«Обеспечение безопасности при работе с мессенджерами»

1. **Актуальные угрозы, связанные с использованием мессенджеров**

- **Вредоносные ссылки и файлы.** Злоумышленники используют методы социальной инженерии, чтобы побудить пользователя открыть файл или ссылку. Зачастую они представляются сотрудниками банка, подделывая «имя пользователя» и «фото профиля».
- **Сообщения с взломанных аккаунтов.** Получив доступ к учетной записи пользователя мессенджера, злоумышленник автоматически получает доступ ко всем его контактам. Это позволяет ему, выдавая себя за другого, рассылать по всем чатам сообщения с просьбой о перечислении денежных средств или с прикрепленными вредоносными файлами. Многие пользователи, получая такое письмо от своего коллеги или знакомого попадаются на уловку мошенника.
- **Предварительный просмотр ссылок.** При получении входящего сообщения, содержащего ссылку или файл, мессенджеры формируют небольшое окно предварительного просмотра с кратким описанием страницы или файла – так называемое «превью». Для того чтобы создать такое превью, программа автоматически открывает эту ссылку или загружает файл, что потенциально может привести к заражению устройства вредоносной программой.
- **Возможность доступа к переписке третьих лиц.** Вы можете использовать все известные способы защиты своего смартфона, но не в силах требовать того же от своих собеседников. Нет гарантии, что к их устройствам не получит доступ кто-то ещё. Например, у вашего знакомого украли телефон, который не был защищен пин-кодом. Злоумышленник сможет прочитать всю вашу переписку или восстановить её из резервной копии.
- **«Текстовые бомбы».** Существуют определенные наборы символов, которые мессенджер не в состоянии обработать. В результате получения сообщения с подобным набором текста нарушается нормальная работа программы, и её приходится переустанавливать.
- **Фишинговые атаки на аккаунты.** Выглядят они как правдоподобные запросы на вход в учетную запись, обновление платежной информации, подтверждение личных данных. При этом приложение будет оповещать о блокировки аккаунта. Если перейти на сайт по ссылке и ввести все данные, которые запрашивает мошенник, вы

рискуете утратить свой логин, пароль, аккаунт и денежные средства на ваших банковских картах.

2. Рекомендации по предотвращению угроз

- Скачивайте приложения мессенджеров только с сайтов разработчиков и официальных магазинов приложений.
- Настройте двухфакторную аутентификацию в приложении мессенджера предварительно завершив активные сессии на других устройствах
- Убедитесь, что выбранные вами приложения используют сквозное шифрование.
- Запретите в настройках получение сообщений от незнакомых контактов.
- Отключите автозагрузку файлов.
- С подозрением относитесь к полученным ссылкам и файлам, даже если они поступили от известного отправителя. Прежде чем переходить по ссылке или открывать файл, узнайте другим способом связи, действительно ли ваш знакомый отправлял их.
- Отключите функцию, позволяющую просматривать ваш профиль всем пользователям (сделайте его доступным только для ваших контактов).
- Избегайте обмена конфиденциальной информацией в чатах.
- Отключите функцию сохранения резервных копий переписки в облаке, т.к. они хранятся в незашифрованном виде.
- Соблюдайте осторожность при использовании мессенджеров через общедоступные сети Wi-Fi.
- Блокируйте свои устройства пин-кодом.
- Регулярно обновляйте все установленные программы и операционную систему своих устройств.
- Если сообщение вызвало у Вас малейшее подозрение, удалите его сразу же.