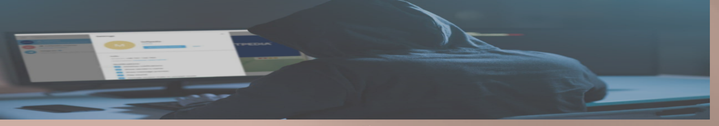
Мошенники в Telegram.

Путилина В.Е
Сибирский Университет Потребительской Кооперации Г.Новосибирск.



Проблема:

Telegram стал основной площадкой для реализации разнообразных мошеннических схем, которые причиняют значительный финансовый ущерб пользователям. Анонимность платформы и возможности автоматизации через ботов активно используются злоумышленниками для массового распространения обманных предложений. Схемы варьируются от предложений «быстрого заработка» на инвестициях и криптовалютах, до фишинговых атак, имитирующих официальные сервисы, и способов получения доступа к аккаунтам пользователей для дальнейшего распространения мошеннических сообщений среди их контактов.

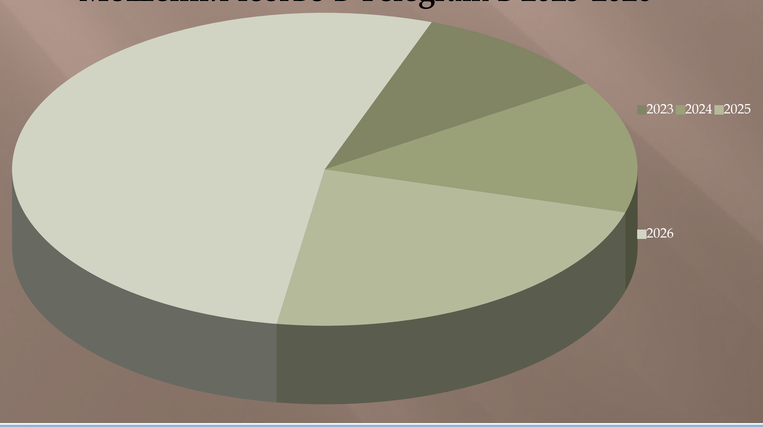
Цели работы:

•.Изучить основные виды мошенничества в Telegram
•Проанализировать методы защиты от мошенничества в Telegram и предложить рекомендации по повышению безопасности.
•Оценить мошенничество в Telegram в последние годы

Актуальность темы:

•Стремительный рост аудитории: Telegram превратился из обычного мессенджера в глобальную экосистему с финансовыми инструментами (криптовалюты, платежные боты), что привлекает киберпреступников огромным количеством потенциальных жертв.
•Инструменты анонимности: Технические особенности платформы (скрытые номера, удаление переписки у обоих участников, создание ботов) позволяют мошенникам сохранять анонимность и автоматизировать массовые атаки.
•Переход к социальной инженерии: Современные атаки всё реже строятся на взломе программ и всё чаще — на психологической манипуляции («угон» аккаунтов через голосования, фейковые админы, схемы «быстрого заработка»), к которым пользователи зачастую не готовы.
•Угроза финансовой безопасности: Масштаб ущерба от мошенничества в мессенджерах ежегодно растет, подрывая доверие к цифровым банковским сервисам и требуя от специалистов банковского дела разработки новых методов защиты клиентов.2

Мошенничество в Telegram в 2023-2026



3.Представленные данные демонстрируют устойчивый и значительный рост случаев мошенничества в Telegram: с 23% в 2023 году до 58% в 2026 году. Это свидетельствует о нарастающей остроте проблемы и необходимости усиления мер безопасности.

Решение проблемы:

Чтобы избежать попадания в ловушку мошенников, рекомендуется соблюдать ряд простых правил:

1.Проверяйте подлинность ссылок. Никогда не переходите по подозрительным ссылкам и проверяйте адреса перед вводом любых данных.

Настройте двухфакторную аутентификацию. Это значительно усложняет процесс взлома вашего аккаунта.

2.Будьте осторожны с незнакомцами. Не сообщайте личную информацию лицам, которым не доверяете.

3.Регулярно обновляйте приложение Telegram. Разработчики регулярно выпускают обновления, устраняющие уязвимости системы

1.Основные типы мошенничества в Telegram:

Фишинговые атаки-заключаются в создании поддельных аккаунтов, похожих на известные бренды или знаменитостей.

Кража аккаунта-преступники используют методы социальной инженерии, взлома SIM-карт или фишинга для кражи учетных записей пользователей. Получив контроль над аккаунтом, мошенники начинают рассылать спам своим контактам или требуют деньги от друзей жертвы, утверждая, что попали в беду.

Фиктивные розыгрыши и акции-

распространенным видом мошенничества являются фейковые конкурсы и лотереи. Преступники предлагают участникам бесплатные призы или скидки, но взамен запрашивают личные данные, номера банковских карт или требуют предоплату за доставку призов.

Создание ботов-мошенников-некоторые злоумышленники разрабатывают вредоносные программы («боты»), способные автоматически собирать персональные данные пользователей или даже осуществлять переводы денежных средств с привязанных счетов.

2.Методы защиты

Технические: Двухэтапная аутентификация (облачный пароль) предотвращает угон аккаунта. Настройки конфиденциальности (скрытие номера, ограничение на добавление в группы) снижают риск таргетированных атак. Функция «Активные сеансы» позволяет контролировать устройства. Система жалоб помогает блокировать мошенников. Верификация (синяя галочка) отличает подлинные аккаунты.

Поведенческие: Основаны на критическом мышлении и проверке информации. Игнорирование предложений быстрого заработка, подозрительных ссылок и просьб о передаче кодов/данных карты. Отделение финансовых операций через ботов от основных банковских карт.

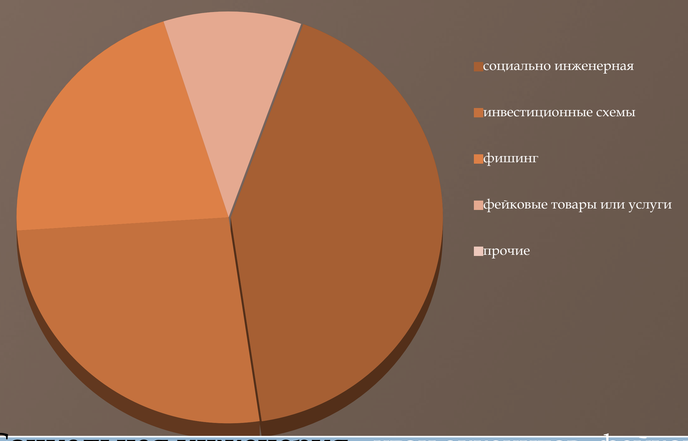
Рекомендации

Обязательно: Активируйте двухэтапную аутентификацию и настройте конфиденциальность (скрытие номера, ограничение на добавление в группы).

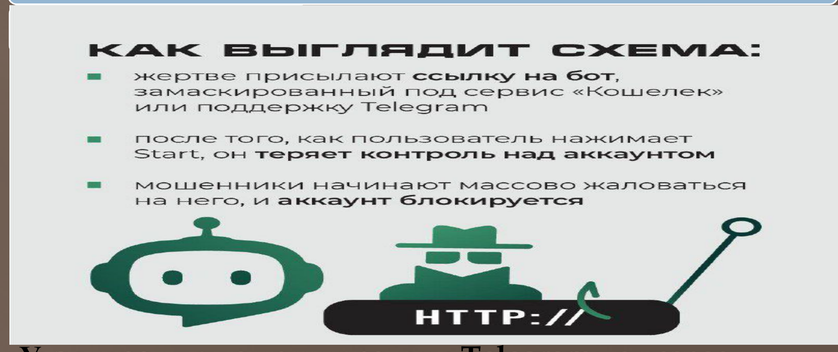
Никогда: Не переходите по подозрительным ссылкам, не сообщайте коды из SMS и данные карты.

Всегда: Проверяйте подлинность отправителя и критически оценивайте предложения о заработке.

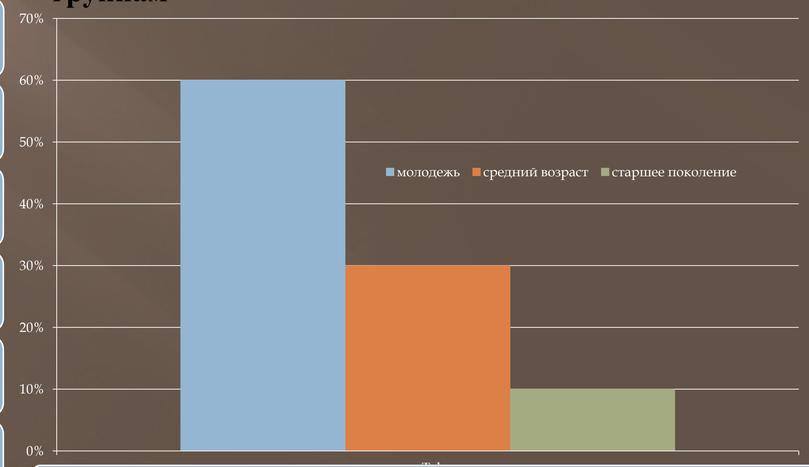
Типы мошенничества в Telegram:



Социальная инженерия - угон аккаунтов, фейковые конкурсы.
Инвестиционные схемы - крипто-пирамиды,псевдо-трейдинг.
Фишинг - поддельные ссылки, сбор данных карт
Прочие - шантаж, вирусы



Уязвимость к мошенничеству в Telegram по возрастным группам



Молодежь - 18-25 лет
Средний возраст - 26-45 лет
Старшее поколение - 45+ лет

Заключение::

Проведенный анализ показал, что мошенничество в мессенджере Telegram представляет собой серьезную и постоянно развивающуюся угрозу, использующую как технические особенности платформы, так и психологические уязвимости пользователей через методы социальной инженерии. Стремительный рост числа зафиксированных случаев и появление новых, более изощренных схем подтверждают актуальность проблемы и её значимость для финансовой безопасности граждан, особенно молодежи.