Как безопасно пользоваться сервисами и мессенджерами.

Как и с любой популярной технологией, наряду с очевидными преимуществами в ряде сервисов есть и риски.

Zoom

Для общения с друзьями или проведения совещаний, он-лайн уроков многие стали использовать программы для видеоконференций. Самым популярным оказалось приложение Zoom. Однако сама программа попала в поле зрения киберпреступников, которые активизировались в последнее время. Произошел небывалый рост регистрации новых сайтов. Это страницы, которые маскируются под официальный сайт приложения Zoom и предлагают пользователю установить свою программу. Под ней скрывается вирусный троян PUA InstallCore. При попадании в компьютер вирус начинает закачивать туда дополнительное вредоносные программы и передает всю информацию своему настоящему владельцу. Либо эти ложные сайты используются для фишинга, обмана и использования людей.

Самая распространенная угроза при использовании Zoom – так называемый zoombombing, когда к онлайн-встрече присоединяется посторонний человек, часто с чисто хулиганских побуждений. «Зумбомбер» может транслировать во встрече провокационные видео, громко включать музыку и тому подобное.

Zoom позволяет записывать видеозвонки и экспортировать их как видеофайлы, как только звонок закончится. Проблема безопасности, возникающая при использовании этого инструмента: участники беседы могут экспортировать записанный файл, он может попасть в руки злоумышленников.

Как защититься в Zoom?

1. Не открывать и не запускать программу с неизвестных сайтов, даже если там обещают установку оригинального приложения. Старайтесь всегда использовать официальный сайт соответствующих программ.

2. Разработчики программного обеспечения регулярно выпускают обновления безопасности, которые закрывают известные уязвимости, и именно поэтому так важно **вовремя обновлять программное обеспечение на ваших устройствах.**

3. Используйте пароль для входа. Требование предоставить пароль перед входом в конференцию, помимо отображения номера вызова, обеспечивает достаточную безопасность.

4. Ни в коем случае не публикуйте свой идентификатор в Zoom и пароль в общем доступе.

5. Для организаторов конференции:

- включить функцию «Комната ожидания»;
- для каждой видеоконференции можно задать пароль и давать его только будущим участникам;
- отключить функцию входа раньше организатора;
- выключить функцию передачи файлов;
- включить оповещения, когда кто-то записывает/заканчивает встречу.

Skype

Вся информация вашей учётной записи Skype находится в открытом доступе, поэтому примите меры для защиты своих конфиденциальных данных.

1. **Добавляйте только тех, кого знаете.** Люди, не входящие в ваш список контактов, не могут разговаривать с вами через Skype или проверять ваш статус, пока вы не примете их запрос.

2. **Не вносите личную информацию в свой профиль.**

3. **Настройте параметры конфиденциальности.** Таким образом, вы сможете указать, кто может связываться с вами.

4. **Никому не сообщайте свой пароль.**

5. **Не открывай вложения электронной почты, полученные от незнакомых людей**, а также подозрительные вложения, даже полученные от известных вам людей. В случае сомнения следует связаться с отправителем и получить от него подтверждение того, что письмо не поддельное, даже если на первый взгляд оно кажется безобидным (например, вам пришла электронная открытка или забавная картинка).

WhatsApp

Как обезопасить свой аккаунт в мессенджере.

1. Включите двухфакторную идентификацию
По умолчанию подтвердить доступ к аккаунту нужно через SMS-сообщение. Но есть опасность, что злоумышленники получат доступ к вашему номеру. Чтобы обезопасить себя на этот случай, задайте дополнительный код-пароль, который нужно будет ввести при проверке учётной записи.

2. Сделайте аккаунт приватным
Не все знают, что в WhatsApp можно ограничивать, какую информацию о вас видят другие пользователи. Настройте, кто может видеть, когда вы были онлайн, смотреть ваши фото профиля, информацию об аккаунте и сетевой статус

3. Настройте, кто может добавлять вас в групповые чаты
Можно дать доступ всем, или же только пользователям из списка контактов — причём при желании вы можете запретить приглашать в группы даже некоторым людям из адресной книги. Для этого выберите вариант «Контакты, кроме…».

4. Регулярно обновляйте приложение
Чтобы обеспечить максимальную безопасность, устанавливайте последние обновления: в них закрывают найденные уязвимости.

YouTube

YouTube - самый большой архив видео с самым высоким трафиком. Для родителей, которые хотят уберечь своих детей от просмотра неподходящего контента, на сервисе предусмотрена функция родительского контроля. **Как поставить родительский контроль на Youtube можно посмотреть на сайте http://global.drfone.biz/ru/parental-controls/youtube-parental-controls.html**