Secure Communications

A walk-through of safe(r) communications recommendations.

This guide will provide practical advice for multiple threat-levels.

Threat	Description
Level 1	Privacy for Family & Friends, Using Personal Devices
Level 2	Personal/Identity Concerns, ISP Logging, Basic Surveillance Evasion
Level 3	Law Enforcement, Journalists, Bloggers, Activists, Lawyers
Level 4	Whistle-Blowers, Intelligence Operators, State-Level Threats

Disclaimer:

- We are not lawyers, and this is not legal advice.
- Technology is constantly evolving, and this information could be outdated.
- Following this advice does not guarantee protection against every threat.
- You accept responsibility for your actions and the repercussions of following this advice.

We believe all individuals should have awareness in regards to their personal privacy, and communication security is extemely important. Even communication metadata can and will be used against you.

Level 1 - Basic Private Communication

Depending on your particular threat level, various issues need to be considered. If you're only needing privacy from family/friends standard information security protocols will be enough to protect you:

OpSec Basics:
ShadowLink Blog - Password Safety (http://shadowlinkit.com/passwords/)
ShadowLink Blog - Malware Basics (http://shadowlinkit.com/malware/)
NetP Wiki - Browsing - Level 1 (http://wiki.shadowlinkit.com/browsing/#level1)

Anytime security or privacy is needed you should create separate email/messenger accounts specifically for this purpose. If you use a cell phone, laptop or device that offers full disk encryption it should be used, especially with a strong passphrase. A weak or guessable passphrase is useless.

There are literally thousands of applications and email services for all platforms that offer encrypted/secure communication. Even Apple's default messaging app iMessage uses encryption. Using these services will encrypt your traffic and authenticate the remote connection. Some do this better than others. This will protect you from packet sniffing and ISP/network provider surveillance.

It should be noted that we may never know what companies have surveillance capabilities built in to their software. State level threats may also utilize zero-day exploits to decrypt captured communications or crack encrypted devices. There are also possibilities for threats to access a device while it is in use and capture keystrokes/screen-shots before anything is encrypted.

> The EFF does an amazing job comparing many 'secure' ways to communicate and created a handy chart:
> **Secure Messaging Scorecard (https://www.eff.org/secure-messaging-scorecard)**

Level 2 -Communication Via Proxy

Communication security in this guide is built on a foundation of browsing security. Think of security in relation to how a castle defense is setup. There are rings. Browsing safety is the outer ring.

Select threat level:
NetP Wiki - Browsing - Level 2 (http://wiki.shadowlinkit.com/browsing/#level2)
NetP Wiki - Browsing - Level 3 (http://wiki.shadowlinkit.com/browsing/#level3)
NetP Wiki - Browsing - Level 4 (http://wiki.shadowlinkit.com/browsing/#level4)

After implementing those protocols, use one the services stated above. If you want something more advanced that standard applications you should consider:

Advanced Chat Methods:
OTR(off-the-record) Messaging (https://en.wikipedia.org/wiki/Off-the-Record_Messaging)
TorChat (https://en.wikipedia.org/wiki/TorChat)

Never use a personal or known account. Only access those accounts after following the recommendations. If you have a high threat level it may be necessary to make an exhaustive checklist to attain safety. Even ONE mistake can be all it takes.

Level 3 - Utilizing Public Key Encryption

GPG or GnuPG (previously known to many as PGP), is a form of public key encryption used for encrypted communications and digitally signing messages to verify integrity.

For a basic introduction to public key encryption, see:
OpenSourceSec Blog - Cryptography Basics (http://shadowlinkit.com/cryptography/)

Special care should be taken when exchanging keys. This can be best done in person (or at a key party). You can also use a key server to retrieve keys.

GPG Resources:
The GNU Privacy Guard (https://www.gnupg.org/)
MANUAL - Using The GNU Privacy Guard (https://www.gnupg.org/documentation/manuals/gnupg/)
MIT PGP Public Key Server (https://pgp.mit.edu/)
Validating Other Keys On Your Public Keyring (https://www.gnupg.org/gph/en/manual/x334.html)

Level 4 - Advanced Communication

At this level, at a minimum, you should be:

Using a public Wi-Fi access point.

- Use a different AP each time.
- Recon for video surveillance before using.

Using a burner device.

Using **Tails (https://tails.boum.org/)** with a spoofed MAC.

Steganography

If the previous recommendations aren't enough there is a higher level of communications security that employs steganography. Steganography is the art of hiding your message within another file. There are various tools that can embed text in the metadata of image files, mp3 files, etc.

You can use GPG to encrypt a message, use a stego tool to inject it into an image file, then you send that file to the recipient who reverses the process.

High Speed Overkill Stego

In the days of the American Revolution, intelligence operators would communicate without ever meeting face to face or communicating directly. They used a form of steganography that uses cleverly written newspaper classified ads. Some researchers say this technique is still used.

Using a stego tool to embed a GPG encrypted message and posting it to a random image board from a clean access point is literally impossible to detect or prevent. There are 1000's of image boards with billions of images being posted constantly.