Safe Communication

To finish out section 3, we're going to talk about one of the most important ways we use the internet: *To communicate! You would think the private communications between you, family, friends, and coworkers would be secure and private.* Well, no. Unfortunately, we communicate on an internet where our messages are inherently insecure with the illusion that what's being shared is kept private. Let's dive deeper into the topic...

Promotional Spot

By default, it is extremely difficult to communicate privately and securely digitally. It's a weird thing to think about. In our society, we respect people's personal space because we want them to respect ours. *If you want a conversation to be kept secret between you and another person, you simply talk in a room where no one else is listening.* So how do you communicate safely over the internet? Glad you asked...

A disclaimer in advance...most of the methods covered in this lesson rely on *not only you to use a specific service, but the person you're talking to as well.* Another disclaimer is you're most likely not going to be able to switch all of your contacts to a service, but the more you can switch the better.

One of the most prevalent and standardized forms of communication is the text message, **** hold two phones up **** sent between two phone numbers. The technology that powers these messages is called *SMS, or short message service,* and this is all handled by your cellular provider, like *Verizon, AT&T, or Sprint.* Unfortunately, these texts are generally not encrypted, and cellular companies collect all of our conversations; *they're known to hand it over to intelligence agencies. As a matter of fact, beginning in 2002, the NSA asked AT&T to build secret rooms in their facilities:* One in *Bridgeton, Missouri, and another on Folsom Street in San Francisco. More were eventually added in Seattle, San Jose, LA, and San Diego,* and these rooms were used to channel all internet, email, and phone traffic through a filter that would look for keywords. *It was recently discovered this practice continues today.* Outside of government surveillance, are there security issues with SMS messages? Absolutely! *There are commercially available eavesdropping devices that steal SMS messages* Because of these issues, I would recommend you avoid SMS if your goal is privacy and security, especially when it involves sensitive data. So what do we use?

The first alternative is what many of your devices come with by default, things like *iMessage, Facebook Messenger, Google Hangouts, one of Google's countless other messengers, Blackberry Messenger, Skype, and so on.* I like to classify these as *'Triple C', or common commercial communication* methods which will typically, (not always) offer decent security, with lackluster privacy. Many of these implement some form of encryption, although it is (for the most part proprietary), and some don't use end-to-end encryption like Hangouts. Proprietary encryption is typically a big no as the company holds a large amount of power that could eventually lead to unauthorized access to your data. Of all the Triple C services out there, I would argue iMessage is one of the better ones, *but you're really just picking between the worst fruit from the tree. Here's a nice website that compares the main messengers for you.*

So what are the good options? Well looking at that chart: *Signal, Threema, Wire, Telegram, and Wickr* seem decent. Each has its pros and cons, so I'd recommend sorting through this yourself. *Be wary of services like Whatsapp whocollect metadata, a problem we discussed in section 1. Telegram is popular as well, although often debated in the security realm. They suffered a hack in 2016 that exposed 15 million phone numbers,* and they use proprietary software on the backend so we can't verify that. On the upside, *Telegram has been banned in many countries, which is interpreted as good news since it means countries are struggling to access data in an unauthorized manner. Just like MF DOOM says "Can't understand it, ban it."*

No matter what service you end up going with, here are some things to research when selecting a messenger: *Try to choose something with off-the-record messaging, or OTR--it's a higher standard of encryption for messages. Also look for 'Perfect Forward Secrecy" or PFS, so if one encryption key is compromised, the others will be safe. Lastly, don't forget what information is required to open an account. Signal requires a phone number; you can fake this easily, but this still concerns people.*

I've already mentioned some services that hit some, or all of these requirements, but there are more options. *Chatsecure utilizes XMPP, more on that soon. Crytocat is okay if you're alright with not having mobile clients.*

I mentioned XMPP. XMPP is a protocol used for sending messages with decentralization, open standards, and security as the main benefits, although keep in mind by default there is no end-to-end encryption, you must configure it. You can use Jabber to set it up, Kontalk, or any other XMPP client. There's also the Matrix protocol, which attempts to improve on XMPP and is used in services like Riot.im.

To summarize, at the end of the day, the messenger you pick is your call, each has pros and cons, and it ultimately comes down to what you trust the most, in combination with where your priorities lie, and what services you can realistically get your friends and family to use.

Outside direct messages, what about phone and video calls? For entry level stuff, *Whatsapp offers both of these, and it'll do an okay job, but remember that metadata is a huge problem. Signal is better, and offers both phone and video calls. Wire is also decent.* For a more advanced phone threat model, consider using prepaid or burner phones for sensitive conversations. If you want a more permanent secondary number: *iNumbr, Burner, and Shuffle are all great services to go check out.*

Moving on to email! This seems to be pretty good, right? Well, depending on your client, email can identify you by the IP address you use to send the message. Proxies do the trick well here, since the encryption is likely being handled by your email provider, and all we need is a tool to hide our IP address. To make email even more private, use something called an *anonymous remailer, which changes the email address of the sender before sending the message, and the recipient responds to the remailer. This essentially works as a proxy for your email address. There are 3 types of remailers: type 1 and 2 don't allow you to respond to emails, it's one way only. Type 3 allows responding, forwarding, and encryption.*

When it comes to email encryption, try to not let a company like Google handle the encryption. Not only do they hold the keys, but services like Google *scan all of your emails and use it to build a profile on you.* You have a lot of options for encryption...there's Pretty Good Privacy, or PGP, there's GPG, or openPGP. They are typically tricky to setup, but there are services like *Mailvelope that simplify things a lot. ProtonMail, disroot.org Tutanota, and CounterMail also seems good. These are just random recommendation to look into.* Lastly don't forget about self-hosting your own email if you can go that route.

Remember though, just because the email is encrypted, *doesn't mean there's no metadata stored within the message.* Make sure to watch the metadata lesson from the first section of the course.

If you need temporary disposable email addresses to use online, *Tempmail is a great site as well as Guerrilla mail; keep in mind neither are inherently anonymous, there are other temporary email alternatives as well.*

As for alternative email solutions, *I2P-Bote is a fully decentralized email system. It supports different identities and minimizes metadata exposure, making it a cool project.*

One final overlooked form of communication *is file sharing. You can use email, but you'll be limited on size and number of files.* No matter how you share the file, make sure you encrypt it before uploading it to the internet, we already covered how to do this in section 3. As for how to share it, if it's encrypted it's not a huge deal to upload on a service like Dropbox, but I'm still not going to recommend it. You can use something like *Nextcloud. There's also Firefox Send, which will encrypt and store a file.. The last service is OnionShare, an open source project on Tor, which lets you securely and anonymously share a file of any size. This is very promising.* No matter what service you choose, encrypt the file before uploading it, and give the password to your recipient using another communication method.

Queue Outro Promos

So that's going to cover the different main forms of communication on the internet. Section 3 has been a ton of fun, time-consuming, but fun. We're halfway done with the entire course! I'll be doing a final little wrap up in the next lesson, so I'll see you there, and thank you for watching!