# Regular SMS Text messages

SMS messages are not well encrypted so you should not rely on them to transmit sensitive information securely. Sent SMS messages can be intercepted and kept by your service operator or by third parties with inexpensive equipment. Those messages will carry the phone numbers of the sender and recipient as well as the content of the message. What's more, SMS messages can easily be altered or forged by third parties.

If you do need to use SMS for something, consider establishing a code system between you and your recipients. Codes may make your communication more secure and may provide an additional way of confirming the identity of the person you're communicating with. Code systems need to be secure and change frequently.

Saved messages on your phone can easily be accessed by anybody who gets hold of your phone so consider deleting all received and sent messages straightaway.

*Regular SMS text messages to or from your mobile phone are not secure.*

# Sending secure SMS on your phone

## SMSSecure

SMSSecure is a free, open-source tool for sending and receiving secure SMS text messages on Android phones. It works both for encrypted and non-encrypted SMS, so you can use it as your default SMS application. It automatically imports all your contacts and existing SMS, so only takes a few seconds to set up. No internet connection is required to send or receive SMS. To exchange encrypted SMS this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. SMSSecure also encrypts all SMS locally, so if your phone is lost or stolen, your messages are protected.

Many people who previously used TextSecure for secure SMS now use SMSSecure.

You can find SMSSecure on google play and installation takes only a few clicks.

# Sending secure online messages on your phone

## Signal

[Signal](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) is a free, simple open-source tool for sending end-to-end encrypted messages and also for having secure calls. It works for both Androids and iPhones and replaces the previous android app called TextSecure. (Users with TextSecure or the old Signal will have already received the update, or can do it manually be visiting the Playstore/Appstore and pressing Update)

Signal now also incorporates secure voice calling app, Redphone ? 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.

## Telegram

A note on Telegram: While Telegram does use end-to-end encryption in some modes, there have been serious concerns with the quality of their encryption and the amount of information it gathers on users, including their full contact lists. Users must also remember to start a new ?Secret Chat?, before encryption is activated. Given these concerns we cannot recommend Telegram as a secure method of communicating.

## ChatSecure

[ChatSecure](https://chatsecure.org/) as a secure text chat application that works for both iPhones and Androids and across a number of platforms. Not only does ChatSecure encrypt your phone to phone messages, it can also operate across a number of platforms, and offers more functions than Signal. ChatSecure offers easy and strong encryption for your chats that provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

See how to set it up in the [ChatSecure tool guide](umbrella://lesson/chatsecure).

# WhatsApp

WhatsApp is the most popular mobile communication tool in the world, offering free messaging to individuals and groups and operating on all phone types. Until November 2014, using WhatsApp was considered highly insecure and was not recommend for anyone who required any level of security in their communications. It now offers strong encryption for some messages on some phones.

Since November 2014, WhatsApp has integrated the secure code of a well-respected privacy and technology company (Open Whisper Systems) into its product. This means that its messages now have a very strong level of verifiable security, and WhatsApp can no longer easily view or be forced to handover messages to authorities.

However it is very important to note:

* This only currently applies to users using WhatsApp on Android phones (users on Apple iOS, Windows Phone, Blackberry and Nokia will be only get the same protection at some point in the future.)
* Only for messages from one individual to another individual (ie: not for group chats)
* Does not encrypt any pictures sent once they arrive on the phone
* While WhatsApp or others cannot view the content of your messages, they can still know that you are communication with someone (e.g metadata). In some cases, this may still have negative security consequences.

For these reasons we still recommend that you use [Signal](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) for secure messaging and calls.

# Secure messaging on your computer

## Pidgin

Instead of using Skype, Google Talk or MSN Messenger to send messages on your computer we recommend you use the secure, free, open-source tool, Pidgin, instead.

Pidgin is a chat program which lets you log in to accounts on multiple chat networks simultaneously. This means that you can be chatting with friends on MSN, talking to a friend on Google Talk, and sitting in a Yahoo chat room all at the same time. Pidgin runs on Windows, Linux, and other UNIX operating systems.

Pidgin supports many features of these chat networks, such as file transfers, away messages, emoticons, and typing notifications.

## Adium

A good alternative to Pidgin that works with OS X on Macs is [Adium](http://adium.im/).

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [TextSecure tool guide](umbrella://lesson/textsecure)
* [ChatSecure tool guide](umbrella://lesson/chatsecure)
* [Pidgin tool guide](umbrella://lesson/pidgin)
* [Adium tool guide](umbrella://lesson/adium)

### 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)