Видеозвонки и видео-конференцсвязь: как защититься от хакеров

Автор лайфхака Колодий Евгения Анатольевна, 1 курс, направление «Менеджмент», гр. ДМ-101, НОЧУ ВО «Московский экономический институт»

Во всём – от домашнего обучения и полноценной удаленной работы до поддержания контактов с друзьями и членами семьи – мы все чаще полагаемся на интернет-технологии, чтобы оставаться на связи.

Во время пандемии видео-конференцсвязь оставалось ключевой при учебе и работе.

Видео-конференцсвязь **– один из важнейших элементов этого процесса.** *Так, в апреле 2020 года ежедневное количество участников встреч с использованием платформы Zoom достигло 300 миллионов человек, в то время как в декабре 2019 года их было всего 10 миллионов.*

В лайфхаке остановимся на основных вопросах, связанных с безопасностью видео-конференц-связи, и мерах, которые вы можете предпринять, чтобы защитить себя.

Насколько безопасны видеозвонки и видео-конференц-связь?

Нужно учесть несколько важных критериев:

- Использует ли сервис сквозное шифрование, которое ограничивает возможность посторонних перехватывать или подслушивать звонки?
- Использует ли сервис многофакторную аутентификацию, которая надежно защищает учетные записи пользователей?
- Основана ли технология на доступном для проверки открытом исходном коде, который считается более надежным, чем закрытое программное обеспечение?
- Ведется ли обмен данными между инструментом для видеозвонков и третьими сторонами или аффилированными лицами?
- Могут ли пользователи при необходимости безвозвратно удалить данные из сервиса и его репозиториев (как с клиентской стороны, так и с сервера)?

Примеры

- **Google G Suite** и **Microsoft Teams** не используют сквозное шифрование и открытый исходный код.
- В **Cisco WebEx**, **Zoom**, **Slack** и **Skype для бизнеса** недостаточно полно реализовано удаление данных.
- У **GoToMeeting** нет мультифакторной аутентификации.

Основные аспекты безопасности видеозвонков

- **Наличие сквозного шифрования**

Сквозное шифрование обеспечивает надежную защиту видео-конференц-связи, открывая доступ к звонку только соответствующим пользователям и никаким другим лицам и службам, включая само приложение.

- **Возможность перехвата и записи видеозвонков посторонними**

Могут ли посторонние наблюдать или записывать ваши видеозвонки? Кто и как может присоединяться к вашим звонкам? Учитывая, что при онлайн-обучении например в Zoom, нарушение приватности видеозвонков может стать вопросом безопасности детей. Доступ к звонку в Zoom осуществляется путем перехода по короткому цифровому URL-адресу, который легко можно сгенерировать или подобрать.

Основные аспекты безопасности видеозвонков

- **Условия использования данных вашей учетной записи**

Насколько строго соблюдаются политики конфиденциальности? Насколько прозрачны условия использования приложения в отношении сбора данных пользователей и предоставления третьим сторонам доступа к этим данным?

- **Хранение данных, связанных с вашим приложением для видеозвонков, на вашем компьютере или смартфоне**

Это особенно важно, если вы имеете дело с закрытыми сведениями или документами. Например:

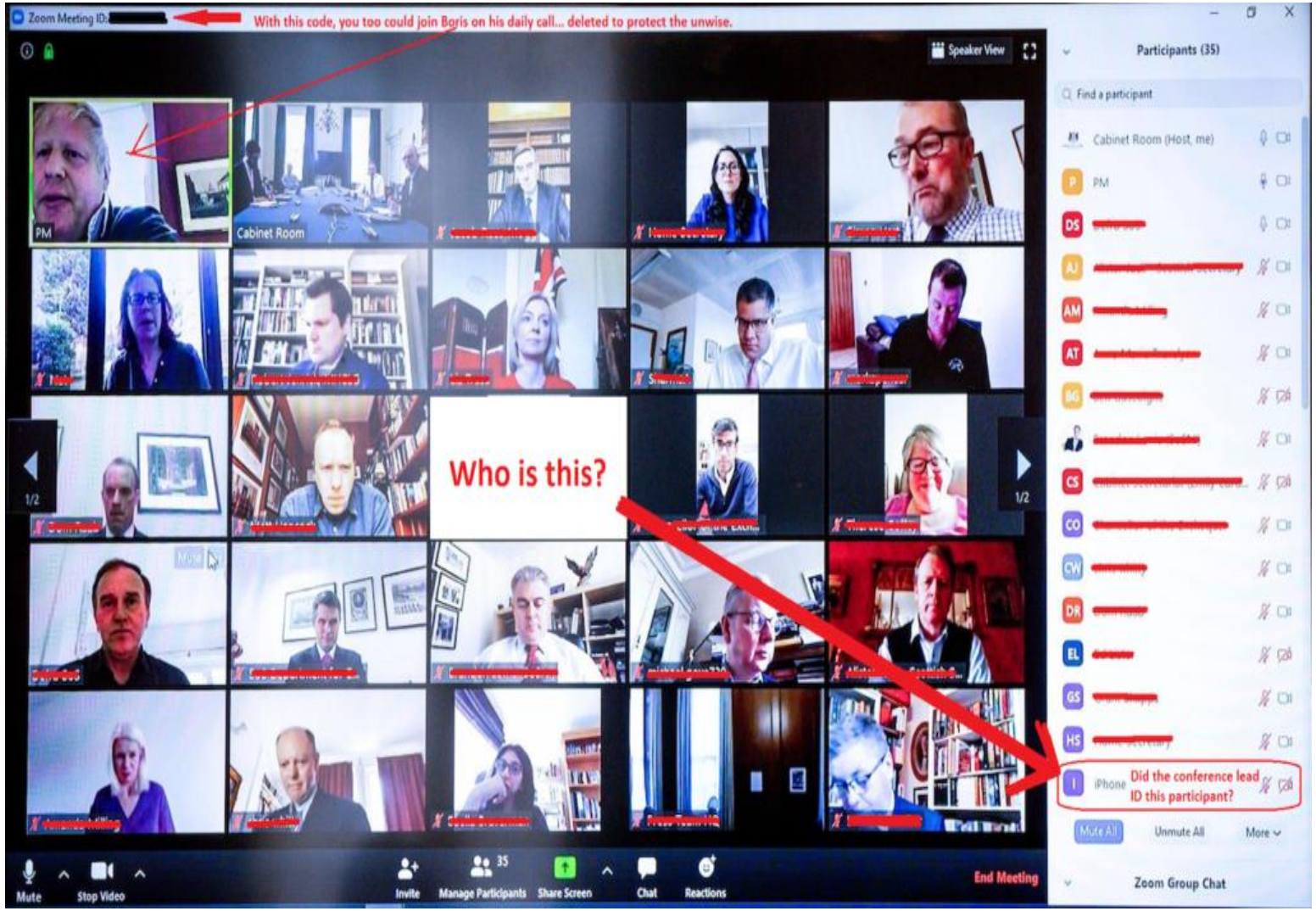
- ***Skype*** *сохраняет полученные вами фотографии на вашем устройстве, если вы не поменяете эту настройку (это можно сделать, выбрав пункт «Сообщения» в меню «Настройки» на устройстве под управлением Android или iOS).*

- *Если скачать переписку из чата видеозвонка в* ***Zoom****, она также будет включать содержание приватных чатов между отдельными участниками звонка. Это может вызвать проблемы, если вы не хотите, чтобы ваши личные сообщения во время рабочего звонка видел кто-то, кроме их адресата.*

- *Наличие инструментов наблюдения внутри приложения*

- ***Zoom*** *часто упрекают за функцию отслеживания внимания, которая информирует организатора звонка, если участник переключился на другое окно на 30 секунд или более. Эта функция позволяет работодателям и учителям проверять, следят ли их сотрудники или ученики за ходом рабочего совещания или урока.*

Примеры хакерских атак, связанных с видеозвонками



- Один из наиболее обсуждаемых в последнее время примеров атак на видеозвонки – **«Zoom-бомбардировки»**.

Так называют вторжения посторонних в видеоконференции с целью их срыва – например, незваные гости могут выкрикивать расистские лозунги или угрозы. Хотя название этого явления относится к приложению Zoom, похожие инциденты происходили и с другими платформами для видео-конференц-связи, включая WebEx и Skype.

Примеры хакерских атак, связанных с видеозвонками

- **На TikTok и YouTube** распространялись записи с видеозвонков в Zoom, на которых посторонние пользователи вторгались в видеочат с оскорбительными, расистскими или антисемитскими заявлениями, после чего организатору звонка приходилось завершать конференцию.
- Ранее обычный поиск в Google адресов, содержащих строку «Zoom.us», выдавал ссылки на не защищенные паролем конференции, что позволяло подключаться к звонкам без приглашения.
- Открытое вторжение в видеоконференции, каким бы неприятным и обескураживающим для участников оно ни было, вызывает куда меньше опасений, чем незамеченное присутствие посторонних, которое может стать серьезным риском как для корпоративной безопасности, так и для приватности персональных данных.

7 советов для защиты ваших звонков в Zoom

1. **Ограничивайте доступ к встречам при помощи паролей и обязательной аутентификации**. Так вы не позволите посторонним подключиться к звонку. Исключайте из беседы нежелательных или нарушающих порядок участников.
2. **Ограничивайте возможность демонстрации экрана**. Так вы гарантируете, что демонстрировать экран смогут только нужные участники.
3. **Будьте бдительны, когда переходите по ссылкам или открываете документы, присланные вам**. Используйте другие каналы связи, чтобы убедиться, что ссылку или документ вам отправил именно ваш собеседник.
4. **Не показывайте в кадре ничего лишнего**. Например, уберите из кадра все личные вещи или фотографии ваших детей, если вы не хотите, чтобы их рассматривали. В Zoom также можно изменить фон позади себя (другие приложения для видеоконференций, например Skype, дают возможность размыть фон).

7 советов для защиты ваших звонков в Zoom

5. **Убедитесь, что на вашем экране нет ничего лишнего, перед тем как демонстрировать его участникам**. Например, другие вкладки или окна приватных бесед, которые могут быть открыты, или документы, которые могут содержать закрытую финансовую информацию или личные данные. Следите за тем, чтобы случайно не показать письмо с вашим адресом на нем, ваш паспорт, кредитную карту или еще что-то, чего не должны видеть посторонние.
6. **Проверяйте настройки. Некоторые настройки безопасности не установлены по умолчанию.** Настройки Zoom для персонального компьютера и мобильного устройства отличаются – в версии для компьютера они более детализированы и дают больше контроля за безопасностью, нежели в мобильной версии. Например, в версии для компьютера организатор звонка имеет в распоряжении больше инструментов управления, а пользователи могут управлять заблокированными учетными записями.
7. **Старайтесь следить за обновлениями приложения.** Так вы будете в курсе всех доступных функций безопасности и приватности.

Способы обезопасить видеозвонки в разных приложениях

- Не показывайте лишнего
- Не давайте ссылку на видеочат всем подряд
- Не публикуйте ее в открытых постах в социальных сетях, онлайн-профилях, не рассылайте в групповых сообщениях электронной почты и не делитесь ею там, где ее могут увидеть посторонние
- Включите уведомления о пересылке сообщений о видеозвонках
- Установите надежный пароль
- Выбирайте приложения, использующие сквозное шифрование (Google Duo, Apple FaceTime, Cisco WebEx, GoToMeeting, WhatsApp, Signal)
- Регулярно обновляйте ПО
- Используйте функцию зала ожидания

Способы обезопасить видеозвонки в разных приложениях

- Загружайте приложения только из официального магазина приложений
- Созванивайтесь только с теми, кого знаете
- Задействуйте двухфакторную аутентификацию
- Закрывайте приложение, когда не пользуетесь им
- Не позволяйте записывать конференции
- Отключите любые опции, которые дают приложению слишком много прав
- Включайте видео с вашей камеры только тогда, когда это необходимо
- Соблюдайте осторожность при использовании публичных сетей Wi-Fi