Рекомендации по использованию платформы «Zoom»

1. Защитите свою учетную запись

В первую очередь учетная запись Zoom — это еще один ценный аккаунт, и его тоже нужно защищать. Используйте надежный уникальный пароль и включите двухфакторную аутентификацию: она защитит ваш аккаунт, даже если учетные данные утекут в Сеть.

У сервиса есть особенность: помимо логина и пароля пользователь получает идентификатор персональной конференции (Personal Meeting ID, или PMI). Его довольно легко обнародовать — через PMI можно приглашать людей на публичные конференции в Zoom. Будьте с ним осторожны: делитесь PMI только с доверенными лицами, поскольку каждый, кто знает ваш идентификатор, может подключиться к любой организованной вами онлайн-встрече.

2. Используйте для регистрации в Zoom рабочую почту

Из-за странного сбоя, который на момент написания рекомендаций не был исправлен, Zoom считает, что все электронные адреса в одном домене (если только это не очень популярный домен, такой как @gmail.com или @yahoo.com) принадлежат одной компании. Поэтому сервис объединяет все аккаунты с одним и тем же доменом в группу, участники которой могут просматривать контактную информацию друг друга.

Например, это произошло с пользователями из Казахстана, чьи адреса заканчивались на @yandex.kz. То же может случиться с клиентами других небольших или малоизвестных провайдеров электронной почты. Поэтому для регистрации в Zoom мы рекомендуем использовать рабочую почту: не страшно, если вашу рабочую контактную информацию узнают коллеги. Если такой почты нет, заведите ящик в любом популярном публичном домене, чтобы сохранить личные данные в тайне.

3. Остерегайтесь поддельных приложений Zoom

Как выяснили исследователи «Лаборатории Касперского», в марте число вредоносных файлов, имена которых включают названия популярных сервисов для видеосвязи (Webex, GoToMeeting, Zoom и др.), увеличилось почти втрое по сравнению с прошлым годом. Это значит, что злоумышленники активно эксплуатируют растущую популярность Zoom и похожих приложений, пытаясь замаскировать вредоносные программы под клиенты для видеосвязи.

Не попадитесь на эту уловку! Загружайте клиенты Zoom для Windows и Mac только на официальном сайте сервиса zoom.us, а приложения для мобильных устройств — в App Store или Google Play.

4. Не делитесь ссылками на конференции в социальных сетях

Возможно, вы хотите не только общаться с коллегами или родственниками, но и проводить публичные конференции. Сейчас это единственный доступный формат публичных мероприятий — во многом по этой причине аудитория Zoom очень быстро

растет. Но даже если ваше событие открыто для всех, мы не рекомендуем публиковать ссылку на него в соцсетях.

Если вы уже знакомы с Zoom, то наверняка слышали о так называемом «зумбомбинге» (Zoombombing). Этот термин обозначает демонстрацию злоумышленниками нежелательного контента в конференции Zoom. О проведении предстоящих конференций злоумышленники узнают из публичных источников, в частности соцсетей. Поэтому старайтесь не публиковать ссылки на конференции Zoom в общедоступных ресурсах. Если вам все же нужно это сделать, отключайте для этих мероприятий опцию **Использовать идентификатор персональной конференции (PMI).**

5. Защищайте каждую конференцию паролем

Защита конференции надежным паролем — самый главный способ ограничить список участников теми, кого хотите видеть вы. С недавнего времени она применяется по умолчанию, и это очень хорошо (внимание: не путайте пароль конференции с паролем учетной записи). Как и ссылки на мероприятия, пароли конференций не должны всплывать в соцсетях и на других общедоступных площадках.

6. Включите комнату ожидания

Комната ожидания — еще одна полезная функция, которая теперь включена по умолчанию. Идея в том, что желающие присоединиться к собранию попадают в «лист ожидания» и остаются в нем, пока организатор конференции не одобрит их участие. Эта функция будет особенно полезна, если пароль от конференции все же попал в открытый доступ.

Также вы сможете переводить уже подключенных к конференции участников обратно в комнату ожидания, если они начнут мешать вам общаться. Мы рекомендуем не отключать эту настройку.

7. Обращайте внимание на настройки демонстрации экрана

Как правило, приложения для видеоконференций позволяют демонстрировать другим участникам экран устройства, и Zoom — не исключение. Обратите внимание на следующие настройки:

Кто может демонстрировать экран — только организатор или любой участник конференции. В случае публичной видеоконференции вы точно не захотите, чтобы случайные пользователи имели такую возможность, так что стоит эту возможность отключить.

Разрешена ли одновременная демонстрация экранов нескольких участников. Если вы не знаете наверняка, нужна ли вам эта возможность, скорее всего, она так и не понадобится, и лучше ее не разрешать. Просто имейте в виду, что такая настройка есть.

8. По возможности пользуйтесь веб-клиентом

Приложения Zoom имеют разные недочеты. Например, одна из версий позволяла злоумышленникам получать доступ к микрофону и камере устройства. Другая версия разрешала веб-сайтам добавлять к звонкам пользователей без их согласия. Разработчики

Zoom быстро исправили вышеупомянутые и некоторые другие проблемы. Также сервис перестал делиться данными пользователей с Facebook и LinkedIn.

Тем не менее, быстро решить все проблемы вряд ли получится. И в отсутствие независимой оценки безопасности приложения Zoom, вероятно, так и останутся ненадежными — например, продолжат раскрывать данные пользователей третьим сторонам. Поэтому для верности рекомендуем использовать Zoom в браузере и **не устанавливать приложения сервиса.** Веб-версия работает в «песочнице» и не имеет разрешений на устройстве, которые обычно требуют приложения. Это ограничивает ущерб, который она может нанести.

К сожалению, тут есть другая проблема. Даже если вы захотите воспользоваться веб-интерфейсом, может оказаться, что Zoom все решил за вас — загрузил установочный файл и для подключения к конференции требует приложение. В этом случае вы как минимум можете ограничить количество устройств, на которых установлен сервис, только одним. Пусть это будет ваш второй смартфон или редко используемый ноутбук — выберите устройство, на котором содержится минимум личной информации.

Кстати, если ваша компания использует Skype для бизнеса (ранее это приложение было известно как Lync), имейте в виду: оно поддерживает конференции Zoom и лишено упомянутых недостатков. Так что его можно использовать вместо клиента Zoom.

9. Не верьте рекламе сквозного шифрования в Zoom

Zoom стал популярен не только благодаря ценовой политике и своим возможностям, но и из-за разрекламированного создателями сквозного шифрования. Оно предполагает, что все коммуникации между собеседниками шифруются и расшифровать их могут только участники звонка (а все остальные, включая сотрудников Zoom Video Communications, — нет).

Звучит отлично. Но, как обнаружили исследователи безопасности, на практике дело обстоит иначе. Разработчикам Zoom пришлось признать, что под «сквозным» они имели в виду шифрование только до сервера Zoom. То есть, хотя видео и шифруется, сотрудники компании, теоретически могут получить к нему доступ. А вот текст чатов действительно защищен сквозным шифрованием, и к нему сотрудники Zoom получить доступ не могут.

10. Задумайтесь о том, что могут увидеть и услышать ваши собеседники

Этот пункт распространяется на все сервисы для видеосвязи, а не только на Zoom. Перед тем как подключиться к конференции, задумайтесь, что увидят и услышат ваши собеседники. Даже если вы одни дома, лучше привести себя в порядок и прилично одеться. Можно заодно убрать стикер с паролем, если он попадает в поле зрения камеры.

То же касается экрана вашего устройства. Если вы собираетесь демонстрировать его, закройте все посторонние окна, которые другим видеть нежелательно. Это может быть страница интернет-магазина, где вы собрались купить подарок для одного из участников, или сайт поиска работы, увидев который, ваш начальник вряд ли обрадуется.