Автор: Алина Саратова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 8389 18.05.2016, 13:35
14

Как защитить телефон от прослушки

13 мая депутаты Госдумы одобрили поправку, которая обязывает операторов сотовой связи в течение трех лет хранить информацию об абонентах, их звонках, переданных сообщениях и изображениях.

Учитывая недавний скандал со взломом аккаунтов Telegram у нескольких активистов, все более актуальным становится вопрос о том, как можно сохранить конфиденциальность своего общения. О прослушке мобильных телефонов в последние дни не говорит только ленивый. Мы уже упомянули о новинке, которая позволит работодателям перехватывать мобильные разговоры сотрудников в офисе.

Сегодня предлагаем поговорить о том, как распознать, что ваш телефон кем-то слушается и пеленгуется, и как от этой прослушки избавиться.

> За аксиому возьмем два факта. Первый: вы – честный и законопослушный человек. И второй: без вашего согласия прослушивать вас не имеют права.

Как избежать слежки?

Обладателям смартфонов приходится защищать сразу несколько аспектов своей конфиденциальности: через телефон можно следить за перемещениями, прослушивать разговоры, читать переписку и получать данные, хранящиеся на данном устройстве.

Самому оператору не так интересно следить за вами. Его данными легально могут пользоваться спецслужбы - через систему СОРМ-2 они имеют прямой доступ к данным, получаемым от оператора. При слежке за одним человеком в поле зрения попадает не только его аппарат, но и телефоны, часто находящиеся рядом с ним. Соответственно, непригодной является схема, при которой две трубки – «публичная» и «секретная» – включены одновременно. Желающие ходить с двумя телефонами должны аккуратно комбинировать режимы их поочередного включения, дабы не быть раскрытыми.

Слежка за вашим мобильником означает, что, например, если вы пришли на встречу, следящим тут же будет известны все мобильные аппараты, лежащие в карманах у ваших собеседников. Популярные приложения, позволяющие искажать местоположение, для конспирации бесполезны: они обманывают конкретно ваш смартфон, но не сотового оператора.

Кстати, снять аккумулятор с трубки – это проверенный и действенный способ избежать отслеживания перемещений. А вот чехлы для мобильных и одежду с карманами, блокирующими сотовый сигнал без снятия батареи, нужно проверять в каждом случае перед покупкой.

Как выявить прослушку и сохранить тайну разговора?

Существует оборудование для дистанционного подслушивания разговоров (помимо спецслужб, такого плана техника вполне может быть и в частных руках). В принципе, смартфон можно использовать как скрытый и управляемый на расстоянии диктофон, и, чтобы услышать разговор, не обязательно слушать в режиме реального времени, достаточно просто записывать все разговоры.

И уж тем более любой разговор может быть записан, когда вы сами звоните по телефону. Вопреки расхожему мнению, щелчки или эхо в трубке вряд ли означают прослушку – это могут быть всего лишь проблемы со связью. Сильный нагрев телефона и быстрая разрядка батареи могут указывать на наличие в телефоне программ-шпионов, но это тоже неоднозначный признак. Другие признаки прослушки или наличия шпионящих программ – слишком долгое выключение, самостоятельная активность телефона, помехи на телевизоре или компьютере при неиспользуемом в настоящий момент мобильнике.

Чтобы сохранить конфиденциальность телефонного разговора, любые чувствительные звонки нужно делать не напрямую через оператора, а через приложения, поддерживающие шифрование. Например, Signal, Skype, WhatsApp, Viber или звонки в Facebook будут более надежным способом сохранить анонимность звонка, чем обычный телефонный звонок. Кстати, аппараты, поддерживающие стандарт связи ***GSM легко поддаются прослушиванию и «забрасыванию» шпионских программ, в отличие от мобильников, поддерживающих стандарт CDMA…***

Как защитить передачу "СМС"?

СМС – самая небезопасная из всех форм общения. Приложения-мессенджеры сейчас по умолчанию шифруют сообщения – если раньше этим славился Telegram, то с апреля сообщения также шифруют WhatsApp и Viber.

Самый защищенный мессенджер - Jabber с шифрованием off-the-record messaging. Далее идет Signal, за ним – Telegram и WhatsApp. В Telegram действуют безопасные «секретные чаты» – для того чтобы прочесть переписку, человеку придется завладеть телефоном, с которого она велась. Для пущей безопасности лучше настроить автоматическое удаление сообщений.

Не так давно в сети появилась информация о взломе Telegram. Его можно было бы избежать при условии двухфакторной авторизации. Но не по смс, а с помощью токена (компактного устройства, своего рода ключа).

Как защитить данные на карте памяти от кражи?

Получить доступ к смартфону можно, заразив его вирусом, но это очень сложно, если есть антивирусы. Так что хранящуюся в мобильнике информацию проще всего получить, физически завладев самим телефоном. Если сохранение конфиденциальности информации на смартфоне для вас очень важно, купите аппарат и программное обеспечение, обеспечивающее блокировку/уничтожение информации в случае нескольких неправильных вводов пароля.

Смартфон должен иметь последнюю версию операционной системы и установленных приложений, все приложения должны быть установлены исключительно из доверенных источников. Мессенджеры с открытым исходным кодом, использующие end-to-end шифрование и, по возможности, двухфакторную аутентификацию, достаточно безопасны при правильном использовании.

Помните, что установить программу-шпиона на чужой телефон не составит большого труда. Интернет буквально кишит предложениями купить то или иное приложение для прослушивания и слежки за мобильным аппаратом. Они способны тайно работать на телефоне жертвы и передавать информацию разнообразными способами: отправлять сообщения СМС с вашими координатами, делать скрытую аудио- и видеозапись, отправлять данные на электронную почту и даже делать снимки стандартной камерой телефона. Поэтому следите за своим мобильником – если не хотите, чтобы мобильник следил за вами.

Автор: Алина Саратова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 8389 18.05.2016, 13:35
14
URL: https://babr24.com/?ADE=270609 Bytes: 6171 / 5894 Версия для печати Скачать PDF

- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

Автор текста: **Алина Саратова**.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта
Архив
Календарь
Зеркала сайта