Как не стать жертвой мошенника в Telegram

Сценарий к презентации

Цель — информирование обучающихся о мошеннических схемах в популярном мессенджере Telegram.

Задачи:
— Знакомство с основными видами, формами и способами мошенничества в Telegram.
— Формирование навыка распознавания мошеннических схем.
— Развитие навыка критического мышления.

Время проведения: 30-40 минут.

Необходимые материалы:
— Презентация с материалом.
— Экран.
— Мультимедийное пространство.
— Столы и стулья для участников.

Ход мероприятия:

Слова модератора (куратора группы)

Добрый день! Сегодня мы поговорим с вами о том, что такое мошенничество, какие схемы мошенничества существуют на данный момент в «Telegram», как нам с вами не стать жертвой обмана.

Современные виды мошенничества уже давно ушли от привычных схем обмана с помощью продаж товаров на улице, рассылок смс-сообщений с внезапными призами и гадалок по телефону. Многие мошенники уже давно перешли в интернет-пространство и стали использовать мессенджеры в качестве наживы.

Это коснулось и такого, на первый взгляд защищенного приложения, как Telegram, который уже стал излюбленным орудием для хакеров и аферистов.

Так что же такое мошенничество и как нам не попасться на удочку обмана? Давайте разбираться.

Под мошенничеством, чаще всего понимается хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием.

При этом обманом может быть как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман). В обоих случаях обманутая жертва передает своё имущество мошеннику.

Вопрос на обсуждение: Какие схемы мошенничества в Telegram вы знаете? (Ответы участников).

С помощью различных методов воздействия мошенники получают от обманутых жертв личные данные (логин, пароль, реквизиты банковских карт, доступ к личным перепискам и далее), денежные переводы и необходимую информацию для дальнейшего обмана.

Многие схемы мошенничества, можно условно разделить на четыре основных вида:

• **Фишинг** – это вид мошенничества, при котором главной целью злоумышленника, является получение доступа к персональным данным пользователя (логин, пароль, банковские реквизиты и т.д.).

• **Фарминг** – это вид мошенничества, при котором злоумышленник устанавливает вредоносные программы или вирусы.

• **Смишин**г – вид мошенничества, при котором пользователям в сообщениях приходит просьба перейти по ссылке.

• **«Двойная транзакция»** – мошенничество, при котором во время оплаты товаров и услуг продавец сообщает об ошибке и предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций.

Давайте более подробно разберем на примерах.

1. Фишинг-мошенничество.

Домовые чаты стали такой же нормой, как чаты с друзьями. Так вот, многие аферисты в последнее время стали размещать в подъездах объявления о создании нового «домового чата» (рисунок 1). Там можно найти сведения по вопросам ЖКХ и общаться с соседями. На данную уловку попадаются многие люди.

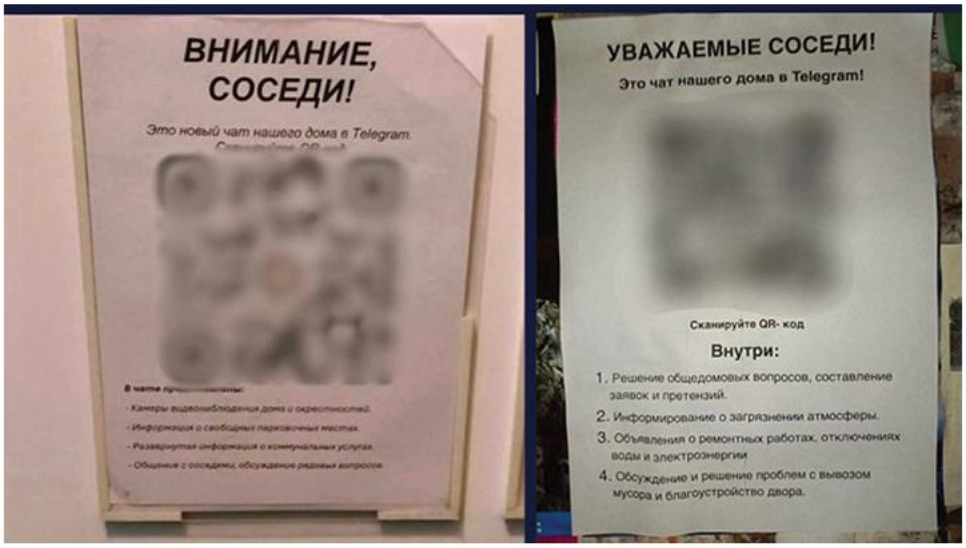

Рисунок 1 – пример мошеннической схемы

Вопрос на обсуждение: как вы думаете, что нужно сделать, чтобы не попасться на этот обман? (Ответы участников).

Чтобы обезопасить себя от данного вида обмана, стоит сначала уточнить у других жильцов или у главы дома, насколько данное объявление правдивое.

2. Фарминг-мошенничество.

Как вы знаете, Telegram имеет возможность создавать каналы и предлагать услуги. Многие компании, маркетплейсы, магазины также перешли в мессенджер для продажи своих услуг, что стало возможностью для мошенников.

В Telegram мошенники создают каналы от лица «известных экспертов», магазинов, блогеров и т.д. Фейковые сайты продают услуги или товары ниже официальных цен, привлекая этим других пользователей. В канале могут быть поддельные отзывы от «покупателей», чтобы расположить к себе других людей. В момент ввода платёжных данных информация попадает в руки к мошенникам.

В первую очередь, стоит обратить внимание на сам канал, с которого происходит взаимодействие с мошенником. Официальные представители имеют верификацию в мессенджере (голубая звездочка), а также ссылки на другие источники и мессенджеры.

3. Смишинг-мошенничества.

Одной из популярных мошеннических схем является «Telegram Premium».

Мошенники взламывают Телеграм-аккаунты и под видом друга, знакомого, коллеги, присылают в подарок подписку на «Telegram Premium».

Чтобы пользователь перешел по ссылке, мошенники маскируют ее за привлекательным предложением.

Фейковое приложение Telegram Premium имитирует страницу авторизации, благодаря чему мошенники похищают данные пользователя и загружают вредоносные программы. С его помощью злоумышленники получают полный доступ к устройству.

Теперь, предлагаю поговорить о том, каких же мошеннических схем в Telegram нужно остерегаться. Рассмотрим основные:

1. Мошенничество «Друг в беде».

Мошенники взламывают аккаунты пользователей, чтобы от их имени рассылать сообщения (рисунок 2). Как правило, в сообщении они пишут от лица родственника, близкого друга, коллеги и рассказывают о трудной ситуации, в которую попал владелец взломанного профиля.

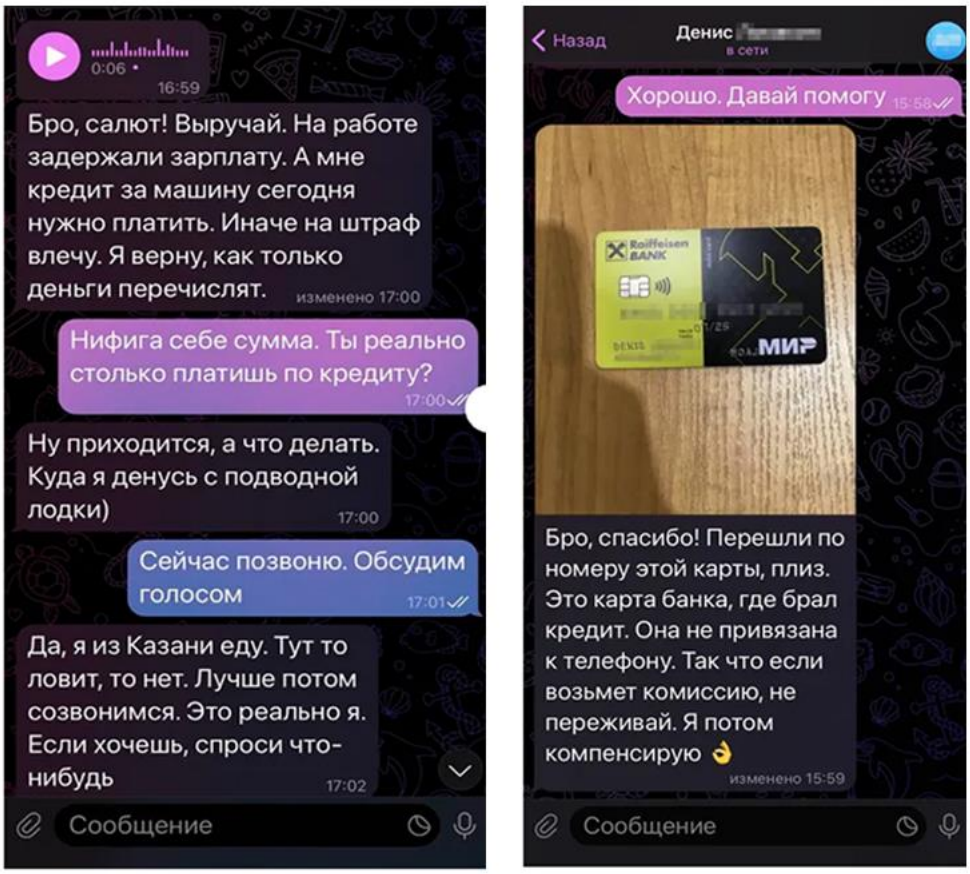

Рисунок 2 — пример общения с мошенником

Как распознать такого мошенника?

— Обращайте внимание на язык общения: похож ли он на манеру выражаться вашего друга или родственника? Нет ли каких-то странностей?

— Фактор времени. Стал бы ваш родной или друг просить о срочной помощи, не поясняя детально, что случилось?

Что делать?

— Позвоните близкому или родственнику, чтобы убедиться в том, что помощь нужна именно он ему, а не мошеннику.

— Если у вас возникли подозрения, задайте вопросы, ответы на которые способен дать только реальный друг или родственник – например, поинтересуйтесь, чем вы занимались, когда виделись в последний раз.

— Если вы убедились, что имеете дело с мошенником, тут же его блокируйте и срочно предупреждайте об этом друзей и родных, чтобы они не стали очередными мишенями обмана.

2. Мошенничество «Лягушонок Пепе».

«Лягушонок Пепе» - популярный интернет-персонаж в Telegram. Основной метод обмана связан с тем, что пользователю приходит ссылка на подарок от Telegram со ссылкой на различные виды коллекционных

предметов, куда входит и Лягушонок Пепе. Для получения призов требуется подключить свой криптокошелёк к сайту или пройти по ссылке. Пользователь авторизуется на поддельном сайте, где ему предлагается подписать транзакцию, после чего доступ к его кошельку получает вредоносная программа, которая быстро опустошает счет.

Как распознать такого мошенника?

— Обращайте внимание от кого именно пришел «подарок с Лягушонком». Если до этого ваш друг или знакомый не проявлял такой щедрости ранее, то стоит насторожиться.

— Помните, что официальным представителям Telegram не выгодно раздавать призы бесплатно.

Что делать в таком случае?

— Скачивайте Telegram предметы только в официальных магазинах приложений.

— Не храните в папке «Избранное» пароли, данные банковских карт, документы и любую другую конфиденциальную информацию.

— Не переходите по сомнительным ссылкам и предложениям.

3. Мошенничество «Бот-атаки».
Платформа Telegram позволяет пользователям создавать бот-аккаунты, с помощью которых злоумышленники атакуют своих жертв (рисунок 3).

Поддельный бот отправляет пользователям сообщения, что их аккаунт не прошел верификацию. Далее бот предлагает перейти по ссылке и ввести свои данные заново — так они попадают в руки злоумышленников.

Есть другой вариант схемы: пользователь получает сообщение о том, что кто-то зашел в ваш аккаунт с другого устройства и необходимо подтвердить свои данные снова.

Рисунок 3 — пример мошеннической схемы

Как защитить себя?

— Обратите внимание на сам бот. Если на него пожаловалось большое количество пользователей, он будет иметь пометку **«Scam».**

— Обратите внимание на орфографические ошибки. Боты мошенников могут содержать ошибки в тексте и предлагать упрощённые программы ответов.

4. Мошенничество «Выгодные крипто-предложения».

Вопрос на обсуждение: кто-нибудь знает, что такое криптовалюта? (Ответы участников).

Криптовалюта – это разновидность цифровой валюты, не имеющая физического выражения (не выпускается в монетах или банкнотах), однако имеющая цену (например, чтобы купить криптовалюту нужно заплатить деньги).

Telegram стал платформой для людей, интересующихся криптой. Многие мошенники стремятся получить доступ к криптокошелькам пользователей или предлагают воспользоваться «заманчивыми» услугами обогащения и вложения (рисунок 4).

Рисунок 4 — пример предложения о криптовложении от мошенника

Вопрос на обсуждение: По каким маркерам, вы понимаете, что это мошенник? (Ответы участников).

Что делать, если вам пишет такой мошенник?

— Игнорируйте всех, кто сулит «гарантированную» прибыль от любых инвестиций.
— Не размещайте средства на криптокошельке, который вам прислали по ссылке – зачастую, они ложные.
— Никогда не посылайте деньги, криптовалюту или данные аккаунта лицам, с которыми вы контактировали исключительно через Telegram.

5. Мошенничество с военными билетами.
Мошенники начали предлагать пользователям Telegram приобрести военные билеты. Злоумышленники размещают объявления в Telegram и обещают внести данные в официальные реестры. Кроме того, предлагаются услуги по возврату водительских прав после их лишения. Правоохранительные органы уточняют, цель злоумышленников — заставить доверчивых граждан, которые стремятся получить желаемые документы, внести предоплату.

Как распознать мошенника?

— Помните, что военный билет или водительское удостоверение оформляют только официальные представители (военкомат, ГИБДД), какая-то сомнительная организация в мессенджере его выдать не может.

Что делать?
— Не отвечайте на предложение и блокируйте мошенника.
— Если вы заплатили мошеннику, то немедленно обращайтесь в полицию.

Завершение.

Мошенничество стало распространенным явлением в нашей жизни. Аферисты с каждым днем внедряют новые схемы обмана, что ставит под угрозу информационное пространство и создает риск оказаться жертвой в их офере.

Для того, чтобы обезопасить себя и своих близких, стоит помнить о простых правилах:

— Не вводите на сторонних ресурсах код, который присылает служба поддержки Telegram, при авторизации с нового устройства.
— Не скачивайте взломанные приложения в целях экономии времени и ресурсов.
— Не соглашайтесь на сомнительные и незаконные услуги. Если вас обманут, вы даже не сможете обратиться с претензией в суд. Вам могут поступать предложения очистить кредитную историю или оформить фальшивые документы. Это уловки!
— Установите антивирус, который будет проверять все скачиваемые файлы.

— Обращайте внимание на оформление официальных аккаунтов Телеграмм (наличие синей галочки). Официальный сервис техподдержки нельзя ни заблокировать, ни добавить в список контактов. Но это можно сделать, если канал фейковый.
— Включите двухфакторную аутентификацию. Так защита аккаунта будет надёжнее.

Главное — проявлять здоровый скептицизм. Не верьте слишком уж заманчивым предложениям и берегите себя.