Guides and Tools

Ideas and options out there for a variety of needs, and information on how to use them.

Note: Answering the question of *Why* to use any of these will normally be outside the scope of the information. If you're here, you know what you're looking for and you're here to learn *How*.

- Communication
  - Matrix
- Money
  - Privacy Cards
- Alerts
  - ntfy
- Encryption
  - Protected Messages

Communication

Things you can use to communicate! There are so many options out there: we live in an age providing numerous methods of communication, each providing its own advantages and disadvantages.

Communication

Matrix

> Multi-platform messaging made easy, convenient, secure, and private.

The Matrix Protocol

Matrix is a messaging *protocol*. The term "Matrix" often refers to the method of communication or the app to be used, but it's actually about *how* the messages are managed and transmitted.

You can read more about it here: https://matrix.org/about/

How it Works

It's a lot like any instant messaging, chatting, or RCS (SMS). One simply types a message to an individual or group (also called a *room*) and sends it for all to see. It supports lots of functionality, like message threading, reactions (emoji responses to messages), and bots.

To get started, simply choose an available client (the app/tool you will use to log in and communicate) and create an account.

Don't fret too much about picking a client; they all do the same thing and have only niche differences important mostly to afficionatos.

> An example benefit is that you can log in from more than one device and keep all your conversations going, rather than having to always go back to the same tiny, pocket device to finger-type as fast as you can.

Easy Start: Element

Element is the easiest and most common client service to get started (in fact, "chat me on Element" is commonly used to mean talking via Matrix), having apps for numerous devices. However, you can *also* use it entirely in a web browser, so you don't even have to install anything!

1. Head to https://app.element.io/ and click **Create Account**.
2. Under "Host account on" will be listed *matrix.org* as the default option.
   - If you know another server you'd like to use, enter it here.
3. Pick a username and password, or sign in using one of the provided linking methods (Google, Facebook, Apple, GitHub, etc.).
4. Enter an email so you can recover your account if you need.
   - Some servers don't require an email.
5. Click Register, and you're in!

> Many servers are End-To-End-Encrypted (E2EE), meaning only you and the people with whom you are *intentionally* communicating will be able to read the messages or data you send. (Not even the owner of the server can see what you're sending!

Once you're in the Element (web) app, you'll be presented with a mostly blank screen. To start talking, you'll need the address of someone or some room to join. If you don't have one yet, try searching for public rooms, such as those listed on https://view.matrix.org/.

Talk to a Person

User contact addresses are formatted as `@user:server.tld`, so your friend Sam at www.popsicles.biz would be `@sam:popsicles.biz`. It should feel just like sending a text message, but with more features!

Send *Me* a Message!

You'll notice that the footer of every page on this Wiki contains a link to Message Me via Matrix using my handle `@starlord:starlord.zip`. Feel free to reach out!

Join a Room

Room addresses are formatted as `#room-name:server.tld`, so if your friend Sam had a room on the www.popsicles.biz server discussing flavors, it might be `#flavors:popsicles.biz`.

Matrix is a Polyglot!

Matrix is a *protocol*; it's about *transmitting* messages as data. As such, it's capable of talking to other messaging services! This is known as a "bridge." Users on apps like Signal, Telegram, Discord, etc. can all be "connected" to a Matrix room and chat with each other in the same space.

> Note: this takes some advanced tooling on the part of the server administrator. At time of writing, there are 26 bridges.

Matrix is Free!

There's no cost to any of this. You can download the apps for free, chat for free, message anyone for free, it's all free! If someone is trying to charge you, it's either for premium features you don't need or can get for free elsewhere, or it's a scam. Don't pull out your plastic digits!

The White Rabbit

It's so easy and it works so well! Dive in and enjoy a seamless, private, feature-rich chat experience.

Neo is waiting for you...

Further Reading

By the way, all of this information is provided by The Matrix Foundation in really easy-to-consume reading. I've just pared it down here.

Money

Handling the root of all evil...

Money

Privacy Cards

> Take control of your payments...

Privacy.com

Privacy.com is a service that allows you to link your bank account to digital debit cards you can generate to protect yourself from illicit use and maintain a measure of privacy and anonymity. All you do is generate a new card number (you get a certain amount per month depending on your plan, **and there *is* a free plan**) and use that as you would any other debit card you have.

> The cards are entirely digital, so you can't carry one with you into a store.

How does Privacy work?

I was gonna summarize, but their support article really puts it nicely:

> Privacy Virtual Cards can be used to make purchases in the same way as a physical card, but without the anxiety that comes with giving out your actual card's information knowing that it's only a matter of time until the next data breach.
>
> Every virtual card is connected to your bank account but comes with a unique, 16-digit card number, CVV, and expiration.
>
> Privacy Cards come with all kinds of additional protections to help shut down fraudulent transactions before they even happen:
>
> - Pause a virtual card between purchases to make sure fraudulent transactions can't sneak through.

> - Set a spending limit so you can control exactly how much and how frequently a virtual card can be used.
> - Close a card and rest easy knowing that even if a fraudster got your Privacy Virtual Card’s information, they couldn’t do anything with it.
> - All Privacy Cards lock to the first merchant they are used with to protect your card details from being improperly obtained.
> - Create one-time use cards that close after the first purchase is made, rendering them useless to hackers.
>
> Privacy connects to your bank and we directly debit your funding source for transactions as you make them.

Think of the uses!

Privacy.com can be helpful in so many ways:

Use multiple cards

You can have a separate card for each subscription, online store, etc., instead of putting the same bank debit card into everything. If your banking information changes, you only need to update the link to the funding source; all the cards on all your services can keep charging you.

Control what you're charged

Being able to set spend limits means you can protect yourself from a merchant over-charging you or adding hidden fees to a transaction. A great example of this is when your cable/internet provider decides to up-charge you one month. If you'd already set your auto-payments to a Privacy card, they'd only be able to charge the amount you'd set and you'd get a warning that they tried to do more.

Protect your buyer information

When entering a Privacy card in an online store, the name, address, and zip code don't matter; you can enter anything and it'll go through so long as the 16-digit number, expiration, and CVV are accurate. Don't want to give your name to a seller? You don't have to!

Stay safe from data breaches

Because Privacy cards lock into the first merchant who uses them, if a company holding your card info notifies you of a data breach and that someone else may possess your card info, you needn't worry: the new holder can't charge the card because they aren't identified as the original merchant.

And it's easy to spin up a new card and replace the old one. No calling the bank and waiting 10-14 days for your new card, and no updating that same card info everywhere you've saved it!

Pause cards

Don't want to make that auto-payment this month? Just pause the card! The card stays active and with the merchant, but they can't charge anything to it. Useful for when your payroll deposit is a few days behind and you don't want to overdraft.

Give out dead cards

Scenario: You sign up for a free-trial of a streaming service that's gonna charge you $24.99 at the end of the 2 weeks. You could try to remember to remove your card info or cancel your account before then, *or* you could give them a Privacy card set to $1 (or a card you paused immmediately after making it) and it won't matter if you forget because they won't be able to charge the card! If you decide to keep the subscription, just update the card to allow the upcoming charge to go through.

But wait, there's more!

Another special benefit that isn't immediately apparent: If you're on a paid plan, you get a certain percentage of cash back in the form of credit! This gets added to your Privacy account and is used on upcoming transactions before funds are actually debited from you.

> It's free and easy to get started at Privacy.com!

Alerts

Ways you can stay up to date with information!

Alerts

ntfy

> Notifications! Some people love 'em, some people hate 'em.

Get Notified!

With our phones playing such a huge role in how we administer our lives, the notifications we receive can sometimes be vital to staying up-to-date with our own needs (or, at least, the needs on our attention).

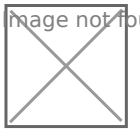
Enter **ntfy**, a service that allows you to send custom notifications, and listen to multiple channels where others might be updating information.

How it Works

All you have to do is either download the app and subscribe to a (new or existing) topic on a server or enter that topic's URL (which will just be `https://ntfy.sh/[topic]`) in a web browser.

> The default server is ntfy.sh, free and usable by anyone, but you can create your own or subscribe to someone else's!

The app listens to topics and uses your phone's standard notification service (the same one used for, for example, recieving a text message). The web URL requires **no** installation and just let's you listen to topics while you have the page open.



Example Android notification

What it Does

Every time a message is posted to the topic, anyone listening to that topic will get a message or notification (depending on how they're listening).

Notifications can be differentiated with emoji tags, contain pictures, be clickable (leading you to another link), and contain buttons that perform other actions.

They can also be scheduled to be delivered at a future date, and contain an Android broadcast to instruct other parts of your device to do something!

Oh the Possibilities

To get started, try it on your phone. There are so many uses! Here's just a few:

1. Send yourself an alert in an hour as a reminder to drink some water.
2. Set up hourly reminders to drink water throuhout the day.
3. Send a notification to a group of users that a new blog post has been created.
4. Update everyone on a project that the deadline has been moved up.
5. Use a sensor in your mailbox to trigger an alert that your mail has been delivered.
6. Teach your kids' phone to send an alert when their battery gets too low so you can see it and remind them to plug in their phone.
7. Publish a notification for certain emails (by forwarding them), like:
   - Bringing messages from an important sender to your attention faster.
   - Turning delivery notification emails into phone notifications.
8. Receive new meeting invite requests as a notification.
9. Subscribe to a support channel to get instant updates when a service goes down.
10. Create a panic button to instantly send a notification with your GPS coordinates to others listening on the same channel, letting them know you need help.

The list goes on and on...

Advanced Usage

You can use ntfy with `curl` and HTTP requests as well as correctly formatted URLs, meaning you can create lots of automation opportunities with things like `cron` jobs, IFTTT, n8n, Tasker, etc.

> I even saw an example of a smart toaster that was capable of making an API call when the toast popped up so the user could get alerted in the other room that the toast was ready.

> I saw another case where someone put RFID tags in the bridles of their horses and a reader outside the gate so they'd get notified of which horse had just escaped.

Encryption

Keep it secret, keep it safe.

--Gandalf

Protected Messages

Sometimes you want to transmit a message (text, a file, whatever) in such a way that only *you* and *the recipient* know what's in the message and can access its contents. Use cases may include:

- Sharing a password with someone.
- Sending a love letter you want to be private.
- Health care providers exchanging private documents (with each other or with patients).
- Contractors exchanging proprietary knowledge with their business partners.
- Telling someone the secret location of your buried treasure.
- etc.

The thing is, you don't always have a secure channel to transmit this information. So this guide is meant to give you some options.

What we're talking about is *Encryption*: obscuring digital information so that it can only be read in its true form once it is "decoded" by some method, like a password, key, etc.

Secure Options

So what are some options for sending a secured message? Let's look at a few useful tools...

Email: PGP

What is PGP Encryption?

> This section is still being written.

Private Links

There are some tools out there to let you deliver some text or a file attachment in the form of a simple URL you send to someone else.

PrivateBin

PrivateBin let's you enter any normal text, format it as plain, source code, or markdown, and generate it as a URL to send to anyone. You can set it to expire after a certain period (so it totally vanishes from history), select it to destroy itself after the first time it's read, and password protect it. You can also attach files and include the option to make an open (anonymous) discussion of the content. You can email the link from within the tool, or generate it as a QR code.

Scrt.Link

Scrt.Link is very similar; it lets you enter text or upload a file with a message, either of which can be password protected and then generated as a URL. It also offers a "Neogram" which is its version of a self-destructing link. While PrivateBin is entirely anonymous, you can opt for a free account with scrt.link to enable features like email or ntfy read receipts, larger content restrictions, a Slack app and browser integrations, and emoji links.

Send

Send is a simple tool to upload a file (or several) and generate a link for someone to download it later. You can set an expiration by time or number of downloads allowed, and set a password. It's simple and quick to use.

Encrypt Files with Hat.sh

Hat.sh is a nifty tool to encrypt any kind of file. Drag-and-drop, add a password or public key, and dowload the encrypted file (it'll have the same file name with `.enc` added to the extension). The best part is; this whole process happens entirely *in-browser*, meaning the file never leaves your device and goes to a server. Whoever you give the file to simply goes to the same site to decrypt it again, *also* entirely in-browser, and you're done!

Encrypt Content with PrivacyProtect.dev

PrivacyProtect.dev will let you enter a message **or** a file (not both) that is password protected and include a little password hint. Then it'll encrypt it for you and give you a `.html` file download. Send this to anyone, and when they open it up they'll see the hint, enter the password, and have the content! Once again, the data you're encrypting *never leaves your device*.

> What's great about this is that you can send it through any medium you like, you don't have to agree on a password before hand (or even have planned who the receiver will be), and, since it's stored as an `HTML` file, it can be read on *any* device, computer, phone, tablet, etc. Oh, and did I mention you can decrypt it entirely offline? No need for a connection!

On Passwords

Most of the options you'll find employ the use of a password that only you and your recipient know to protect the information. From a security standpoint, it is advised that you **exchange this password via a different channel than the one you are transmitting the message** or else **agree on a password beforehand another way**. This forces a potential leak to be in two places in order to break your system, which is much harder to do.

> **Good example:** You are working with a client's sensitive data and are about to send a confidential report via email. You encrypt the file with a password you agreed to over a private messaging service to avoid including the password along with the file in the same email.

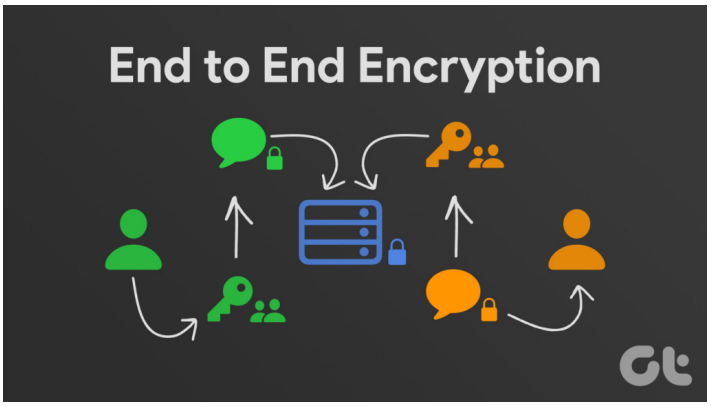
> **Bad example:** You SMS someone a link containing a protected document and then also text them the password to open it. Now anyone who gains access to the text messages (or even just looks over the recipient's shoulder) can *also* access that file.

Think of it this way: If you attached your address to your key ring and then somebody got a hold of your keys, it'd be a lot easier to return the keys to you, but it'd *also* be a lot easier to use them against you.

On Encryption

There are many different kinds of encryption, but for the sake of brevity I only want to point out E2EE, as it's used in most of the tools I recommend. E2EE, or End-to-End Encryption, means that something is encrypted from sender to receiver and at every step in between so that nobody but the sender and the receiver can decode it.

When you use email, text/SMS, or one of the tools I'm about to detail, the service provider handles the data you're transmitting. E2EE means that your message is encrypted *before* that provider gets it and isn't decrypted until *after* they've handed it off to the recipient.



> Think of it like sending a letter in the mail. If that letter gets intercepted at any point (or opened by the postal worker!), someone else gets to read it. However, if you wrote the letter in a language that only you and the recipient speak/read, then it's a lot safer!