Актуальные угрозы в мессенджерах

Мошенничество с фейковыми аккаунтами

Злоумышленники могут создавать фейковые аккаунты, выдавая себя за известных личностей, топ-менеджеров, близких друзей и родственников. Они могут просить деньги, предлагать инвестиции или участвовать в розыгрышах, обвинять в финансовом мошенничестве или просить помочь с расследованием дела о государственной измене.

Как защититься:

- Относитесь критически к любым сообщениям в мессенджерах (текстовым, аудио, видео), содержащим просьбы о помощи, запросы от государственных органов, просьбы от топ-менеджеров, запросы конфиденциальной информации.
- Любые запросы и обращения подтверждайте у автора сообщения лично. О любых запросах от топ-менеджеров сообщайте непосредственному руководителю.

Кейс из жизни:

В апреле российские работодатели и сотрудники компаний стали жертвами нового вида мошенничества с использованием мессенджеров.

На этот раз активно используются полномочия сотрудников подразделений безопасности. Атаки развиваются по двум сценариям:

- Создание фейковых аккаунтов руководителей служб безопасности

- Взлом аккаунтов руководителей служб и подразделений безопасности в мессенджерах, общение от имени руководителя в рабочих чатах

При контакте преступники шантажируют сотрудников, обвиняя их в переводах денежных средств на Украину, а потом требуют перевести деньги на «безопасные счета», используя страх и манипуляции, чтобы заставить жертву действовать быстро.

Схема затронула и сотрудников ГК «Ростелеком», которые стали получать письма от имени фейкового аккаунта одного из руководителей по ИБ дочерней компании «РТК ИТ». В сообщении использовалось личное обращение, что свидетельствует об осведомленности мошенников

Вредоносные ссылки и файлы

Мошенники часто используют заражённые ссылки и файлы для распространения вирусов и шпионского ПО. Такие ссылки могут приходить в виде сообщений от организаций или знакомых и выглядеть как легитимные.

Рекомендации:

- Никогда не переходите по подозрительным ссылкам.
- Не открывайте файлы от незнакомых отправителей.
- Используйте антивирусное ПО для защиты устройства.

Кейс из жизни:

В марте злоумышленники начали массово рассылать сообщения, давя на страх и эмоции. Пользователи получали текст с трагической новостью о смерти знакомого, к которому прикреплено «фото умершего» — но на самом деле это вирусный apk-файл!

Как работает схема?

- Вы получаете сообщение: «Привет, знаешь же его? Сегодня ночью скончался... Мои соболезнования»
- Вложенный файл — НЕ фото, а троян, который заражает устройство
- Вирус начинает рассылать такие же сообщения всем контактам уже от вашего имени

Советы по безопасности:

- Никогда не скачивайте файлы с расширением *.apk или *.exe — фото и видео не бывают в таком формате!
- Незамедлительно удаляйте подобные сообщения
- Не переходите по подозрительным ссылкам и не открывайте вложенные файлы, если не уверены в их отправителе.

Развод на деньги

Существует множество схем, при которых мошенники обманом заставляют пользователей переводить деньги. Это могут быть просьбы о финансовой помощи, выгодные инвестиционные предложения, фальшивые благотворительные акции.

Советы по безопасности:

- Всегда проверяйте информацию перед тем, как переводить деньги.
- Не отправляйте деньги незнакомцам, даже если они утверждают, что находятся в бедственном положении.
- Будьте внимательны к предложениям, которые выглядят слишком привлекательно.

Кейс из жизни:

Алексей получил сообщение от «благотворительной организации», которая якобы собирала средства для помощи детям. Поверив в благую цель, он перевел деньги.

После тщательного расследования он выяснил, что сайт, на который он перевел деньги, был создан мошенниками, которые использовали лживые истории для обмана добрых людей. Алексей почувствовал себя преданным и разочарованным. Он осознал, что его добрые намерения были использованы в корыстных целях, и что он стал жертвой злоумышленников. Теперь Алексей понимает, насколько важно тщательно проверять организации, прежде чем помогать им финансово.

Шантаж и вымогательство

Мошенники могут угрожать пользователям раскрытием личной информации или компрометирующих материалов. Если вы оказались в такой ситуации, важно знать, как правильно поступить.

Действия при шантаже:

- Не поддавайтесь на угрозы и не переводите деньги.
- Сообщите о шантаже в правоохранительные органы.
- Убедитесь, что ваши аккаунты защищены надежными паролями и двухфакторной аутентификацией.

Кейс из жизни:

Ольга стала жертвой шантажа, когда ей на электронную почту пришло сообщение от неизвестных. В нем утверждалось, что у мошенников есть компрометирующие фотографии, которые могут подорвать её репутацию. Угрозы звучали очень убедительно: они требовали значительную сумму денег в обмен на молчание, угрожая распространить эти изображения в интернете и сообщить о них её близким. Ольга была в шоке и испытывала сильный стресс, но вместо того чтобы поддаться панике и выполнить требования злоумышленников, она решила действовать решительно.

Немедля, Ольга обратилась в полицию и рассказала о ситуации. Правоохранительные органы отреагировали на её заявление и начали расследование. Благодаря собранным доказательствам и информации, предоставленной Ольгой, злоумышленники были задержаны в кратчайшие сроки.

Социальные блага

Мошенники предлагают заменить полис ОМС, продлить договор услуг связи, бесплатно поменять электросчетчики, приглашают на бесплатную диспансеризацию. Цель таких действий, как правило, одна – получить код авторизации на портале Госуслуг, при помощи которого потом можно будет узнать всю информацию о владельце личного кабинета, а при низком уровне защиты – взять кредиты или осуществить незаконные сделки.

Действия при подобных звонках:

- Не продолжать разговор с позвонившим, перезвонить в организацию, от имени которой поступил звонок, по официальному телефону.
- Никогда и никому не сообщать СМС-коды.
- В личном кабинете портала госуслуг установить настройки безопасности, которые не позволят проводить никакие сделки без вашего присутствия.

Кейс из жизни:

Одному из сотрудников Ростелекома позвонил представитель страховой компании с предложением обновить полис ОМС с бумажного на пластиковый. Для замены необходимо было «взять талон на получение полиса, а код электронной очереди продиктовать собеседнику». Наш коллега, к разочарованию злоумышленника, назвал случайную комбинацию из 6 цифр, а вовсе не пришедший ему по СМС код от личного кабинета госуслуг. Мошенник разозлился и бросил трубку.

Если ваш аккаунт в Telegram угнали…

Если вы столкнулись с ситуацией, когда ваш аккаунт в Telegram был скомпрометирован и от вашего имени ваши друзья, знакомые и коллеги стали получать просьбы о финансовой помощи, важно быстро и правильно отреагировать. Ниже представлены различные сценарии и рекомендации по их разрешению.

Вариант 1: Злоумышленник завершил вашу сессию, но вы смогли авторизоваться заново

Если вы смогли повторно войти в свой аккаунт, это означает, что с момента авторизации злоумышленника прошло менее 24 часов. В течение этого времени пользователь не может завершать активные или новые сеансы.

Что делать?

- Завершите все неактивные сеансы:
  Настройки › Устройства › Активные сеансы › Завершить все другие сеансы.

Вариант 2: Вход в ваш аккаунт с постороннего устройства

Если вы потеряли доступ к аккаунту на своем смартфоне, но всё еще можете войти с другого устройства, подумайте, где еще вы могли авторизоваться (например, на ноутбуке или ПК).

Что делать?

1. Завершите все неактивные сеансы:
   Настройки › Устройства › Активные сеансы › Завершить все другие сеансы.

2. Если ваш email всё еще привязан к аккаунту, незамедлительно смените облачный пароль:
   Настройки › Конфиденциальность › Облачный пароль › Установить пароль.

3. Если злоумышленник сменил облачный пароль и привязал свою электронную почту, сбросьте «чужую» почту:
   Настройки › Конфиденциальность › Облачный пароль › Забыли пароль › Нет доступа к электронной почте › следуйте инструкциям.
   Обратите внимание, что процедура сброса пароля занимает до 7 дней.

Вариант 3: Полный контроль злоумышленника над аккаунтом

Если злоумышленники сменили пароли и привязали новую электронную почту, вам, вероятно, придется удалить аккаунт и создать его заново. При этом все данные и история чатов будут удалены, а возможность создать новый аккаунт на тот же номер появится через несколько дней.

Как удалить аккаунт:

Запрос в техподдержку:

- abuse@telegram.org
- https://telegram.org/support

Для восстановления утраченного аккаунта рекомендуем обращаться по трем каналам:

- В техподдержку мессенджера: https://telegram.org/support
- По электронной почте: recover@telegram.org
- В волонтёрскую службу поддержки: Настройки › Помощь/Задать вопрос › следуйте инструкциям в чате.

Рекомендации по безопасной работе в мессенджерах

Используйте надежные пароли

Создавайте уникальные и сложные пароли для каждого мессенджера. Избегайте использования одинаковых паролей для разных аккаунтов. Рекомендуется использовать комбинацию букв, цифр и специальных символов.

Включите двухфакторную аутентификацию

Двухфакторная аутентификация добавляет дополнительный уровень защиты. Даже если злоумышленник получит ваш пароль, ему потребуется второй фактор (например, код, отправленный на ваш телефон) для доступа к вашему аккаунту.

Будьте осторожны с личной информацией

Не делитесь личной информацией, такой как номера телефонов, адреса или финансовые данные, в мессенджерах, особенно с незнакомыми людьми. Помните, что мошенники могут использовать эту информацию для обмана.

Проверяйте источники информации

При получении сообщений с просьбами о помощи или финансовых предложениях всегда проверяйте информацию. Используйте официальные каналы и сайты для подтверждения достоверности сообщений. Если кто-то просит вас о помощи, попробуйте связаться с ним через другие средства связи, чтобы убедиться, что это не мошенничество.

Регулярно обновляйте приложения

Обновления приложений часто содержат исправления безопасности, которые защищают вас от новых угроз. Убедитесь, что у вас установлены последние версии мессенджеров и других приложений.

Будьте внимательны к настройкам безопасности

Настройки безопасности в мессенджерах играют важную роль в защите вашей личной информации и контроле над тем, кто может с вами общаться. Правильная настройка этих параметров поможет ограничить доступ к вашим данным и обеспечит большую защиту от нежелательных контактов. Давайте обратим внимание на настройки безопасности вашего аккаунта в Telegram, чтобы избежать потенциальных угроз:

1. Убедитесь, что ваш аккаунт привязан к актуальному номеру телефона, который находится под вашим контролем.
2. В личном кабинете вашего мобильного оператора включите двухфакторную аутентификацию для номера, к которому привязан аккаунт Telegram.
3. В настройках Telegram в разделе «Конфиденциальность и безопасность» активируйте двухфакторную аутентификацию.

4. Проверьте настройки видимости вашего номера телефона в разделе «Конфиденциальность» и отредактируйте их по необходимости.
5. В разделе «Конфиденциальность/Устройства» отключите все неиспользуемые устройства и установите минимальный срок автоматического завершения сеансов — не более одной недели.
6. В настройках «Данные и память» отключите автозагрузку медиафайлов, чтобы предотвратить загрузку нежелательных материалов.
7. Убедитесь, что на вашем телефоне установлено актуальное и регулярно обновляемое антивирусное приложение.
8. Запретите установку приложений из неизвестных источников в настройках вашего мобильного устройства.
9. В настройках Telegram отключите возможность добавления вас в различные каналы без вашего согласия.

Следуя этим рекомендациям, вы сможете значительно снизить риски и сделать свое общение в мессенджерах более безопасным. Помните, что безопасность — это не только технологии, но и ваша бдительность!

Перейти в канал

Полезную информацию из мира кибербезопасности вы можете найти не только в наших кибердайджестах, но и в телеграм-канале «Кибербез в Ростелекоме»