# Regular phone calls

When you make a call from a landline or a mobile phone, your call is not end-to-end encrypted. If you're using a mobile phone, your call may be weakly encrypted between your handset and the cell phone towers. However as your conversation travels through the phone network, it's vulnerable to interception by your phone company and, by extension, any governments or organizations that have power over your phone company. There are also inexpensive techniques which other people can use to listen to your calls if they are close to your phone.

*Regular phone calls to or from your mobile phone are not secure.*

# VoIP Calls

The easiest way to ensure you have good encryption on voice conversations is to use VoIP instead of regular calls. VoIP (Voice over Internet Protocol) refers to calls made using the internet. Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. Good call encryption software is currently only supported on a few models of smart phones.

In order to have end-to-end encrypted VoIP conversations, both parties must be using the same (or compatible) software. Conversations between providers such as Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place.

# Making secure calls on your phone

## Signal

Signal is a free, simple open-source tool for having end-to-end encrypted phone calls and also for sending secure messages. It works for both Androids and iPhones and replaces the previous android app called Redphone. (Users with RedPhone installed will be prompted to install Signal instead. If you already have Signal installed, you can just uninstall RedPhone. It will no longer be maintained as an independent app.)

Signal now also incorporates secure messaging app, Textsecure ? meaning there is one simple app you can use for both secure calling and messaging, whether on Android or iPhone, as long as the person you are communicating with has Signal too.

Signal uses your existing phone number and address book. There are no separate logins, usernames, passwords, or PINs to manage or lose. It uses your mobile number as your identificator (like a user name) ? this makes it easier for the user, though it also makes it easier to analyze the traffic it produces and trace it back to you. Signal uses a central server, which is a point of centralization and thus puts it in the powerful position of having control over some of this data. However they cannot hear your conversations or see your messages, so no one else can either.

## Ostel

Another notable tool for having end-to-end encrypted phone calls is OStel. It works on every smartphone (Blackberry, iPhone, Nokia, Android) and every desktop (Mac, PC, Linux, etc). It is one of the most secure means to communicate via voice and comes with many easy set-up wizards for different VoIP services, available [here](https://ostel.co/). (The accompanying app for Android phones is CSipSimple.) Both you and the person you want to talk to will need an ostel account. It securely encrypts all your speech and makes it very difficult to trace your data and find out who you are talking to. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use.

## Redphone

[RedPhone](https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone) is a free and open-source tool for having end-to-end encrypted phone calls that works only on Android phones. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contacts system. People you want to talk to also need to install and use RedPhone (or, if they have iPhones, Signal, as noted below). For ease of use RedPhone uses your mobile number as your identificator (like a user name on other VoIP services). However it also becomes easier to analyze the traffic it produces and trace it back to you, through your mobile number. RedPhone uses a central server, which is a point of centralization and this puts RedPhone in a powerful position (of having control over some of this data).  
You can learn how to set it up simply in the RedPhone tool guide.

Signal is the version of RedPhone that works on iPhones. The two systems are fully compatible and can be used to communicate securely with one another. Learn how to set it up in the Signal tool guide.

# Making secure calls on your computer

## JitsiMeet

When using voice communication to exchange sensitive information it is important to choose a tool that encrypts the call all the way from your computer to the recipient's computer. We would recommend that you use the free and open-source tool, JitsiMeet as your choice for VoIP. It provides a free, easy to use, open source, more secure alternative to Skype and can be used for video and voice and for group video chat. There is no requirement for you or the person you?re communicating with to sign-up. You just visit <https://meet.jit.si> enter a meeting name, (make sure it has no spaces and is difficult to guess), and share the link with whoever you want to speak with. Simple as that.

## Skype

Beware! Most popular VoIP providers, such as Skype and Google Hangouts, offer transport encryption so that eavesdroppers cannot listen in, but the providers themselves are still potentially able to listen in. Depending on your threat model, this may or may not be a problem, but we would recommend that you avoid Skype if you discuss sensitive information. It is important to keep in mind that Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies access to all your communications history.

While we can't recommend Skype as a secure communication tool, it is very important to take some precautions if you still decide to use Skype as a tool for sensitive communication:

* Download and install Skype only from its official website [www.skype.com](http://skype.com/) to avoid a Skype program infected with spyware.
* Change your Skype password regularly.
* Set the privacy settings on Skype so that it does not keep a history of chats.
* Disable the Skype setting which automatically accepts incoming files, as this has occasionally been used to introduce malware/spyware onto computers.
* Always independently verify the identity of the person with whom you are communicating. It is easier to do this when voice chatting, especially if you know the person you want to talk to.
* Decide if your Skype username should identify your or have any relationship to your real name, or the name of you organisation.  
  ? Be careful of what you say - develop a code system to discuss sensitive topics without using specific terminology.

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Mobile Phones Lesson](umbrella://lesson/mobile-phones)
* [Redphone Tools guide](umbrella://lesson/redphone)
* [Signal Tool Guide](umbrella://lesson/signal)
* [Jitsi Tool Guide](umbrella://lesson/jitsi)

### FURTHER READING

* [EFF - Communicating with others](https://ssd.eff.org/en/module/communicating-others)
* [Security in a Box - Secure communication guide](https://securityinabox.org/en/guide/secure-communication)