



Вся моя деловая переписка — в мессенджерах. Как ее защитить?

9 карточек · 06:32, 23 февраля 2018

[Ссылка на материал](#)

Это PDF-версия материала, опубликованного на «Медузе». Вы можете отправить этот файл в любом мессенджере или по электронной почте вашим близким в России, особенно тем, кто не умеет обходить блокировки. Вы можете также распечатать этот текст и показать его тем, кто не пользуется интернетом.

«Медуза» признана «нежелательной» организацией на территории РФ, поэтому, пожалуйста, будьте осторожны и делитесь нашими материалами только с теми, кому доверяете.

Подробнее о «нежелательном» статусе.

Самый удобный способ читать «Медузу» без VPN — это скачать наше приложение. Оно работает в России, несмотря на блокировку, и это абсолютно безопасно. Версия для iOS и для Android.

Приложение на Android также можно скачать по прямой ссылке. Устанавливайте приложение не только себе, но и близким!

- 1. Что случилось?**
- 2. Постойте, но зачем кому-то вообще нужна моя рабочая переписка?**
- 3. Если я не топ-менеджер, мне стоит опасаться взлома?**
- 4. Обычные бесплатные мессенджеры отличаются друг от друга в плане безопасности?**
- 5. Если я использую секретный чат, все будет в порядке?**
- 6. Для деловой переписки существуют специальные корпоративные мессенджеры, за многие из них приходится платить. Они надежные?**
- 7. Есть ли какой-то один, самый безопасный мессенджер?**
- 8. Как защитить от взлома собственный телефон?**
- 9. Что делать, если я параноик?**

Что случилось?

Вы — один из тех двух миллиардов человек на Земле, кто переписывается в мессенджерах. В том числе с коллегами, партнерами, контрагентами. Вероятно, вы даже знаете, что такой способ связи не очень безопасен, но поскольку пока ничего страшного не произошло, вы не начали в этом разбираться. Вместе с экспертами в области цифровой безопасности из компании «Электронное облако» мы подготовили карточки о том, насколько безопасна ваша переписка и можно ли ее защитить.

Постойте, но зачем кому-то вообще нужна моя рабочая переписка?

Вариантов может быть несколько. Например, конкуренты хотят получить доступ к клиентской базе или к документам, которые содержат коммерческую тайну, чтобы использовать их для дискредитации вашей компании. Хакеры — чтобы вас шантажировать тем, что конфиденциальные документы станут общедоступными. Наконец, не стоит забывать и про государственные

службы (как внутренние, так и зарубежные), которые тоже могут заинтересоваться вашей перепиской.

3

Если я не топ-менеджер, мне стоит опасаться взлома?

Да, хотя и меньше, чем топ-менеджеру или сотруднику бухгалтерии. Много зависит от рода деятельности вашей компании. Например, если в банках с корпоративной перепиской должны быть аккуратны все сотрудники без исключения, то фирме по доставке цветов необходимо в первую очередь беречь счета и клиентскую базу.

4

Обычные бесплатные мессенджеры отличаются друг от друга в плане безопасности?

Да. Прежде всего нужно обратить внимание на наличие сквозного шифрования, с помощью которого все сообщения зашифровываются и расшифровываются

непосредственно на вашем телефоне и не хранятся на серверах самого приложения.

Есть и дополнительные функции безопасности. Например, приложение Confide открывает сообщение только после проведения пальцем по строке, а после прочтения безвозвратно его удаляет. То же самое произойдет, если пользователь попытается сделать скриншот.

Среди самых популярных мессенджеров — например, Facebook Messenger и Viber — ни один не открывает своих алгоритмов, что не дает возможностей для независимого анализа мессенджеров. Сообщения об их небезопасности появляются регулярно. В WhatsApp в некоторых случаях (например, когда владелец теряет телефон, меняет номер или надолго уходит в офлайн) приложение без ведома пользователя меняет ключ шифрования. Из-за этого посторонние могут получить доступ к сообщениям, отправленным после успешной атаки.

Эта карточка была исправлена. В предыдущей версии на основе рейтинга Фонда электронных рубежей говорилось, что WhatsApp может считаться одним из самых безопасных мессенджеров из числа популярных. Эта версия рейтинга ФЭР устарела, сейчас разрабатывается новая. «Медуза» приносит извинения читателям.

Если я использую секретный чат, все будет в порядке?

Действительно, в некоторых мессенджерах, например в Telegram, есть функция секретного чата. Это значит, что сообщения в незашифрованном виде гарантированно не будут храниться на сервере компании, а только на устройстве, с которого вы пишете. Даже если к аккаунту привязано несколько устройств, то на другом сообщение посмотреть будет нельзя (за исключением мессенджера Signal, о котором мы скажем отдельно). Часто можно выставить таймер — и по истечении необходимого вам срока сообщения безвозвратно удалятся.

Для деловой переписки существуют специальные корпоративные мессенджеры, за многие из них приходится платить. Они надежные?

На рынке довольно много корпоративных мессенджеров, например Slack, FlowDock, HipChat. Они более удобны

для решения собственно деловых задач, позволяют работать в группах и так далее. Не секрет, например, что «Медуза» использует для каждодневного общения именно Slack.

Как и в обычных мессенджерах, в них бывают уязвимости. Например, в сентябре 2017 года обнаружилась «дырка» при рассылке обновлений Slack, которая позволяла отправлять пользователям скомпрометированное приложение. Позднее выяснилась еще одна особенность деловых мессенджеров: оказалось, что злоумышленник может зарегистрироваться в рабочей группе условной компании NN, если использует в адресе электронной почты доменное имя этой компании (скажем, @nn.com), а служба поддержки при этом не проверит адрес вручную.

7

Есть ли какой-то один, самый безопасный мессенджер?

Одним из самых безопасных среди популярных мессенджеров считается Signal (его, например, рекомендовано использовать американским сенаторам). Через него советовал общаться, например, Эдвард Сноуден. Signal создан на основе открытого исходного кода. Это значит, что любой может посмотреть код

мессенджера и убедиться, что он не отправляет информацию третьим лицам. В случае с Signal независимые аудиторы многократно проверяли исходный код — и не нашли в нем серьезных уязвимостей.

Однако у Signal есть несколько минусов, среди которых не очень удобный интерфейс и большое количество технических ошибок при работе на платформе Android. Кроме того, при переходе на другое устройство пользователь теряет историю переписки.

Эта карточка была исправлена. В предыдущей версии говорилось, что Signal получил наивысшую оценку рейтинга Фонда электронных рубежей, однако эта версия рейтинга ФЭР устарела, сейчас разрабатывается новая. «Медуза» приносит извинения читателям.

8

Как защитить от взлома собственный телефон?

Нужно придерживаться двух базовых правил. Во-первых, у вас всегда должен быть сложный пароль (о том, как подобрать и не забыть такой, мы рассказывали

в карточках). Во-вторых, следует быть в меру подозрительным, чтобы не стать жертвой манипуляций или того, что специалисты называют социальной инженерией. Если в вашей компании работает хотя бы сотня человек, вы уже не можете быть на сто процентов уверены, что ваш собеседник — именно тот, кем представился. Предположим, что вам пишет некто, называющий себя помощником системного администратора. Он говорит, что ему дали задание проверить ваш корпоративный компьютер или смартфон на вирусы, и спрашивает разрешения подключиться. О том, что на самом деле это злоумышленник, вы можете не догадаться. Поэтому перед тем, как давать кому-то доступ к своим устройствам, нужно получить подтверждение у службы безопасности.

9

Что делать, если я параноик?

Как это ни странно, но «Электронное облако» рекомендует по-настоящему серьезные и важные вопросы решать, как и раньше, при личной встрече. Если вы все-таки вынуждены переписываться, то будьте на сто процентов уверены, что на той стороне действительно тот, кому вы хотите передать информацию. Используйте мессенджеры с дополнительным шифрованием

и секретные чаты, информация в которых сгорает; следите, чтобы ваш телефон не попадал в чужие руки.

И самое важное: помните, что главная уязвимость — это человек. Если у вашего собеседника не установлен пароль на телефоне, то никакое сквозное шифрование не защитит переписку при краже устройства.

«Электронное облако» предлагает комплексные решения по безопасности для бизнеса — от личной переписки до хранения конфиденциальных документов (серверы компании находятся в Германии). А еще «Электронное облако» проводит семинары по безопасности. Ближайший — как раз про мессенджеры — пройдет 28 февраля в Digital October. Вход бесплатный, но надо зарегистрироваться.
