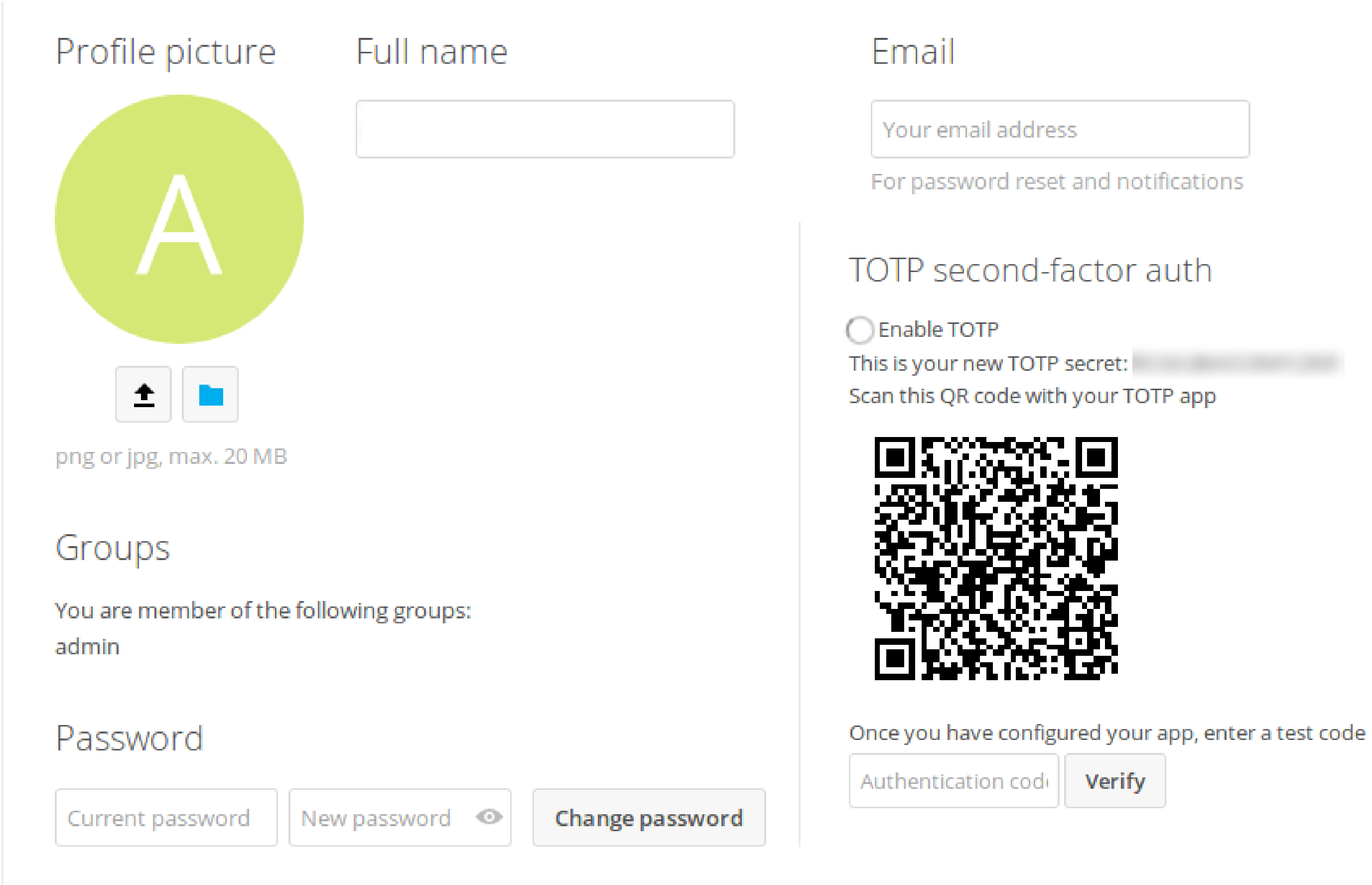
GIBBERFISH QUICKSTART

Welcome to Gibberfish! Our focus is on your privacy and security, but we need you to be an equal participant. Below are a couple of suggestions to get you started.

PROFILE

If this is your first time logging in, you should take a few minutes to fill out your profile, and while you’re there change your passphrase! Click on the ⚙ in the upper right corner and choose **Personal** to edit your profile.



Profile picture

A

png or jpg, max. 20 MB

Groups

You are member of the following groups:
admin

Password

Current password | New password | Change password

Full name

Email

Your email address

For password reset and notifications

TOTP second-factor auth

○ Enable TOTP

This is your new TOTP secret: [redacted]

Scan this QR code with your TOTP app

Once you have configured your app, enter a test code

Authentication cod | Verify

PASSPHRASES

Good passphrases are extremely important for safeguarding your data. We (and many security experts) recommend creating passwords using the Diceware method. **This is the only method** of passphrase generation we consider secure. Its easy to do, and it provides ultra-strong passphrases that can defeat even the most resourceful adversaries.

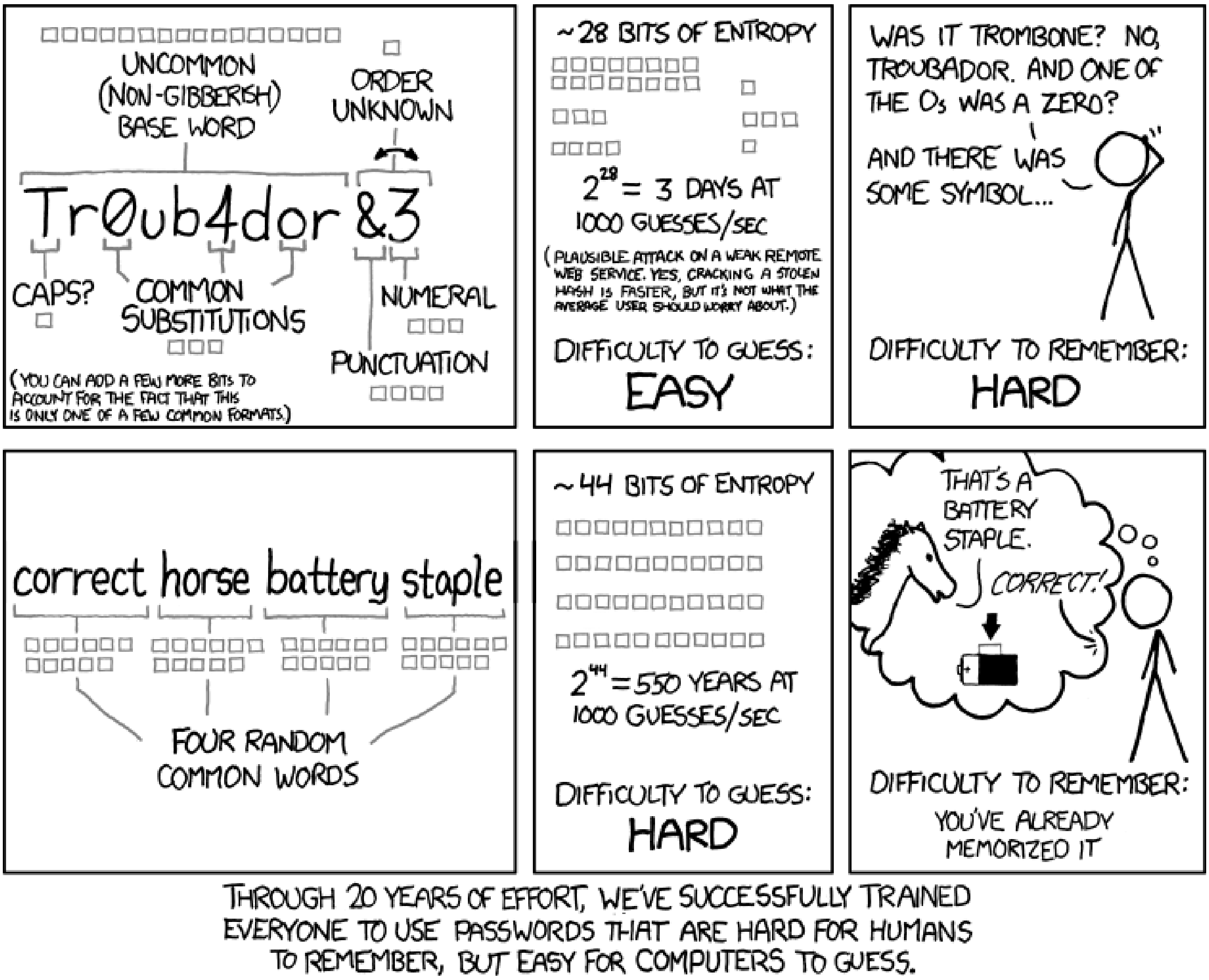

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Image courtesy xkcd.com.

While the comic above explains the concept, the Diceware method recommends a passphrase length of **5 or more words** for optimal security.

Never use a passphrase for your Gibberfish login that you use anywhere else.

Always generate a unique passphrase for any service, account or device.

TWO-FACTOR AUTHENTICATION

Once you’ve changed your passphrase, we also strongly encourage you to enable Two-Factor authentication (“2FA”). This involves installing an app on your mobile device that generates a unique 6-digit code you must enter each time you log in. For someone to hack your account, they would need to know your passphrase *and* physically possess your phone. This combination keeps you more secure. Because Gibberfish is part of the Nextcloud ecosystem, you can use the Nextcloud 2FA app. This app supports FreeOTP, which can be downloaded in the app store for Android and iOS devices.

KEY VAULTS

If you’re not already in the habit of doing so, it would be a good idea to store your passphrases in a key vault like KeePass. Key vaults make it easy to securely remember all your passphrases. You will need to lock your key vault itself with a Diceware generated passphrase. In addition, we **strongly** recommend you enable full-disk encryption on the device storing your key vault.

Using this method ensures you only need to remember one passphrase: the one to unlock your key vault.

DIGITAL HYGIENE

Good Digital Hygiene is the consistent use of robust security practices.

By ‘robust’ we mean procedures that have been established or vetted by trusted security experts. These include, but are not limited to, the Electronic Frontier Foundation (EFF), the Guardian Project and Tor project.

We use ‘consistent’ to emphasize that the intermittent use of any security practice is as bad as not using one at all. Once you develop a threat model and a strategy to defeat it, you must apply that strategy **every** time you engage in private activities.

THREATS

Understanding the threats you and your group will encounter is an important step in establishing a useful security strategy. The goal is to use only the techniques necessary to protect against your likely adversaries. This will prevent your security regime from becoming so burdensome that you stop using it. Your administrator may have already created a Threat Model describing the security challenges you and your group may expect. If you are unsure, please contact them and ask.

Every user must understand your group’s Threat Model and consistently use the same security practices.

For more information on Threat Models, please refer to this excellent primer produced by the EFF.

EXISTING COMMUNICATIONS

It is likely that you are adding Gibberfish to a variety of existing accounts and services associated with your online activities. These older accounts and services may already be compromised. We recommend using fresh accounts for any activity that involves your Gibberfish server, the content stored there, or the activities associated with it.

We recognize that this is not always convenient or appropriate for every user. In this case, please take the time to re-secure any account or service you intend to use for private activities. Change your passphrases in order to lock-out unauthorized users who may have gained access without your knowledge. Wherever possible, enable two-factor authorization. Check for software updates for all your devices, including your phone, and install them.

TOR

Using Tor is the single best way to guard your online privacy. This is why we use Tor to deploy your Gibberfish server. While it specifically refers to **T**he **O**nion **R**outer project, Tor has come to encompass a variety of free products and services people can use to safeguard their online activities. We recommend that everyone use the Tor browser to help anonymize their online presence.

Please carefully read the documentation and FAQ that Tor provides about browsing on their network. They have important recommendations for maintaining your privacy. Importantly, using the Tor browser does not guarantee that all your online activities are anonymous.

As your security needs escalate Tor has other free tools to help. When you evaluate your Threat Model, you may wish to investigate Bridge servers and Tails. Bridge servers allow people to access Tor in countries that block it. Tails is a Linux operating system, complete with commonly used programs, all on a USB stick. It allows extremely private computing.

Discover these and other Tor services at:

https://www.torproject.org/projects/projects.html.en

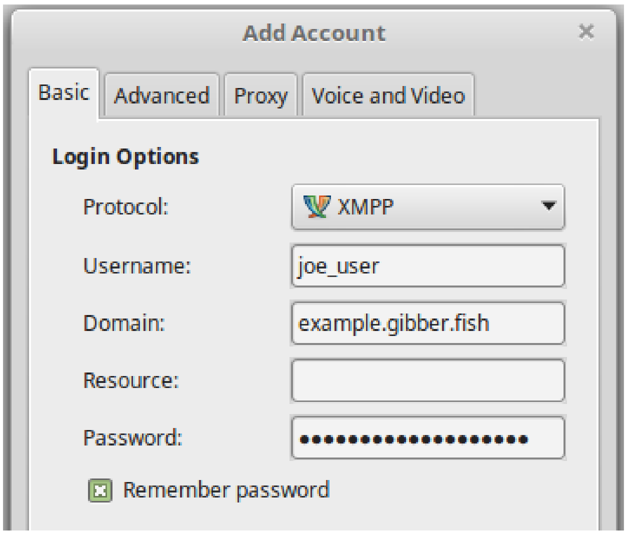
CHAT

The chat system uses the standard XMPP protocol, which will allow you to chat not only with fellow Gibberfish users, but also with anyone else in the world using an XMPP server. Your XMPP address is <your username>@<your gibberfish server>. For example,

joe_user@example.gibber.fish

When you first log in, your chat roster on the right side of the screen will be empty. From the menu at the bottom you can **Add Contact**. Just start typing and it will automatically search for existing users on the server, or you can type in the XMPP address of external users.

To stay connected when you're not logged in to Gibberfish, you can also connect to the server directly using an XMPP-compatible client such as Adium, Pidgin, or one of many mobile apps.



Login Options

Protocol: XMPP

Username: joe_user

Domain: example.gibber.fish

Resource:

Password: •••••••••••••••••••

☒ Remember password

The chat server is also reachable as a Tor “onion service” on port 5222. Ask your administrator for your server’s Tor address.

However, when chatting with users outside your server, you have no guarantee of privacy unless you **and** your contacts use an end-to-end encryption plugin such as “OTR”. Most chat clients support end-to-end encryption, and have guides to help you understand and enable it.

DESKTOP AND MOBILE CLIENTS

Gibberfish works with the Nextcloud desktop and mobile clients to allow you to automatically sync files to and from the server. This is disabled by default as a security measure. If you wish to use these clients, talk to your Administrator about changing the file access rules. If you decide to sync files locally, **only do so** if you have turned on full-disk encryption for your device. This protects your files if your device is lost, stolen or hacked

It is difficult, but possible, for your data to be intercepted by resourceful adversaries while in transit. For this reason we **do not** recommend syncing your data without carefully considering your Threat Model and your security practices.

FURTHER READING

For more extensive documentation of the core features, please refer to the Nextcloud User Manual, which is also located in your Gibberfish home folder.

Administrators should also familiarize themselves with the Admin Manual.

Finally, we recommend subscribing to the Gibberfish Blog in the News app to keep up to date on important announcements and our canary statement.

FINAL NOTES

We hope you enjoy using Gibberfish. We have worked hard make it a secure and easy-to use platform, as have the *many* independent contributors to the various open source projects that we have integrated into our service. Special thanks goes to the folks at Nextcloud, without whom our platform would not be possible.

We rely on donations to survive. If you can afford it, please consider making a charitable contribution of any amount at https://gibberfish.org/donate. We will appreciate it immensely. Thanks!

For security reasons, we only respond to requests from your registered Administrator. If you have service-related questions, please ask your administrator.