Актуальные угрозы кибербезопасности в Telegram

Telegram — один из самых популярных мессенджеров в России. Он используется для общения, ведения бизнеса, является источником новостей. На фоне роста количества пользователей платформы увеличивается и активность мошенников

Количество российских пользователей Telegram достигло 85 млн. В апреле 2024 г. сооснователь мессенджера Павел Дуров сообщил, что общая аудитория Telegram составляет около 900 млн пользователей. Разработчики позиционируют мессенджер как один из самых защищённых, поэтому уровень доверия пользователей к нему очень высок. Этим пользуются и мошенники. Они придумывают всё более изощренные схемы обмана и применяют методы социальной инженерии, направленные на кражу денег и данных.

Но наличие в мессенджере функций безопасности (например, шифрования) не даёт гарантий защиты от мошенников. Поэтому пользователи должны понимать, что при использовании даже технически защищённого мессенджера возможны киберугрозы. Кроме того, часть функций безопасности в Telegram отключена по умолчанию, их надо активировать для защищённой работы.

Основные цели атак через мессенджер:

Мошенничество:

Пользователя убеждают перевести денежные средства, подписаться на платный сервис, взять кредит, передать личную информацию.

Мошенничество с использованием вирусов:

Пользователя убеждают установить опасную программу (вирус, эксплойт и т.д.), которая может украсть деньги из интернет-банка, криптокошельков или других платежных сервисов. Возможно также использование устройства клиента для DDoS-атаки, чтения или отправки сообщений от имени пользователя;

Кража авторизационных данных (несанкционированный доступ):

Получение данных для сброса пароля с целью завладеть доступом к аккаунту пользователя, в том числе к его контактам и группам. Сделать это просто, если у пользователя не активирована двухфакторная идентификация.

Мошеннику достаточно перехватить сообщение с кодом сброса пароля, используя боты-двойники, приложения, сайты-дубликаты или дубликат сим-карты;

Получение конфиденциальной информации (утечки):

От карточных данных до паролей к системам и другой компрометирующей информации, в том числе составляющей коммерческую тайну.

Подробнее рассмотрим сценарии реализации атак через Telegram.

Фальшивые сборы средств

Злоумышленники используют новостной фон для сбора средств от имени правозащитных или благотворительных организаций. Они могут просить деньги или криптовалюту на юридическую защиту политзаключенных, помощь беженцам или животным в приютах. В таких схемах мошенники часто давят на эмоции, чтобы вызвать у жертвы желание срочно помочь. Для имитации правдоподобности могут использоваться реальные фотографии и истории.

Бесплатная премиум-подписка

Мошенники предлагают пользователям якобы бесплатный доступ к премиум-функциям Telegram, присылают ссылку для активации подписки. Однако она ведёт на фейковый Telegram-бот, замаскированный под официальный @PremiumBot. Для получения подарка бот запрашивает у пользователя номер телефона и авторизационный код. Как только злоумышленники его получат – сбросят пароль и получат доступ к учётной записи.

Фейковое голосование

Мошенники создают поддельные опросы или голосования, используя для привлечения внимания актуальную новостную или социально значимую повестку. Чтобы «проголосовать», пользователю необходимо перейти на страницу фишингового сайта, ввести свой номер телефона и авторизационный код. Так данные оказываются в руках мошенников, которые могут использовать их для сброса пароля и получения доступа к учётной записи.

Поддельные лотереи и розыгрыши

Злоумышленники запускают розыгрыши с привлекательными призами (смартфоны, автомобили или крупные денежные выплаты). Для привлечения внимания пользователей мошенники иногда создают фейковые аккаунты знаменитых личностей и имитируют розыгрыш призов от имени звезды. Для участия нужно заплатить небольшой «регистрационный взнос», скачать «специальное приложение» или ввести номер телефона и авторизационный код – так злоумышленники получают доступ к учётной записи. Часто для расширения охвата потенциальных жертв злоумышленники просят участников розыгрышей репостить сообщение или пригласить определённое количество друзей.

Мошеннические инвестиционные проекты

Злоумышленники создают фальшивые инвестиционные проекты или имитируют размещение токенов (Initial Coin Offerings или ICO), которые выглядят как перспективные стартапы в сфере криптовалюты или блокчейна. Мошенники активно рекламируют свои проекты в Telegram, обещая участникам быстрый и высокий доход. А после привлечения значительных денежных сумм фонд просто исчезает.

Иногда мошенники создают групповые чаты с предложением быстрого заработка — надо только вложить деньги. С подставных аккаунтов в группу пишут другие люди и делятся тем, как они якобы получили большую прибыль, прикладывают «доказательства» в виде скриншотов банковских приложений. А когда жертва переводит свои деньги – мошенники блокируют её аккаунт и удаляют группу.

Некоторые мошеннические инвестиционные проекты работают по принципу пирамиды, где выплаты первым инвесторам производятся за счёт средств, вложенных последующими. Такая схема может работать, пока поток новых инвесторов не иссякнет. После этого организаторы исчезают вместе с собранными средствами.

Фальшивые распродажи и сервисы

Мошенники создают Telegram-каналы или группы, где рекламируют популярные товары по привлекательным ценам. Это могут быть электроника, одежда, подписки на сервисы и даже авиабилеты. Визуально такие магазины могут выглядеть как настоящие, там могут использоваться профессионально оформленные баннеры, фото товаров и «отзывы довольных клиентов». Пользователей просят внести предоплату за товар или услугу, часто с обещанием быстрой доставки или моментального предоставления сервиса. После получения оплаты мошенники исчезают, закрывая канал или блокируя пользователя.

Пиратский контент и ПО

Некоторые каналы наряду с легитимным контентом публикуют ссылки на бесплатное скачивание фильмов, книг, музыки или ПО. Любители бесплатного контента не только нарушают авторские права, но и могут загрузить вредоносное ПО на своё устройство. Такая программа может украсть финансовую и личную информацию, зашифровать данные или сделать пользователя участником DDoS-атаки.

Мошенничество с криптовалютами

Мошенники создают фальшивые сервисы в Telegram, где предлагают выгодные курсы обмена криптовалют. Пользователи отправляют свои средства на указанный кошелёк, но обмен не происходит, и средства исчезают.

Под видом легитимных приложений или ботов злоумышленники распространяют криптодрейнеры – специальное вредоносное ПО для кражи денег из криптокошелька.

Мошенники могут продвигать несуществующие криптовалютные проекты и предлагать участвовать в первичном размещении токенов (ICO). Вкладчики теряют свои средства, так как проект оказывается фикцией.

Мошенничество с использованием поддельных аккаунтов

Злоумышленники создают профили, имитирующие аккаунты сотрудников правоохранительных, налоговых органов или других государственных учреждений. Они используют официальную символику организации и пишут зачастую под предлогом какой-либо проверки. Запугивая своих жертв, они просят перевести деньги на «безопасный счёт», который на самом деле является мошенническим.

Мошенники могут представляться руководителем конкретной организации и просить сотрудника предоставить конфиденциальные данные или перевести деньги со счёта компании. В таких случаях для большей убедительности используются не только фотографии поддельных документов, но и дипфейки.

Иногда мошенникам удается взламывать аккаунты пользователей и рассылать по списку контактов просьбу занять денег. При получении такого сообщения от родственника, друга или коллеги не стоит торопиться с отправкой перевода, нужно связаться с ним альтернативным способом и уточнить ситуацию.

Как защититься от мошенничества в Telegram

- Оставайтесь спокойными и не поддавайтесь давлению. Мошенники часто пытаются пугать или торопить жертву, чтобы не дать ей возможности критически оценить

ситуацию. Не совершайте никаких действий под давлением, дайте себе время подумать и проверить полученную информацию.

- Будьте осторожны с предоплатами и предложениями быстрого заработка. Если вам предлагают купить товар по слишком низкой цене или вложить деньги с обещанием дохода выше рыночного – это наверняка мошенничество. Внимательно проверяйте репутацию продавца и никогда не переводите деньги заранее.
- Проверяйте подлинность аккаунтов, сообщений и присланных документов. Если вам пишут от имени организации или известной личности, а вы сомневаетесь – свяжитесь напрямую через официальный сайт или по телефону.
- Не переходите по подозрительным ссылкам и не вводите личные данные, пароли или финансовую информацию на незнакомых сайтах или через сторонние приложения.
- Защитите ваш аккаунт в Telegram. Установите двухфакторную аутентификацию. Проверьте, не взломан ли ваш аккаунт и завершите все сеансы на незнакомых устройствах. Если с телефона это сделать не получается – попробуйте с компьютера. Помните, что первые 24 часа после сброса пароля очень важны. По правилам мессенджера, новый владелец не может вас исключить из сеанса в течение этого времени.