# Biovibe Quick Guide to Secure Internet Sharing

William Lohaus
510-990-0440
lohaus@pm.me

## Overview

This document covers the basics of email, messaging (including conferencing), and file and data sharing; how to do them with maximum protection for you and your business. Individual sections provide background material on known threats and solutions.

## Email

Common email providers (google, yahoo, msn, etc.) are known to scan content and the network nodes that transmit email are known to be leaky; leaked content is sold to private firms which aggregate demographic data and mine that data for gems: content of particular worth and resale value. The best course is to get all company email on the same server and keep it there: it never leaves the server to be intercepted and is not scannable by common email providers (google, yahoo, msn, etc.). Two good options are: protonmail.com or your own private, hosted server. If you host your own, I recommend dreamhost, bluehost, or hostinger. I can set up email hosting for you for up to 20 people in 1 hour, or you can follow the hosting knowledge base directions and do it yourself easily.

## Messaging and conferencing

Messenger apps like Facebook Messenger, Whats App, Zoom, and Google Voice have the same issues as email: the providers scan content. Your content is not truly private. Other services like Slack are marginally more enterprise-grade but not encrypted, and leaks happen. Non-audited, non-open-source apps like Telegram are dubious: Their claims of security cannot be verified, and as they are for-profit enterprises, should not be trusted. At the extreme end of security you find Signal Messenger, an audited, open-source, totally encrypted app put out by a non-profit whose funding is usage independent. This is definitely a secure option. The problem

is, features that many businesses want are not available on Signal *deliberately* to make it more secure.

Many businesses want features like call recording, auto dictation and message search capability. These show up in services like Slack and in dedicated VOIP solutions like Dialpad (and countless others). The trade off for the features is security. Nearly all of these apps use artificial intelligence (AI) and there is no knowing where your data is going. Simple examples are Siri and Alexa, Apple's and Amazon's speech recognition software implementations. Both of them capture users' voices and study users' idiolect: one's unique way of talking. This information is sold to government contractors who monitor online speech, identify people by their speech patterns, whether the voice waves or the content, and enable surveillance of these people. You do not want your employees to be the people surveilled. You do not want to give away data about your employees' voices and ways of speaking. A compromise must be reached between security and features and you must reach that decision. I can help you model that decision, but cannot make it for you.

## File sharing and data sharing

Like email and messaging, the big players scan your files. Government agencies may casually request access without a warrant and the default response is full compliance: big tech companies give it to them without thinking. They get paid for doing it, and they do it freely. It is now a significant part of their business model. The current data architecture of big players is designed to give these agencies maximum access to your data. Starting in OS 10.8, Apple changed features specifically in that direction. Up to that point, Mac users could sync their computer and phone directly, using a cable. After that, the sync had to be done using Apple's iCloud service (or its predecessor, MobileMe). This meant that all your data, including addresses and call records, were now on Apple's servers. They did not have to be, but they were. The old system worked, but was too "surveillance opaque." The upgrade provided Apple with billions in potential annual revenue for data sharing with law enforcement.

What Apple did is now industry standard. All the big platforms do it. They bend over backwards to find ways to sell your data. For this reason, less known, higher security solutions are preferable. I recommend sync.com, proton drive, and nordlocker. All encrypt data in the cloud and in transit and are zero knowledge, meaning that the company cannot access your data (and thus cannot sell it). Each has advantages and disadvantages, that follow. Keep in mind that using end-to-end encrypted cloud drives is *much slower* than using Google Drive, Drop Box, or One Drive, because all the data has to be rearranged then sent.

Sync.com is cost effective and has software for older as well as newer machines and has team plans. Files are automatically synced between machines, operating like a WebDAV (web based Distributed Authoring and Versioning) system. Once the contents of your machines has been uploaded, the demands on your internet connection will be reasonable. Run it at night for a few weeks after the initial install, then it will work fine.

Proton Drive is from a leading global security and encryption company based in Switzerland. These people take security seriously. Downsides are that older operating systems are not supported and you must have newer machines to use the service. They are still developing desktop sync apps at this point.

Nordlocker is, in some ways, more secure than the other two because it encrypts data on your device and in transit and in the cloud. The downside is, if you lose your keys, or there is a glitch, the data is truly lost and no one can help you. With the others, the chance of technical support saving you is greater.

All of these three allow you to setup fully anonymous input/output work areas that can be used with clients. The clients do not have to do anything particular on their end. The out-of-the box solution is as secure as can be. Costs are modest for all of them. I do not review top-of-the-line Mossy Oak or iDrive because I am not familiar enough with them to do them justice. They may be fine for you, but I do not offer support.

## Conclusions

The internet is a predatory environment where governments and their contractors are the primary privacy concerns and big tech companies are the primary people selling your data. Hackers are usually only an issue in data breaches related to using free, insecure email, messaging, and cloud storage, or allowing online retailers to keep your credit card information on file. Hackers do ransom systems, but they tend to target large distributions (like those provided by Microsoft) because the payoff per programming effort is greatest. Go with smaller companies with good customer support for all software as a service (SAAS) and your chances of being attacked are minimal. Make sure any service has been around at least five years with a solid security track record. Startups and cheapest rates are red flags you should notice.

As a final note, certain password saving apps, like LASTPASS, are actually data gathering apps. Like Telegram, LASTPASS' claims of safety have never been audited and should be doubted. I highly recommend requiring your team to use either Proton Pass or Nord Pass, from one of the very respected providers already discussed. Stay safe and stay sane.