Как защитить переписку и выбрать правильный мессенджер для чата

Давно пожухли, пожелтели страницы веб-форумов. Молодое поколение интернет-пользователей вряд ли помнит, как расшифровывается «IRC». Слово «аська» вызывает ностальгическую улыбку на морщинистых седобородых лицах интернет-аксакалов. Но идея чатов не умерла и даже не постарела. Появились социальные сети и мессенджеры. Они сделали общение более живым и насыщенным. В современных онлайновых чатах протекают серьезные рабочие процессы и льется беззаботный треп. Есть симпатичные эмодзи и яркие стикеры? Нет? Что это, набор унылых смайликов? Ты отстал от времени, разработчик.

Ладно. Как там с безопасностью?

Восемь коротких историй

Безопасность – не только технические штучки: пароли, шифрование, двухфакторная аутентификация. Безопасность зависит от модели угроз, организационных решений, от мотивированности и аккуратности пользователей.

История первая. Студент отправился на публичную акцию. Его задержали полицейские, доставили в отдел, отобрали смартфон, угрозами вынудили приложить к сканеру палец. А-а-а, смотрите, что у него тут: чат с друзьями, весь целиком, никак не защищенный. «Новое величие», версия 2.0.

История вторая. Идет вебинар, острая тема, каверзные вопросы в чате. Где-то в верхней части окна горит красная точка. Идет запись. Как эта запись будет использоваться? Где будет храниться? Кто получит к ней доступ? Участникам чата все это неведомо.

История третья. Конфиденциальная беседа. Поговорили – разошлись. Самый запасливый, не афишируя, перед выходом из виртуальной комнаты скопировал историю чата и сохранил ее в Word в папке «Документы» под названием «Чат от 20 декабря 2019 года». Мало ли что. Вдруг пригодится.

История четвертая. Чат под паролем, муха не залетит, но пароль тот же, что у онлайн-банка, у аккаунта на сайте путешествий, в интернет-магазине зоотоваров, у старого аккаунта на mail.ru.

История пятая. В правозащитной организации обыск. Изъяли компьютеры, смартфоны, прочие носители данных. У сотрудников организации есть доступ к важному чату (группе). Надо перекрыть этот доступ, временно удалить/выбросить этих людей из чата. Оказывается, сделать это удаленно можно, лишь зная их пароли.

История шестая. По совету зарубежных коллег в организации было принято решение перейти на корпоративный мессенджер. «Он очень хорош», – уверял консультант и показывал аппетитные скриншоты. Через пару месяцев выяснилось, что треть сотрудников избегают пользоваться новым чатом и не сообщили об этом ни менеджменту, ни техническому консультанту. Этап внедрения не продуман, ситуация с безопасностью усложнилась.

История седьмая. В защищенном корпоративном чате несколько десятков человек. Все они подключались в разное время. Уже месяц идет оживленная дискуссия о внутренней политике организации. Внезапно обнаружилось, что к чату имеют доступ люди, покинувшие команду полгода и год назад. Их просто забыли отключить.

История восьмая. Реплика с чрезвычайно важными данными о подготовке доклада по нарушениям прав человека случайно «попадает мимо». Вместо важного чата с коллегами, который подразумевал конфиденциальность, информация оказывается в совершенно другой группе. Окошки оказались рядом и были похожи.

Можно понять желание активистов заполучить «волшебную кнопку», универсальный, простой, хорошо защищенный чат. Раз и навсегда закрыть вопрос безопасности в этой части работы. К сожалению, волшебной кнопки не существует.

Выбираем чат

Что можно посоветовать команде, которой нужно выбрать рабочий чат.

1. **Оцените риски.** Прикиньте список **ценностей,** самых важных данных, которые могут оказаться в чате. Спросите себя, что угрожает этим ценностям, например, кто может хотеть получить информацию из чата?
2. Определите, какой **функционал** вам нужен. Достаточно ли текстового чата, или вы хотите также общаться голосом и проводить видеоконференции? Нужен ли чат с несколькими каналами? Требуются ли расширенные функции администрирования, скажем, возможность удалить из чата некорректно ведущего себя человека?
3. Посмотрите разные **технические решения,** которые обладают нужным функционалом (п. 2). Позволяют ли они защитить вашу ценную информацию (п. 1) на адекватном уровне? Оцените, какие ресурсы понадобятся, чтобы приобрести и внедрить то или иное решение в вашей команде. Например, сколько человек из вашей команды уже используют этот чат? Понадобится ли тренинг? Придется ли помогать коллегам устанавливать приложения на мобильные устройства?

Я знаю случаи, когда команды вынужденно и успешно «перестраивались» с одного технического решения на другое, но еще больше – увы! – мне известно ситуаций, когда члены команды пробовали какой-то продукт или сервис, сталкивались с трудностями, отступали и теряли всякую мотивацию («не пошло»). Скорее всего, второго шанса этот продукт/сервис не получит. Поэтому пусть ваше решение будет взвешенным.

На что обратить внимание в смысле безопасности.

1. Будете пользоваться **готовым сервисом** или устанавливать программное обеспечение **самостоятельно** (self-hosted)? Первый вариант подразумевает определенное доверие к разработчику – зато не понадобятся технические знания. Во втором случае возможна более тонкая настройка параметров безопасности, но и усилий придется приложить больше.
2. **Открытый код.** Продукт доступен пользователям не только готовым к запуску, но и в виде кода, на котором написан. Квалифицированный программист может проверить качество кода и убедиться, что в нем нет ошибок или заведомых «закладок» – лазеек для доступа к пользовательским данным.
3. Поддержка **шифрования** (в том или ином виде). В эпоху мессенджеров сквозное шифрование постепенно становится одним из «золотых стандартов».
4. Отсутствие непременной **привязки к телефонному номеру** – шаг на пути к анонимности участников чата (если она вам важна).
5. **Юрисдикция:** вряд ли можно советовать продукт или сервис, разработанный в стране с репрессивным или авторитарным режимом.

6. **Популярное** (распространенное) решение часто выигрывает потому, что пользователю легче найти квалифицированную техподдержку «на месте» – в своем регионе и даже в своей организации.

7. Важно, чтобы проект **активно поддерживался** разработчиком. Кому нужен чат, полный дыр, которые никто не спешит латать?

8. Есть информация о независимом **аудите** кода продукта? Это хорошо.

9. Если продукт/сервис **локализован,** ваши коллеги, плохо знающие язык оригинала, будут допускать меньше ошибок во время работы.

10. Хорошо, если чат **кросс-платформенный,** то есть его можно использовать на компьютерах и мобильных устройствах под управлением разных операционных систем.

Параметры безопасности чата (сервиса, приложения) – еще не все. Важно, чтобы было защищено само устройство (компьютер, смартфон).

Telegram и мессенджеры

Почему бы не сделать активистский чат на базе какого-нибудь популярного мессенджера? Нередко это самое простое и эффективное решение. Тысячи WhatsApp-чатов для родителей школьников по всей стране – яркий тому пример.

Среди российских активистов широкое признание получил Telegram, в немалой степени благодаря грамотной кампании продвижения со стороны Дурова и его команды, а также удивительно неэффективным репрессивным действиям государства. Организовать чат в Telegram и правда легко, но сам мессенджер не обладает полностью открытым кодом, привязывается к номеру телефона и не поддерживает сквозное шифрование по умолчанию. Эта функция доступна только в так называемом «секретном чате», который нужно инициировать отдельно и в котором может беседовать только два человека.

Рекомендуемый Сноуденом мессенджер Signal тоже привязывается к телефонному номеру, но выглядит предпочтительнее Telegram в смысле безопасности.

Если вы хотите большей анонимности и не боитесь экспериментировать, посмотрите в сторону групповых чатов на базе мессенджеров Wire и Briar. Они не требуют привязки к телефонному номеру (у Briar, правда, пока нет версии для iOS).

Среди полезных функций мессенджера стоит выделить возможность задания времени исчезновения сообщений. В Signal, например, можно указать значение в диапазоне от 5 секунд до 1 недели. При выборе этой опции через заданное время сообщения будут удалены у всех участников чата. Исчезающие сообщения – эффективный способ избежать попадания деликатной информации в чужие руки.

Чат на базе мессенджера хорошо подходит для организации быстрой работы в небольших командах, где нет потребности в параллельных чат-комнатах (каналах). Такое решение сравнительно легко внедрить, особенно если часть людей уже пользуются мессенджером.

Facebook и соцсети

Вы скажете, что Facebook Messenger – отдельное приложение, полноценный мессенджер, и будете правы. Почему я рассматриваю его отдельно? Для огромного числа пользователей этот мессенджер плотно интегрирован в социальную сеть и воспринимается как часть этой сети. Пользователи Telegram, с которыми я общался,

всегда знали о существовании функции «секретных чатов». Пользователи Facebook порой бывали удивлены тем, что, оказывается, такая функция есть в «их» мессенджере. На практике если «секретная переписка» (так она называется в Facebook Messenger) не включена по умолчанию, она используется только высоко мотивированными людьми и сравнительно редко.
Сколько ни повторяй мантры о конфиденциальности и защите важных данных, вам все равно будут сбрасывать «что-то срочное» в удобный чатик, который всегда под рукой.
Есть и другая особенность таких чатов: из-за того, что соцсети наполнены личной информацией, бывает весьма трудно разделять рабочее и личное. Пофигизм по отношению к безопасности личного контента может распространиться и на рабочую информацию.

Чаты «ВКонтакте» мы здесь рассматривать не станем по соображениям, связанным с юрисдикцией.

В целом чатики в соцсетях, на мой взгляд, подходят для эпизодического быстрого обмена не секретной информацией.

Jitsi Meet, вебинары и видеоконференции

Если вы не хотите приводить участников чата к единому «техническому знаменателю», возможно, вам подойдет Jitsi Meet (не путайте с Jitsi Desktop того же разработчика). Команда Jitsi Meet предлагает воспользоваться сервисом бесплатно и без обязательной установки на ваш сервер (при желании вы можете это сделать). С помощью Jitsi Meet можно проводить видеоконференции, там есть и функция текстового чата. Это бесплатное программное решение с открытым исходным кодом. Ничего не надо устанавливать, регистрировать и настраивать: достаточно любого веб-браузера и подключения к Интернету. (Руководство по использованию Jitsi Meet)
С точки зрения безопасности чудес ждать не стоит. Здесь нет регистрации и персональных аккаунтов, нет и такого понятия, как ведущий (владелец чата) с расширенными правами. Но есть, например, возможность выбрать для чат-комнаты любое название и установить на нее пароль: это как минимум уменьшит вероятность появления вторжения в беседу случайных людей. Содержимое чата исчезает, когда последний участник выходит из виртуальной комнаты. Это хорошо – не остается следов. При желании можно составлять что-то вроде протокола в документе Etherpad, вести аудиозапись чата с сохранением в облако и даже организовать трансляцию чата в Youtube.
Jitsi Meet лучше подойдет для нерегулярных онлайновых встреч маленькой команды, где высока степень доверия друг другу (вы знаете, что коллега не запишет ваш секретный разговор «на всякий случай») и не требуются серьезные права администратора/модератора. Jitsi Meet годится для простых вебинаров и видеоконференций с малым числом участников и без серьезных требований к правам модератора. Отсутствие регистрации означает не только простоту использования, но и возможность присоединиться к чату анонимно.
У Jitsi Meet есть конкуренты, работающие с использованием той же технологии WebRTC. На момент написания статьи я затрудняюсь назвать сопоставимое по функционалу бесплатное решение с приемлемым числом участников, работающее «из коробки».

Если ваши интересы лежат в области регулярных видеоконференций и вебинаров, а команда готова заплатить за такие приятные функции, как автоматическая рассылка email-оповещений о скором начале вашей встречи и настраиваемые права ведущих и участников, вам потребуется сервис типа Zoom (в бесплатной версии – не более 100 участников и не более 40 минут на чат). Здесь есть сквозное шифрование, хотя его придется включать отдельно, и другие опции безопасности.

Случается, что организатор чата собирает регистрационные данные не для эффективной работы сервиса, а для своих собственных нужд (например, для отчетности перед донором). Неискушенному пользователю может показаться, будто «система требует имя, фамилию, город проживания и место работы» (добавим сюда IP-адрес, используемые операционную систему и браузер), иначе «вебинар не получится». Если вас пригласили на подобное мероприятие и просят заполнить анкету с персональными данными, обратите внимание, есть ли у организаторов политика обработки персональных данных, и если да, что она собой представляет. Не сообщайте избыточную информацию. Не стесняйтесь настаивать на анонимности, если она для вас важна (например, не давайте реальные имя и фамилию).
Перед началом встречи – как и для офлайновых мероприятий – уточните у организаторов правила работы, в частности, ведется ли запись звука/видео, как и где эта запись будет впоследствии использована. Применяйте функции для защиты приватности, например, персональные сообщения. Так, хотя в Jitsi Meet все участники видят друг друга, вы можете отправить кому-то из них персональное сообщение. Во время вебинара Zoom можно задавать вопросы ведущим («панелистам») так, что их не увидят обычные участники.

Slack и корпоративные мессенджеры

У вас крупная команда с разными направлениями работы? Например, многопрофильная НКО с отделениями в разных регионах? Или редакция СМИ, где существуют разные отделы, да и бухгалтерии хочется иметь собственную площадку «для поговорить»? Может быть, вы ведете проект, включающий несколько направлений и целую компанию разных людей? Тогда вам пригодится корпоративный мессенджер с настраиваемыми каналами для чата. Самым известным таким сервисом является Slack. Его использование позволит забыть об одной из главных уязвимостей – внутрикорпоративной электронной почте. Slack позволяет эффективно отделить работу от личного, а рабочие процессы – друг от друга.
Ближайший конкурент Slack, с которым его чаще всего сравнивают, – Mattermost. Он бесплатный, имеет открытый код и, в отличие от Slack, является self-hosted, то есть Mattermost нужно устанавливать на свой сервер. (Slack «живет» в облаке.) С одной стороны, это требует технической квалификации от пользователя (или расходов на соответствующего технического специалиста). С другой стороны, пользователь становится полным хозяином всех опций и настроек, в том числе связанных с безопасностью (например, может обеспечить защиту хранящейся на сервере базы Mattermost с помощью полнодискового шифрования).
Если для вас в приоритете безопасность и вы готовы потратить некоторые ресурсы на установку/настройку корпоративного мессенджера силами специалиста, Mattermost –

хороший выбор. Если вы предпочитаете решение «из коробки», пусть даже и платное, и для вас важны возможности интеграции с разными сервисами, например, облачными хранилищами (Dropbox) или системами управления проектами (Asana, Trello), возможно, стоит выбрать Slack.

И напоследок

- **Позвольте!** – воскликнет раздраженный читатель, добравшийся до этой строчки. – Как это «напоследок»? А где наш любимый гиковский Riot/Matrix? А Microsoft Teams? Как насчет Google Hangouts? Что вы нам скажете за Skype? Почему не рассмотрены аспекты безопасности OpenMeetings? Вы вообще за открытый код или так, прикидываетесь?

  Дорогой читатель, мир программного обеспечения для коммуникаций не имеет границ. В Интернете несложно найти материалы с привлекательными заголовками вроде «12 лучших сервисов видеоконференций в 2020 году!». А у каждого из нас в смартфоне установлено не меньше трех мессенджеров, и каждому из этих чудесных приложений можно посвятить вдумчивую, детальную статью, даже если ограничиться вопросами безопасности. Мы надеемся на вашу способность находить полезные материалы на просторах Интернета, а тему безопасности коммуникаций Теплица будет освещать еще не раз.

Еще по теме:

- Безопасность мобильных устройств: зачем вам «полевой» телефон
- Видеоурок Теплицы: приложение для обхода блокировок Lantern
- «Пожалуйста, укажите свой номер…»: почему этого лучше не делать

Сергей Смирнов 23.12.2019

https://te-st.ru/2019/12/23/how-protect-activist-chat/