**Защищенные мессенджеры для секретной переписки**

Мессенджеры на смартфонах так быстро вошли в нашу жизнь, что мы даже не заметили то, как практически перестали пользоваться обычной мобильной связью и общаться при помощи смс сообщений. Ежедневно по всему миру люди обмениваются различной информацией, включая в себя текстовые, фото и видео послания, и неустанно продолжают спорить о том, какой же мессенджер самый безопасный. В данной статье мы рассмотрим подборку самых защищенных из них.

**Signal**

Signal Protocol – программное обеспечение разработанное специально для данного мессенджера, позволяет надежно шифровать передаваемую между пользователями информацию, такую как – текстовые и голосовые сообщения, а также видео звонки. Его исходный код хранится в открытом доступе, что позволяет специалистам находить различные уязвимости и сообщать о них производителю.

К его основным преимуществам можно отнести возможность скрыть от своего собеседника Ваш IP адрес и установить таймер для удаления отправленных сообщений. Минусом же является то, что авторизация в нем происходит по номеру телефона, а вся передаваемая информация хранится на серверах компании.

**Wire**

Создателями данного приложения являются бывшие разработчики Skype и по их заверению, новый созданный ими мессенджер является одним из самых защищенных, и в своей работе использует протокол шифрования по принципу Signal - end-to-end, что позволяет его клиентам безопасно обмениваться сообщениями и видео.

Для создания аккаунта можно использовать не только номер телефона, но и адрес электронной почты, что, безусловно, увеличивает шансы пользователей на анонимность. Также к плюсам можно отнести тот факт, что у данного мессенджера также открыт его исходный код, регулярно проходящий проверку независимыми экспертами.

**Threema**

Первое, чем данный продукт отличается от других – за его использование придется заплатить деньги. Второе – при регистрации у Вас нет необходимости указывать номер телефона или адрес электронной почты. При первом использовании приложения каждому пользователю присваивается уникальный идентификатор, по которому его смогут найти другие пользователи чтобы начать с ним общение.

Все передаваемые данные между участниками шифруются по технологии end-to-end на используемых ими устройствах и не хранятся на серверах компании после доставки. Минусом данного сервиса является то, что его исходный код недоступен для всех желающих, поэтому не имеется возможности его проанализировать на заявленную авторами безопасность.

**Keybase**

Это некая многофункциональная платформа, которая помимо общения участников внутри нее при помощи секретного чата, позволяет отправлять зашифрованные сообщения на другие популярные сервисы, такие как twitter и facebook. Кроме того данный ресурс позволяет хранить Ваши файлы в зашифрованном виде на собственных облачных хранилищах, а также имеет собственный криптовалютный кошелек.

Плюсом данного сервиса является анонимная регистрация и возможность обмениваться зашифрованными сообщениями с пользователями по всему миру, не зная их номера телефона и email. К минусам можно отнести сложность в освоении программы и отсутствие перевода на русский язык.

**Silence**

Программа Silence изначально создавалась как дополнение к приложению Signal, но вскоре начала развиваться отдельно от него. На данный момент работает лишь на операционной системе Android и больше напоминает обычное приложение для обмена смс. Не требует предварительной регистрации и доступа к интернету. Для полноценной работы ресурса достаточно доступа к мобильной сети.

Шифрование передаваемых сообщений происходит по методу Signal и позволяет передавать их даже на те устройства, на которых не установлено данное приложение, преобразуя текст в обычные смс. Существенным недостатком Silence является отсутствие голосовой и видеосвязи.

**Confide**

Если Вы искали безопасный мессенджер не похожий ни на один другой, то Confide именно то, что Вам нужно. При создании профиля не обязательно указывать номер своего телефона, достаточно будет адреса электронной почты и имени пользователя.

Все приходящие текстовые послания скрыты за прямоугольниками и для того, чтобы иметь возможность их прочитать необходимо провести по ним пальцем. После прочтения информация хранится на устройстве непродолжительное время и затем полностью удаляется с него. Тоже самое происходит и с полученными изображениями.

Как мы видим в погоне за званием самого безопасного мессенджера, производители придумывают все новые и новые способы шифрования информации, но, однако, ни один из них не может дать стопроцентной защиты Вашей переписки. Необходимо понимать, что злоумышленники тоже не дремлют и работают над способами обхода защиты любой сложности.

