ГУ МВД РОССИИ ПО СВЕРДЛОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО СОЦИАЛЬНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ
ГКУ СОН СО «ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ ЦЕНТР
СОЦИАЛЬНОЙ ПОМОЩИ»

Профилактика мошеннических действий для организаций социальной политики Свердловской области, оказывающих социальные услуги

Методические рекомендации

2023

ГКУ СОН СО «Организационно-методический центр социальной помощи»

Профилактика мошеннических действий для организаций социального обслуживания Свердловской области / методические рекомендации – Екатеринбург. – 2023. – 37 с.

Методические рекомендации предназначены руководителям и сотрудникам организаций социального обслуживания для использования в практической деятельности, а также получателям социальных услуг.

В методических рекомендациях обобщены и систематизированы сведения о видах и способах мошеннических действий в отношении граждан. По каждому из них даны методы предотвращения и способы реагирования. Приведены примеры расследования правоохранительными органами Свердловской области и привлечения к ответственности злоумышленников. Доведение информации и контроль за исполнением правил профилактики поможет избежать подобных случаев в отношении как сотрудников, так и клиентов системы социальной защиты.

Редакторы-составители: методисты ГКУ СОН СО «Организационно-методический центр социальной помощи» И.А. Киселев, И.П. Ризничок.

СОДЕРЖАНИЕ

Введение

В последние годы в России наблюдается устойчивая тенденция роста преступлений, совершаемых путем мошеннических действий. Однако, если ранее преобладало мошенничество, выражавшееся в обмане о потребительских свойствах товара, доставке товаров, производстве работ, то теперь получило распространение мошенничество, осуществляемое с использованием мобильной связи и сети Интернет, или иначе, с использованием современных информационно-телекоммуникационных технологий.

Число мошенничеств, совершенных дистанционно за восемь месяцев 2023 года, выросло на 40% в сравнении с аналогичным периодом прошлого года. Об этом сообщили в пресс-службе Генпрокуратуры России, отвечая на запрос ТАСС. Всего совершено 226,8 тыс. таких преступлений. Дистанционно совершается 80% всех регистрируемых в стране случаев мошенничеств.

Ущерб от действий телефонных мошенников, нанесенный жителям Свердловской области, составил 1 млрд рублей с начала 2023 года, что на 400 млн рублей больше, чем за аналогичный период прошлого года. Количество преступлений выросло на 20% (прирост 2 200 преступлений). В настоящий момент с начала года у нас в области зафиксировано 9 700 указанного вида преступлений - кражи денег с банковских карт и хищений денег с использованием мошеннических схем.

Глава 1 Общие сведения о мошенничествах

Мошенничество — это уголовное преступление, когда жертва отдает преступнику имущество или деньги. Обычно — добровольно, из-за обмана. Аферисты обманывают и при личном контакте, и дистанционно. УК РФ Статья 159 Уголовного кодекса Российской Федерации дает такую официальную формулировку: «Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

Жертвой мошенников может стать кто угодно, и государственные служащие, и сотрудники учреждений, и клиенты пожилого возраста, и дети. Но самые уязвимые — пожилые люди. Им не хватает общения, они не всегда владеют современными технологиями и не могут сразу попросить о помощи. А еще они доверчивы и открыты к посторонним — этим мошенники и пользуются. Умудренные жизнью, но неожиданно уязвимые, если уделить им внимание и пообещать легкой жизни. Мошенники пользуются этой особенностью и иногда пытаются отнять единственное, что есть у пожилых – их дом.

Распознать, что перед вами - не чистый на руку человек, несложно: «Основные приемы, которые используют мошенники: запугивание, напор, нереальные обещания «всего и сразу» и решение надо принять немедленно». Могут прикрываться авторитетом вышестоящих руководителей.

Кроме того, к подозрительным признакам следует отнести и излишнюю необоснованную заботу с порой преувеличенным сочувствием. В иных случаях пожилого человека могут начать запугивать: «страх парализует волю и отключает критическое мышление, а умелые манипуляторы используют это в своих корыстных целях».

Обработка при этом очень энергичная: человека ни на минуту не оставляют без внимания и участвуют в его жизни почти постоянно. Часто при мошенничестве с пожилыми людьми участвуют несколько человек.

Еще один признак – нереальные обещания: пятизвездочные пансионаты с элитными шеф-поварами и геронтологическими спа-процедурами крайне редки. А значит, рассчитывать, что старика в обмен на квартиру переселят в такие роскошества – наивно.

Сюда же следует отнести предложения, связанные с подписанием «чисто формальных» бумаг: маскироваться под них может и дарственная. Аргументировать мошенники умеют: обычно они наступают на больные мозоли – маленькие пенсии, плохое здоровье и отсутствие внимания со стороны тех, от кого его хотелось бы получать побольше (тут можно иметь ввиду как родственников, так и, например, участкового терапевта).

Серьезным поводом задуматься должна стать и срочность принятия решения: мошенникам важно не дать успеть опомниться или посоветоваться с близкими. Так что повод заподозрить неладное - наличие в лексиконе новых друзей таких слов как «срочно», «немедленно», «только сейчас», «последний день».

Глава 2 Как мошенники обманывают пенсионеров

При личном контакте. Такие преступники подстерегают в торговых центрах и уговаривают бесплатно обследоваться, а потом навязывают дорогое лечение. Или ходят по квартирам и предлагают отрегулировать окна, вывести тараканов, улучшить карму и купить чудодейственный аппарат для снижения давления. При этом деньги пенсионер отдает наличными. Уголовный кодекс называет такое мошенничество классическим.

Классические аферисты очень убедительны: носят поддельные бумаги с гербовыми печатями, документы и удостоверения. А иногда и договоры на оказание услуг с несуществующими организациями. Они никогда не повышают голос, относятся с уважением, готовы к долгой и обстоятельной беседе. А еще они всегда знают, в чем проблема, и готовы помочь. Таким сложно не поверить.

Дистанционные мошенники используют для махинаций телефон, интернет, страницы в соцсетях и недобросовестную рекламу. А деньги получают на электронные кошельки и банковские карты, оформленные на подставных лиц. Особые шпионские программы им не нужны: это дорого и сложно, а пенсионеры и сами сообщают данные для перевода денег.

Чаще всего пенсионеров обманывают с помощью электронных платежей или используют их персональные данные.

Мошенничество с электронными платежами — это когда пенсионер теряет деньги через банковские карты, виртуальные кошельки. Например, если ему звонят якобы из банка, спрашивают данные карты и воруют деньги со счета.

Мошенничество с персональными данными — это когда их похищают или изменяют, чтобы получить права на имущество. Например, оформляют за пенсионера электронную подпись и сами подписывают договор купли-продажи его квартиры.

Что делать: пенсионер может подать в Росреестр или через МФЦ заявление о невозможности государственной регистрации перехода, прекращения, ограничения права и обременения объекта недвижимости без его личного участия.

Глава 3 Самые распространенные схемы мошенничества

По сотовому телефону через СМС

Примеры сообщений.

- «Вам по ошибке перечислили деньги — верните их через смс-банк».
- «Вы выиграли в лотерею — следуйте инструкциям и получите выигрыш».
- «Вам положена компенсация. Чтобы ее получить, отправьте СМС-сообщение…».
- «Ваша карта заблокирована, для разблокировки отправьте в ответ…».

Аферисты регистрируют на номер телефона человека множество аккаунтов на сайтах разных интернет-магазинов, онлайн-сервисов, банков, маркетплейсов и т.д. И сайты начинают засыпать владельца номера СМС-сообщениями, устраивают СМС-атаки. Среди этих сообщений скрывается код, который служит аналогом подписи под договором на получение онлайн-займа. Чтобы им завладеть и разработана такая схема.

Среди потока сообщений владелец номера может даже не заметить, что одно из них — от микрофинансовой организации. Пока СМС-сообщения продолжают приходить, аферисты связываются с человеком в соцсетях или мессенджерах, пытаются втереться в доверие и выманить данные. Например, обманщик может представиться сотрудником оператора связи, предупредить о техническом сбое и попросить прислать скриншоты сообщений. По его словам, они нужны, чтобы разобраться в проблеме — от каких отправителей идет спам.

Что нужно мошенникам. Чтобы пенсионер отправил деньги, коды регистрации или данные карты через смс.

Что не нужно делать. Блокировать родственнику входящие смс, отключать исходящие и мобильный банк. Опасны не сами смс, а то, что пожилой человек переведет аферистам деньги. К тому же в смс бывает что-то полезное: акции из супермаркетов, напоминания о записи к врачу, уведомления о зачислении пенсии и списаниях по карте.

Что делать. Когда пенсионер оформляет в банке карту, можно пойти с ним и привязать ее к отдельному номеру телефона. Перед этим придется купить сим-карту. Можно настроить смартфон так, чтобы он принимал смс на обе карты, а отвечать можно было с одной — не привязанной к счету.

А можно купить для нее отдельный телефон. Пенсионер не будет проверять его постоянно, а у кодов подтверждения короткий срок действия. Для оплаты онлайн в интернете завести отдельную карту и пополнять её только для совершения покупок. Таким образом на «засвеченной» карте не будет находиться много средств. И даже при утечке данных потери будут минимальные.

Пример из практики. Бабушка 76 лет получила смс от банка: «Код для регистрации в онлайн-банке — 7735». Следом пришла смс с незнакомого номера: «Извините, ошибся в одной цифре, и мой пароль пришел вам. Перешлите его, пожалуйста». Бабушка хотела помочь незнакомцу, но дома была внучка и отговорила ее. А если бы карта была привязана к номеру, где невозможно отправить смс, бабушка бы и без внучки не попалась на уловку.

По телефону

Что говорят.

- Мама/папа/бабушка/дедушка, я попал в беду! Нужны деньги на взятку / лечение / компенсацию пострадавшему.
- Это служба безопасности банка, по вашей карте обнаружена подозрительная активность, давайте отменим операцию. Продиктуйте номер карты, срок действия и пин-код.
- Мы из полиции: ваш внук кого-то сбил, нужна взятка пострадавшему.
- Вам положены компенсации, выплаты, надбавки и перечисления из бюджета. Нужно только комиссию оплатить.
- Это из поликлиники. У вас плохой диагноз — нужны лекарства и волшебные медицинские приборы, сейчас мы их доставим.
- Поучаствуйте в беспроигрышной лотерее.

Что нужно мошенникам. Данные карты для перевода денег: номер, срок действия и CVV — трехзначный код на обратной стороне карты. Пенсионеры диктуют всю информацию голосом.

Что не нужно делать. Совсем отказываться от банковских карт. Деньги в банке защищены лучше, чем наличные под матрасом. Те вообще невозможно контролировать.

Что делать. Не говорите и не вводите ПИН-код, трехзначный код с обратной стороны карты, или одноразовый пароль из СМС. Не набирайте на телефоне никаких комбинаций и не переходите по ссылкам. Не называйте кодовое слово. Набирайте номер вручную, Телефон горячей линии банка указан на обратной стороне карты и на официальном сайте банка. Сотрите с обратной стороны карты трехзначный код. Для этого подойдет даже кухонный нож. Картой можно будет платить в магазинах, снимать с нее деньги и пополнять счет. Но без кода пожилой человек не переведет аферистам деньги, ничего не купит в сомнительном телемагазине и не сделает ставку в онлайн-лотерее. Для этого придется позвонить вам и спросить код. А вы как раз и спросите, зачем он нужен.

Некоторые мошенники звонят и убеждают принести деньги наличными. Лучше отказаться от наличных в повседневной жизни, а снятие с карты ограничить несколькими тысячами рублей. Это можно сделать в мобильном приложении или в отделении банка, если прийти туда с родственником. Когда пенсионер не сможет снять большую сумму, он запаникует и позвонит вам.

Задайте собеседнику вопрос, ответ н который может знать только близкий вам человек. Прервите разговор и перезвоните родным, чтобы убедиться, что с ними все в порядке. Если собеседник представляется работником правоохранительных органов, попросите его назвать фамилию, имя, отчество, а также должность и место службы. Позвоните в соответствующее ведомство и узнайте, действительно ли в нем работает такой сотрудник. Помните, что передача денежных средств должностным лицам за незаконные действия или бездействие является уголовно наказуемым деянием.

Пример из практики. Дедушке 74 лет позвонили и сказали, что его сын сбил человека. Пострадавший якобы в порядке, но за молчание просит 20 000 Р.

Дедушка побежал к банкомату, но тот не работал. Тогда он позвонил внучке и спросил, где еще есть банкомат, — она и распознала развод. Если бы банкомат работал, дедушка лишился бы денег. Еще помогает ограничение на снятие крупных сумм.

В квартирах

Что говорят.

- Мы из собеса, тут вам компенсация положена.
- Мы из газовой службы, нужно срочно счетчик поменять или установить датчик утечки газа, почистить за деньги вентиляционные каналы.
- Мы из оконной фирмы, давайте окна отрегулируем.
- В доме тараканы и клопы, требуется санобработка.
- Для пенсионеров у нас техника/лекарства/посуда со скидкой.
- Частный «честный» мастер по ремонту бытовой и компьютерной техники.
- Вам положено бесплатное медицинское обследование на дому.
- Подпишите петицию за справедливость. Надпись «кредитный договор» — это просто форма такая.
- Распространение листовок и квитанций с информацией о том, что подошел срок проверки и замены счетчиков.

Что нужно мошенникам. Вынудить подписать кредитный договор, впарить втридорога бесполезный товар или обманом выманить наличные.

Что делать. Для начала — осложнить мошенникам поиск жертвы. Они не обходят все квартиры в доме, а заранее выясняют, где живет пенсионер. Чтобы никто не догадался, что в квартире живет ваша бабушка, приведите в порядок ее почтовый ящик и входную дверь, убедите переводить пенсию на карту и уберите лишнее с ее балкона. Еще можно приклеить на дверь наклейку, что объект охраняется. Установите видеонаблюдение в подъезде с помощью ТСЖ или управляющей компании. Не пускайте никаких посторонних в квартиры. Обо всех проверках спрашивайте по телефону в ТСЖ, в Управляющей компании или газовой службе. При официальных проверках ответственные сотрудники обязательно вывешивают объявления со сроками и номерами телефонов. В квартире в коридоре на видном месте разместите телефоны коммунальных, медицинских служб, органов защиты прав потребителей, полиции.

В старых домах почтовые ящики часто без замков, и из них легко достать содержимое. Из платежных извещений аферисты узнают данные пенсионера, а потом называют его по имени и отчеству. Там же смотрят, сколько в квартире прописано человек: если один, то, возможно, это одинокий дедушка. Еще в документах бывает информация о льготах.

Выход — установить замок на почтовый ящик и следить, чтобы там не скапливалась корреспонденция.

Еще два признака, что в квартире живет пожилой человек, — хлам на балконе и обшарпанная дверь. Убедите родных не хранить на балконе старье и не сушить там половики. И поставьте бабушке хотя бы недорогую железную

дверь. Внешне она будет не так уж сильно отличаться от дорогих и навороченных.

Почтальон, который разносит пенсии в определенный день, — тоже знак, что в квартире живет бабушка или дедушка. Причем банковских карт у них нет, зато есть наличные.

У таких почтальонов мошенники тоже часто выуживают информацию. Например, представляются участковыми и спрашивают, кто в подъезде всегда дома и мог быть свидетелем преступления. Почтальоны не только называют таких пенсионеров, но и дают им характеристики.

Лучше отказаться от доставки пенсии наличными и оформить начисление на банковскую карту. Это бесплатно.

В медицинских и торговых центрах

Что говорят.

- Для вас есть заём на выгодных условиях. Внукам не говорите — купите им подарки и сделаете сюрприз.
- В нашем медцентре для вас бесплатная диагностика по госпрограмме. Заболевание у вас тяжелое, а лечение нужно дорогое. Но в соседнем кабинете можно оформить кредит на выгодных условиях.
- Для пенсионеров мы проводим бесплатный курс по торговле на бирже. Сейчас подскажем, какие акции купить, чтобы и вам на безбедную старость хватило, и внукам на подарки.
- Только два дня распродажа элитных натуральных кожаных курток и меховых изделий с зазывалами через звукоусилитель и нарядными воздушными шариками. При проверке либо завышенная в разы цена, либо искусственный залежалый товар.

Что нужно мошенникам. Вынудить подписать кабальный договор купли-продажи, кредитный договор или развести на большие траты.

Что делать. От такого мошенничества труднее всего защитить родных. Фирмы аферистов часто официально зарегистрированы и даже платят налоги. Почти всегда они подписывают с пенсионером договор, а с ним нет оснований для возбуждения уголовного дела. При наличии договора полиция отправляет человека в суд. Привлечь виновных к ответственности и вернуть деньги почти невозможно. Наоборот, если пенсионер не платит по кредиту, мошенник может подать на него в суд.

Гарантированных способов борьбы с этим пока нет. Пожилым людям можно порекомендовать ходить за покупками в торговые центры не в одиночку, а брать с собой знакомых или родственников. Можно ограничить пенсионеру доступ к паспорту — без него невозможно заключать договоры. Изымать паспорт необязательно — он может быть в квартире бабушки, но в сейфе, код от которого знаете только вы.

Пример из практики. В торговом центре женщине предложили полежать на ортопедическом чудо-матрасе. Он стоил 30 000 Р, и ее убедили купить его в кредит. Оказалось, ставка — 10% ежемесячно.

Женщина уже год ходит по судам, чтобы расторгнуть кабальный договор. Если бы у нее не было с собой паспорта, она бы не оформила кредит. Паспортные данные пенсионеры редко помнят.

Финансовая пирамида

Это мошеннический проект, который имитирует выгодные инвестиции. Вас призывают вложить деньги в фиктивный бизнес и агитируют приводить друзей и родственников. В результате можно потерять не только деньги, но и доверие своих близких.

Какими бывают финансовые пирамиды? Пирамиды могут маскироваться под любые компании: кредитные потребительские кооперативы, микрофинансовые организации и просто интернет-проекты.

Фантазия обманщиков безгранична. Они предлагают вложиться в сельское хозяйство или криптовалюты, открыть бизнес по франшизе.

Ключевое отличие от реального бизнеса – организаторы ничего не производят и ни во что не инвестируют деньги вкладчиков. Мошенники просто собирают их в свой карман.

Признаки финансовой пирамиды.

Обещают высокий доход. Если Вам «гарантируют» десятки или даже сотни процентов в год без всякого риска, это точно аферисты.

Вас просят приводить новых клиентов. И обещают начислить процент от их взноса. Так преступники пытаются побыстрее вовлечь как можно больше людей в свою аферу, собрать с них деньги и скрыться.

Нет подтверждения инвестиций. Вам показывают только красивые презентации и не дают взглянуть на финансовые документы, бухгалтерскую отчетность. Деньги просят перевести на чей-либо персональный счет либо электронный кошелек или же внести наличными, при этом не выдают никаких чеков.

Как не столкнуться с пирамидой.

Найдите компанию в реестрах Банка России. Доверяйте деньги только легальным финансовым организациям. Их можно найти на сайте Банка России cbr.ru в разделе «Проверить участника финансового рынка» (cbr.ru/fmp_check/).

Посмотрите в госреестре юридических лиц (ЕГРЮЛ). На сайте Федеральной налоговой службы ww.nalog.gov.ru в разделе «Риски бизнеса: проверь себя и контрагента» изучите информацию о компании. Узнайте, кто учредители и владельцы. Выясните дату создания и основной вид ее деятельности. Если компания зарегистрирована как пекарня, а предлагает инвестиции в криптовалюту, на дрожжах будет расти только доход ее создателей, а Вы потеряете деньги.

В первую очередь сверьте полное название и реквизиты с данными на сайте Банка России и ФНС. Изучите, какие обязательства берет на себя компания и что будет, если она их не исполнит.

Почитайте отзывы в интернете. Много однотипных хвалебных откликов должны скорее насторожить – вероятнее всего, они фальшивые.

Что делать.

Если пирамида еще действует, составьте письменную претензию и потребуйте вернуть деньги. Сообщите, что иначе обратитесь в полицию.

Соберите документы: договор, выписку по банковскому счету, с которого перевели деньги в пирамиду, или приходный кассовый ордер, если отдали наличные. Со всеми бумагами обратитесь в полицию и прокуратуру.

Постарайтесь найти других пострадавших. Вместе обратитесь к проверенному адвокату и подайте коллективный иск в суд.

Предупредите других людей, которые тоже могут попасться на удочку мошенников. Расскажите о своем опыте в соцсетях, напишите в СМИ, сообщите в Банк России. Чем больше огласка – тем меньше денег смогут украсть преступники.

Можно вернуть деньги, если пирамида рухнула. Но при условии, что пирамид попала в реестр Федерального фонда по защите прав вкладчиков и акционеров. Только он выплачивает компенсации обманутым клиентам некоторых компаний. На сайте Фонда fedfond.ru можно посмотреть список пирамид, по которым идут выплаты.

Оформить самозапрет на кредитование — это ограничение, которое банк накладывает на онлайн-операции по заявлению клиента. Запретить можно как отдельно кредитование, так и другие банковские операции или ограничить их отдельные параметры — например, установить максимальную сумму для одного перевода или нескольких переводов, но на определенный период времени. Такая услуга призвана ограничить возможности оформления кредитов или выполнение операций с денежными средствами клиента без его ведома. Если вы хотите оформить именно самозапрет на кредитование или переводы, это можно сделать непосредственно в банке. Конечно, потребуется время, чтобы обратиться во все кредитные организации, но для начала можно подать заявления в банки, услугами которых вы когда-либо пользовались.

Госдума 10 октября 2023 года приняла в первом чтении законопроект о праве гражданина установить в своей кредитной истории запрет на заключение с ним кредитными и микрофинансовыми организациями (МФО) договоров потребительского займа (кредита). Вводится особый механизм защиты от мошенников. И когда его примут, граждане смогут оформить самозапрет на выдачу кредитов. Тогда никто не сможет ни получить кредит за спиной гражданина, ни сбить его с толку и заставить взять деньги, чтобы тут же с ними расстаться.

Это такой механизм защиты, который не позволит мошенникам «вешать» какие-либо долги на граждан. Ограничение будет накладываться на онлайн-операции по заявлению клиента, и человек сможет сам решить, вводить его или нет. Для установки запрета нужно поставить специальную отметку в бюро кредитных историй через банк или МФО и в будущем - через единый портал госуслуг и МФЦ. Снять или вновь ввести его можно будет бесплатно и множество раз.

Для установления (снятия) запрета гражданин сможет бесплатно подать во все квалифицированные бюро кредитных историй соответствующее заявление, а также

запросить информацию о наличии в его кредитной истории сведений о запрете (снятии запрета).

Глава 4 Рекомендации сотрудников полиции

Сотрудники полиции предлагают несколько простых советов, как не стать жертвой мошенников.

- Остерегайтесь открывать двери незнакомым людям.
- Ни в коем случае не пускайте в дом посторонних лиц. Если они выдают себя за работников социальных служб или других учреждений спросите фамилию и телефон этой службы. Позвоните туда и убедитесь в достоверности. Если за дверью мошенник, он не станет дожидаться выяснения Вами ситуации.
- Если же Вы открыли дверь, не впускайте незнакомца в квартиру или дом, разговаривайте на пороге.
- Никому не сообщайте свои персональные данные.
- Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения.
- Не следует отдавать документы (паспорт, пенсионное, ветеранское удостоверения и т. д.).
- Не оставляйте незнакомца одного в комнате.
- Не покупайте никакие приборы, медикаменты или БАДы на дому, через курьера, либо с рук, ничего хорошего не приобретете.
- Ни в коем случае не вступайте в контакт с незнакомыми людьми, которые навязывают Вам любые услуги, в том числе и по телефону.
- Не доверяйте свои деньги и ценности гадалкам и ясновидящим, встретившим вас на улице или явившимся к вам в дом.
- Не поддавайтесь предложениям обменять деньги. Никакие операции с деньгами на дому не проводятся, а разного рода доплаты к социальным выплатам поступают гражданам привычным путем - на счет в банке или их приносит почтальон.
- Не обращайте внимание на СМС-сообщения о выигрыше и просьбой отправить определенную сумму денег на незнакомый счет или номер;
- Если вам позвонили по телефону и сообщили о том, что Ваш родственник попал в ДТП или другую беду и для этого необходима определенная сумма денег, обязательно проверьте эту информацию, свяжитесь со своими родными;
- Не верьте людям, предлагающим оформить путевку в санаторий со скидкой и требующих предоплаты.
- Если неизвестный звонит гражданину, представляясь сотрудником банка, государственных структур, сотрудником сотовой компании немедленно прекратить разговор и самостоятельно позвонить в банк, государственный орган или сотовую компанию;
- В случае, если к гражданину пришли неизвестные и предлагают «обмен купюр» или «получение доплат к пенсии» не открывать двери. Если неизвестные проникли в квартиру или дом не передавать денежные средства, сообщить о случившемся в полицию.
- Избегать общения с теми, кто предлагает купить дешевые товары или продукты питания, погадать или снять порчу.

- Обо всех фактах попыток мошеннических действий сообщайте в дежурную часть вашего территориального ОВД по номерам **02** для стационарных телефонов, **102** для сотовых телефонов или в единую службу спасения **112**. Телефон дежурной части ГУ МВД России по Свердловской области **8-343-358-83-38**.

Сотрудники полиции также обращаются к сотрудникам организаций социального обслуживания, оказывающих социальные услуги гражданам пожилого возраста:

- При посещении граждан организовать вручение информационных памяток профилактического характера каждому под роспись.
- Организовать проведение лекций/семинаров по данной тематике.
- К родным и близким пенсионеров: доведите эти рекомендации до своих пожилых родителей и других родственников, чтобы оградить их от перечисленных неприятностей. Причем делать это нужно постоянно, с периодичностью не менее раза в месяц.
- К соседям ветеранов и жителям района: при появлении на улицах, во дворах жилых домов незнакомых подозрительных автомашин, женщин и мужчин, незамедлительно сообщите об этом в полицию.

Глава 5 Схемы обмана от имени Социального фонда России

Сетевое мошенничество

В Интернете появился ряд сайтов, где предлагается при помощи номера СНИЛС или паспортных данных проверить наличие денежных выплат со стороны частных страховых фондов.

Некий Внебюджетный финансовый фонд развития призывает граждан: «Проверьте Ваш СНИЛС на наличие денежных выплат со стороны частных страховых фондов за 3 минуты!». Фонд сообщает, что от граждан якобы скрываются субсидии на выплаты, которые положены всем россиянам и обещает довольно большие суммы.

На первом этапе гражданин вводит номер СНИЛС или паспортные данные, после чего сайт показывает якобы положенные к выплате суммы. В большинстве случаев это порядка 100 тысяч рублей. На втором этапе гражданину предлагается оплатить доступ к базам данных частных страховщиков, за что мошенники обещают моментальный перевод средств на счет клиента. Предположительно, именно после перевода злоумышленники и пропадают.

Сайт снабжён лестными отзывами людей, которые якобы уже получили реальные деньги. При этом отметим, что даже при вводе вымышленных данных всё равно выдается положительный результат.

Специалисты СФР отмечают, что на индивидуальном лицевом счете гражданина хранятся не деньги, а сведения о сформированных пенсионных правах. Эта информация является конфиденциальной. Нам неизвестно, в каких целях собираются персональные данные граждан, поэтому необходимо игнорировать подобные сайты и бережно относиться к своим персональным данным. Доверять информации о положенных пенсионных выплатах можно на официальном сайте Социального фонда России.

Мобильное мошенничество, афёры с банковскими картами

Еще один вид мошенничества в отношении людей пожилого возраста – по средствам телефонной связи. Когда некие люди, представляясь сотрудниками СФР, входят в доверие к пенсионерам и оставляют их без последних средств к существованию.

Мошенники звонят по телефону и сообщают о якобы возникших проблемах при перечислении пенсий или социальных выплат. Для скорейшего их решения пенсионерам предлагают подойти к ближайшему банкомату и произвести ряд манипуляций с банковской картой. Доверчивые граждане выполняют продиктованные злоумышленником действия, а спустя некоторое время все деньги с банковской карты «исчезают».

Мошенники могут действовать под видом сотрудников СФР

Неизвестные ходят по домам или предприятиям, представляясь сотрудниками Социального фонда, просят показать личные документы – паспорт и СНИЛС. Неизвестные используют двусмысленные формулировки и выражения и применяют иные приемы и средства, чтобы войти в доверие. Когда им удаётся

ввести человека в заблуждение, они сообщают о том, что надо срочно заключить договор с одним из негосударственных пенсионных фондов.

Специалисты СФР не запрашивают по телефону персональные данные, не уполномочены посещать граждан, а также оказывать государственные услуги на дому. Получение услуг проходит только в клиентской службе или через «Личный кабинет гражданина» на сайте СФР.

Специалисты рекомендуют, если к вам обращается якобы сотрудник СФР, обязательно попросите его предъявить служебное удостоверение.

Сценарии аферисты применяют разные: звонят по телефону, отправляют СМС-сообщения, действуют под видом сотрудников социальных или коммунальных служб, пенсионных фондов, продавцов. Будьте бдительными и осторожными! Не сообщайте посторонним людям номер вашей банковской карты и код, паспортные данные, номер СНИЛС и не подписывайте в спешке какие-либо документы.

Глава 6 Мошенничество в социальных сетях и мессенджерах

Кража пользовательских аккаунтов в мессенджерах — явление не новое. По данным «Лаборатории Касперского», с конца 2022 года широкое распространение схемы с «голосованием» пришлось на пользователей WhatsApp, Telegram,Viber и других систем. Что именно является целью мошенников, использующих такой вид фишинговой атаки?

Целью злоумышленников в таких случаях является кража конфиденциальных данных. Перейдя по ссылке, которая ведет на фишинговый сайт, пользователь теряет доступ к аккаунту. Завладев учетной записью, мошенники смогут не только рассылать сообщения уже от лица жертвы взлома, но и видеть переписки, вложения и другую информацию, что в некоторых случаях может обернуться шантажом, потерей денежных средств и вымогательством.

Доступ к аккаунту мессенджера дает мошеннику больше возможностей, чем может показаться на первый взгляд. На многих ресурсах в качестве двухфакторной аутентификации абонента может использоваться и аккаунт в мессенджере, и тогда преступник без проблем проникнет и в другие учетные записи человека. А используя возможность писать с вашего аккаунта вашим близким и играть на их чувствах, похищать деньги.

Например, вашему другу может прийти сообщение «Привет, я попал в ДТП. Помоги, пожалуйста, отправь мне 5000 рублей на карту по этому номеру…» К сожалению, из-за чувства страха за близких мы порой теряем бдительность, что может привести к печальным последствиям. Защитить свой аккаунт в мессенджере от взлома несложно, важно просто следовать нескольким правилам.

— Сохраняйте бдительность независимо от того, знакомы вы с человеком, от которого получили сообщение со ссылкой, или нет. Самый верный способ проверить надежность такого собеседника — связаться с отправителем через другие каналы связи. Не забывайте также об использовании двухфакторной аутентификации для всех аккаунтов, где это возможно, и не пренебрегайте использованием защитных решений, которые не дадут перейти на фишинговый сайт.

Зачастую причиной появления таких ситуаций являются действия самого пользователя. Невнимательность в Сети играет с нами злую шутку.

Каждый раз людей берут на простейших вещах. Я не верю в схему «я ничего не делал, а мой телефон взломали». Вы сами перешли по ссылке, вирус у вас распаковался и заработал. Не нужно переходить, если вы не понимаете адресата и всего остального. А в адресе такой ссылки мы видим название ресурса, и, если ресурс нам не знаком, мы не переходим. И нужно задаваться вопросом своей информационной безопасности. Сам WhatsApp регулярно выпускает в разделе сторис инструкции по безопасности. Как пометить, жалобу отправить, как заблокировать пользователя, как не переходить по непонятным ссылкам и прочее. Наша безопасность — наша ответственность.

Глава 7 Мошенничество через WhatsApp: новые схемы и советы для защиты

WhatsApp – одно из самых популярных мессенджеров в мире, и это делает его привлекательной целью для мошенников. Они постоянно разрабатывают новые схемы, чтобы обмануть пользователей и получить доступ к их личным данным или деньгам.

Схема фишинга

Одна из самых распространенных схем мошенничества через WhatsApp – это фишинг. Мошенники отправляют пользователю сообщение, в котором предлагают перейти по внешней ссылке. При переходе по этой ссылке пользователь попадает на поддельный сайт, похожий на страницу авторизации WhatsApp. При вводе своих учетных данных на этой странице мошенники получают доступ к аккаунту пользователя. Схема обмана выглядит следующим образом. Ничего не подозревающие пользователи мессенджера получают от знакомых одно и то же сообщение: «Привет! Прошу прощения, что отвлекаю. Можешь тут за Лену проголосовать, пожалуйста? Это моя племянница. У них в балетной школе конкурс проходит, путевка в детский лагерь на кону. Немного голосов не хватает до победы». И ниже — подозрительная ссылка на сайт с «голосованием». Перейдя по ней, человек дает преступнику доступ к своей учетной записи.

Сначала у пользователя действительно высвечивается какое-то голосование, но затем сразу же происходит переход на новый ресурс с непонятным содержанием. И даже если закрыть эту страницу, уберечь себя от взлома уже не выйдет. Так мошенник получает в распоряжение целый аккаунт со всеми переписками и возможностью распространять вредоносное сообщение с номера телефона жертвы.

Параллельно на телефон могут приходить десятки SMS, подтверждающие попытки мошенников взломать другие аккаунты, привязанные к мобильному телефону, в том числе системы онлайн-банков и «Госуслуги».

Чтобы защититься от таких схем, всегда будьте осторожны, если вам сообщили о каких-то проблемах со счетом или аккаунтом. Никогда не переходите по ссылкам, которые пришли вам в сообщениях, особенно если они выглядят подозрительно. Лучше вручную откройте приложение WhatsApp и проверьте информацию там.

Схема перехвата аккаунта

Вторая распространенная схема мошенничества через WhatsApp – это перехват аккаунта. Мошенники используют социальную инженерию, чтобы убедить провайдеров услуг связи перевести номер пользователя на другое устройство. После этого они получают доступ к аккаунту и могут отправлять сообщения от имени пользователя.

Чтобы предотвратить перехват аккаунта, установите на свое устройство двухфакторную аутентификацию. Это дополнительный уровень защиты, который требует ввода пин-кода при попытке зарегистрировать аккаунт на новом

устройстве. Также будьте внимательны, если вдруг ваш номер перестал работать в WhatsApp – свяжитесь с вашим провайдером услуг связи, чтобы проверить, не было ли изменений.

Схема вымогательства

Третья схема мошенничества через WhatsApp – это вымогательство. Мошенники представляются сотрудниками службы поддержки WhatsApp или правоохранительных органов и угрожают, что у вас возникли проблемы или вы будете арестованы, если не предоставите им определенную сумму денег.

Важно помнить, что сотрудники WhatsApp или правоохранительные органы никогда не будут просить деньги или личные данные через WhatsApp. Если вы получаете подобное сообщение, не паникуйте и никогда не отправляйте деньги мошенникам. Свяжитесь с местными правоохранительными органами и предоставьте им информацию о случившемся.

Фейковые аккаунты

Один из распространенных способов мошенничества через WhatsApp – использование фейковых аккаунтов.

Мошенники создают аккаунты, которые выглядят так же, как настоящие аккаунты пользователей WhatsApp. Они могут использовать поддельные имена и фотографии, чтобы сделать свои аккаунты максимально правдоподобными. Для этого мошенники копируют фотографию и имитируют название и биографию настоящего аккаунта. Они также могут добавить вас в группу, сочинить историю или придумать срочный запрос помощи, чтобы получить доступ к вашим личным данным или деньгам.

С помощью фейковых аккаунтов мошенники могут отправлять сообщения с просьбой о переводе денежных средств или предложением участвовать в мошеннических схемах. Они могут писать от имени знакомых или даже сотрудников организаций, чтобы создать впечатление, что сообщение приходит от надежного источника.

Мошенники могут подменять аккаунты друзей или родственников, чтобы получить финансовую помощь. Они также могут требовать переводы денег на предполагаемые счета или просят предоставить личную информацию, которую они после используют для своих злонамеренных целей.

Чтобы предостеречь себя от фейковых аккаунтов, следуйте следующим рекомендациям:

- Остерегайтесь аккаунтов с подозрительно выглядящими именами или фотографиями профиля. Если что-то кажется слишком хорошим, чтобы быть правдой, скорее всего, это злоумышленники. Перед тем, как делиться личной информацией или осуществлять финансовые операции, всегда проверяйте аккаунт тщательно. Сравните фотографии, имена, номера телефонов и биографии. Если что-то выглядит подозрительно, свяжитесь с этим человеком другим способом для подтверждения отправителя (звонок, личная встреча).
- Найдите официальный веб-сайт или официальные профили в социальных сетях, связанные с человеком или организацией, с которыми вы общаетесь в

WhatsApp. Проверьте, есть ли там какая-либо информация о передаваемой вам информации, и сравните ее с тем, что вы получили через мессенджер.

- Остерегайтесь срочных запросов: Будьте осторожны, если вам приходит срочный запрос помощи или требование перевода денег от вашего друга или родственника через WhatsApp. Проверьте информацию через другие каналы связи и уточните ситуацию, прежде чем предпринимать какие-либо действия.
- Не делитесь личной информацией: Никогда не отправляйте свои личные данные, такие как паспортные данные, номера кредитных карт или адреса проживания, через WhatsApp. Мошенники могут использовать эту информацию в своих злонамеренных целях.
- Не открывайте ссылки или прикрепленные файлы, отправленные сомнительными аккаунтами. Они могут содержать вредоносное ПО или привести к фишинговым сайтам.
- Проверяйте правильность написания номера телефона или адреса электронной почты аккаунта, прежде чем принимать важные решения или делать денежные переводы. Будьте внимательны к подробностям – грамматическим или орфографическим ошибкам, странным ссылкам или предложениям, требующим вашего личного или финансового участия.
- Если у вас есть подозрения по поводу определенного аккаунта, не стесняйтесь сообщать об этом службе поддержки WhatsApp или другим соответствующим организациям.
- Чтобы усилить безопасность вашего аккаунта WhatsApp, установите двухфакторную аутентификацию. Это добавит дополнительный уровень защиты и предотвратит несанкционированный доступ к вашему аккаунту.

Соблюдение этих мер предосторожности поможет вам защититься от мошенничества, связанного с подделкой идентичных аккаунтов в WhatsApp. Помните, что мошенники могут использовать различные методы, чтобы выглядеть достоверно, поэтому всегда оставайтесь бдительными и внимательными.

Сообщения с просьбой о помощи

Мошенники через WhatsApp могут использовать различные сценарии и истории, чтобы развить доверие и убедить вас предоставить им деньги или конфиденциальные данные. Один из распространенных способов мошенничества — это отправка сообщений с просьбой о помощи.

Мошенники могут притворяться вашим другом, родственником или знакомым и отправить вам сообщение с просьбой о финансовой помощи. Они могут задать ситуацию, в которой им нужны срочные деньги для оплаты медицинских счетов, спасения из тюрьмы или другой срочной проблемы. Часто они предлагают отправить деньги через мобильные платежи или переводы на банковские карты.

Оказавшись в такой ситуации, не спешите отсылать деньги незнакомому человеку или проверьте информацию, предоставленную в сообщении. Важно подтвердить подлинность просьбы о помощи и убедиться, что фактический отправитель — это ваш знакомый или родственник.

Для этого, откройте приложение WhatsApp и свяжитесь с предполагаемым отправителем за пределами чата, используя уже известный вам номер или средства связи, которые вы нормально использовали для коммуникации. Задайте вопросы, которые только настоящий отправитель мог бы знать, чтобы убедиться, что человек, который просит вас о помощи, действительно тот, для кого себя выдает.

Также мошенники могут использовать случаи экстренных ситуаций, таких как землетрясения, природные катастрофы или чрезвычайные происшествия, чтобы попросить вас пожертвовать деньги на благотворительность через мобильные платежи или посторонние сайты. В таких ситуациях всегда проверяйте правдивость информации и пожертвования через официальные и проверенные каналы.

Помните, что ваше финансовое благополучие и конфиденциальность должны быть важнее, чем срочная просьба о помощи. В случае сомнений лучше не рисковать и проконсультироваться с другими доверенными лицами перед предоставлением финансовой помощи.

Помните эти меры предосторожности, чтобы защитить себя от мошенничества через WhatsApp.

Подозрительные ситуации

Неизвестный контакт. Если вы получаете сообщение от незнакомого контакта, будьте осторожны и не раскрывайте личную информацию. Проверьте его профиль и действия, прежде чем начинать общение.

Спам и нежелательные сообщения. Если вы получаете чрезмерное количество сообщений от одного или нескольких контактов, содержащих рекламу, промо-коды или предложения, которые кажутся подозрительными, будьте настороже. Не открывайте ссылки или вложения из таких сообщений.

Прошение о финансовой помощи. Если вам поступает сообщение от ваших знакомых или родственников с просьбой о финансовой помощи, тщательно проверьте подлинность сообщения. Мошенники могут использовать информацию о вас или ваших близких, чтобы попросить деньги. В случае сомнений обратитесь к контакту, указанному в вашей адресной книге, и уточните ситуацию.

Лотереи и выигрыши. Если вам сообщают о выигрыше в лотерее или призе, о котором вы не помните, что участвовали, будьте осторожны. Это может быть мошеннической схемой для получения ваших личных данных или денежных средств. Никогда не отправляйте деньги или личные данные по этим запросам.

Предложения о работе. Будьте внимательны к предложениям о работе, которые приходят через WhatsApp. Если предложение кажется слишком хорошим, чтобы быть правдой, вероятнее всего, это мошенничество. Никогда не предоставляйте личные данные или оплачивайте какие-либо услуги без проверки легитимности компании.

Контроль личной информации

Не разглашайте конфиденциальные данные в переписке. Никогда не отправляйте банковские данные, пароли, СНИЛС или другую чувствительную

информацию через WhatsApp или любые другие мессенджеры. Если вы не уверены, с кем взаимодействуете, лучше воздержитесь от передачи какой-либо личной информации.

Ограничьте доступ к вашему профилю WhatsApp. В настройках аккаунта WhatsApp вы можете выбрать, кто может видеть вашу фотографию профиля, статус и информацию о последнем посещении. Ограничьте доступ только к своим контактам или выберите настройку «Никто», чтобы обеспечить максимальную конфиденциальность.

Не доверяйте неизвестным контактам. Будьте осторожны при добавлении новых контактов в WhatsApp. Мошенники могут использовать разные способы, чтобы получить доступ к вашим личным данным. Подозрительные номера телефонов или сообщения с предложениями сомнительных услуг являются признаками потенциальной угрозы.

Будьте внимательны при использовании публичных Wi-Fi сетей. Публичные Wi-Fi сети могут быть небезопасными, и неизвестные лица могут перехватить вашу личную информацию.

Соблюдение этих мер предосторожности поможет вам контролировать свою личную информацию и снизить риск стать жертвой мошенничества через мессенджеры. Оставайтесь бдительными и не стесняйтесь обращаться за помощью к службе поддержки в случае возникновения сомнений или подозрений.

Заманчивое предложение «по ошибке»

Некоторые граждане стали получать странные сообщения в мессенджерах: «Уважаемый Ф. И. О., начисление по вашим инвестициям за месяц…» — далее указывается ставка 15% и приличная сумма, а ниже — подпись «Ваш менеджер» с указанием имени и контактного телефона. При этом на аватарке отправителя фото с респектабельным молодым человеком или девушкой. Кто-то из получателей игнорирует такое послание, но некоторые люди пишут отправителю, мол, вы ошиблись. «Менеджер» в ответ вежливо извиняется и указывает, что да, на самом деле это отправление ошибочно, и даже просит его удалить, так как там содержатся конфиденциальные данные, адресованные другому человеку.

В послании «Уважаемый Ф. И. О…» указывают имя реального человека, который есть в списке контактов того, кому пришло это якобы ошибочное сообщение. Информация о том, каким образом знакомый получает повышенный доход, для многих представляет интерес, и на это очень рассчитывают мошенники. На вопрос, можно ли «ошибочному» адресату тоже разместить деньги под такой высокий процент, злоумышленники реагируют мгновенно. В ответном послании «менеджер», как правило, заявляет, что может управлять финансами только тех, кто подписал официальный договор, но в связи с допущенной им ошибкой по отправке сообщения он может сделать исключение и оформить такой документ онлайн, но нужно быстро прислать свои паспортные данные, а через день приехать в офис и поставить подпись в договоре.

Дальше события развиваются так: присылается некий договор-инструкция, согласно которому человеку предлагается перевести на некую биржу от 30 тысяч рублей. Если деньги отправляются, то по завершении рабочего дня, ровно в 18:30,

присылают сообщение о доходе, но оказывается, что для его получения необходимо перевести в финансовую кампанию 17% либо разместить ранее отправленные средства ещё на месяц под ставку 15% — тогда никакой процент платить не надо. При любом ответе примерно через час вся переписка удаляется — и деньги никто не возвращает.

Предложение лёгкого заработка и ссылки на сомнительные сторонние сайты — первый признак того, что пользователь мессенджера попал под прицел мошенников. Аферисты почти никогда не пользуются официальными формами оплаты. Они просят перевести деньги на карту, на кошелёк ЮMoney или произвести оплату в биткоинах. Как правило, преступники зарегистрированы как интернет-магазины и могут принимать любые расчёты, позволяющие им выводить деньги в тень.

Ложная покупка

Человеку в мессенджере приходит сообщение якобы от службы поддержки пользователей банка, в котором у того есть карта. Лжебанковские сотрудники запрашивают, совершалась ли в течение часа покупка на сумму в несколько тысяч рублей, и указывают конкретную цифру. Вне зависимости от ответа самозванная «служба поддержки» просит проверить данные карты, для чего предлагает заполнить специальную форму. После чего присылается электронная ссылка, при переходе по которой открывается страница, внешне похожая на банковское приложение. После заполнения формы в этом приложении все деньги с карты исчезают.

Код сброса

Приходит сообщение о том, что кто-то пытается получить доступ к вашему устройству и, для того чтобы подтвердить свои права, требуется ввести код из СМС. Объяснения подобным СМС могут быть разные: например, не работает функция сообщений на собственном телефоне и поэтому якобы знакомый просит написать через мессенджер. Доверчивый собеседник отправляет этому якобы знакомому, а на самом деле мошеннику вожделенный код.

После ввода этого кода человек теряет доступ к своему аккаунту в мессенджере. Он уже не сможет войти в собственные учетные данные, поскольку они будут активированы на другом устройстве – мошенническом.

Вместе с кодом авторизации мошенник получает целую телефонную книгу контактов жертвы. А уж там найдется, где разгуляться. И в случае систематического резервного копирования, которое время от времени предлагает приложение, злоумышленник получает все сохраненные переписки. Восстановить доступ мошенники предлагают только после отправки нескольких тысяч рублей в счёт пополнения баланса некоего телефонного абонента. При этом после перечисления денег возврат доступа не гарантирован.

Что делать, чтобы не попасться. Мессенджер использует номер телефона в качестве уникального идентификатора. Последний по умолчанию связан с учетной записью. И если пользователь по какой-то причине решит сменить

устройство или переустановить приложение, WhatsApp должен убедиться, что новый гаджет действительно находится в распоряжении у хозяина аккаунта.

Если код из сообщения будет введен на любом другом устройстве, ученая запись пользователя откроется именно на нем. То есть, сообщать посторонним код от WhatsApp категорически не рекомендуется. Ввиду сложившейся ситуации, разработчики предлагают использовать дополнительную защитную функцию двухфакторной идентификации.

Вам подарок

Присылается сообщение якобы от самого мессенджера, в котором заявляется, что вам на месяц дарится промодоступ к дополнительным премиальным возможностям и, чтобы активировать их, достаточно перейти по короткой ссылке. После перехода по такой ссылке на устройство устанавливается вредоносное программное обеспечение, которое передаёт мошенникам значительный объём данных, включая список контактов, а иногда и информацию о трансакциях и банковских картах.

Схема обмана бюджетников «Звонок от начальника»

В WhatsApp и Telegram работникам здравоохранения, образования либо социальной сферы поступает сообщение от якобы их вышестоящего руководства о том, что к ним поступил запрос из ФСБ о каких-либо компрометирующих операциях, проводимых работниками в банковской сфере. В коммерческие организации приходят сообщения от директора, в которых сообщается, что спецслужбы якобы инициируют проверку банковских счетов. Поэтому «руководитель», «директор» просит сообщить личные данные. После этого потерпевшим поступают звонки якобы от силовиков, которым те доверяются и переводят средства.

Например, в ЦГБ No 14 Екатеринбурга мошенники создали копию страницы главного врача в соцсетях и рассылали бывшим и действующим сотрудникам сообщения. В них говорилось, что медики якобы замешаны в нарушениях антикоррупционного законодательства и обязаны ответить на вопросы силовиков, которые с ними вскоре свяжутся.

До логичного конца схему довести не удалось ни разу, так как потенциальные жертвы проявляли бдительность и проверили информацию.

Глава 8 Рекомендации для защиты от мошенничества

- Будьте осторожны с входящими сообщениями. Никогда не доверяйте сообщениям с подозрительными ссылками или просителями личной информации.
- Проверяйте информацию. Если вам сообщают о проблеме с аккаунтом или счетом, проверьте информацию в самом приложении WhatsApp или обратитесь напрямую в службу поддержки.
- Установите двухфакторную аутентификацию. Это поможет предотвратить перехват вашего аккаунта. Двухфакторная аутентификация — метод защиты учетных записей, требующий наличия двух независимых способов подтверждения легитимности пользователя. Чтобы обезопасить себя от взлома, необходимо использовать для входа в аккаунт два или более факторов, которые должны быть независимыми друг от друга. Это может быть номер телефона, электронная почта, кодовое слово, ответ на секретный вопрос и прочее. Это усиливает защиту учетной записи, так как мошеннику будет сложнее получить доступ к системе, даже если он получит доступ к одному из факторов аутентификации.
- Не храните пин-код рядом с картой, а карту рядом с телефоном.
- Установите антивирусное программное обеспечение.
- Сохраняйте в закладках адреса нужных вам сайтов и пользуйтесь только ими при совершении покупок через интернет. У поддельного сайта адрес может отличаться от настоящего лишь парой символов В адресной строке нет https и значка закрытого замка Дизайн скопирован некачественно, в текстах могут быть ошибки, а у самого сайта мало страниц или даже всего одна — для ввода данных карты.
- Самостоятельно установите лимит, больше которого нельзя потратить с карты. Так вы сбережете основные средства, даже если карту или её данные похитят.
- Сообщите об инциденте. Если вы стали жертвой мошенничества, обратитесь в правоохранительные органы и предоставьте им всю информацию, которая может помочь в расследовании.
- Если вам звонят от имени Центрального банка или есть сомнения в отношении финансовых структур, то наберите номер горячей линии Банка России **8-800-300-3000.**

Помните, что важно быть бдительным в сети и всегда проверять информацию, прежде чем предоставлять свои личные данные или отправлять деньги. Следуя простым советам, вы сможете защитить себя от мошенников и сохранить свои данные в безопасности.

Глава 9 Примеры работы правоохранительных органов и органов власти по расследованию и предотвращению мошеннических действий

- Как рассказали в пресс-службе УМВД России по Екатеринбургу. 21 сентября 2023 года судье в мессенджер написал якобы председатель суда и предупредил, что позднее на нее выйдут представители Министерства юстиции. И лжесотрудник ведомства вскоре объявился, но опять же уведомил, что далее с судьей будут общаться правоохранители и представители Центробанка - нужно скорейшим образом предотвратить дистанционное оформление кредита мошенниками. Женщине предложили взять "зеркальный заём" на 1 млн 980 тысяч рублей, обналичить сумму через кассу и сохранить ее на "безопасном счете". Так и было сделано. Когда обманутая поняла, что натворила, обратилась в полицию. В настоящее время по факту хищения денежных средств сотрудники органов внутренних дел предпринимают комплекс оперативно-розыскных мероприятий, направленных на раскрытие данного преступления.
- Трое жителей Екатеринбурга стали жертвами телефонных мошенников, орудующих под видом госслужащих. В общей сложности они перевели на чужие счета 8,7 миллиона рублей. Как рассказали в пресс-службе городской полиции, от действий злоумышленников пострадали преподаватель вуза, логопед детского сада и учитель средней школы. Во всех случаях мошенники входили в доверие, представляясь сотрудниками Центробанка, Министерства просвещения и ФСБ. Так, логопед детсада из Орджоникидзевского района «инвестировала» в некий финансовый проект 4,3 миллиона рублей. Преподавателя педуниверситета аферисты убедили отправить 3,8 миллиона рублей на «безопасный счет» — аналогичным образом с полумиллионом рублей расстался учитель школы из Ленинского района. Ни банки, ни тем более правоохранительные органы никогда не обзванивают горожан по поводу "зеркальных займов", а "безопасных счетов" и вовсе не существует. Если вы стали участником такой "беседы", немедленно прекратите разговор и сообщите о случившемся по официальным телефонам клиентской поддержки, а также обратитесь в полицию.
- В октябре 2023 года суд города Серов в Свердловской области по материалам полиции отправил на 2 года и 8 месяцев в колонию 20-летнюю уроженку Пермского края, которая в составе организованной группы мошенников обманула 9 граждан преклонного возраста по схеме «Ваше родственник попал в ДТП». Выявили и задержали гражданку сыщики уголовного розыска в тот момент, когда она выходила из съемной квартиры в Екатеринбурге и собиралась ехать к очередной своей жертве в город Каменск-Уральский. Установлено, что любительница легких денег действовала с января по февраль 2023 года на территории Серова, Первоуральска, Режа и Каменска-Уральского. Женщина представлялась пенсионерам их родственницей или знакомой, вводила их в заблуждение о виновности в ДТП и необходимости передачи крупных сумм, что избежать тюрьмы. Приходя в дом потерпевших, предприимчивая особа всегда заботилась о собственной безопасности, на лицо одевала медицинскую маску и переодевалась в другую одежду, как опытный конспиратор. В момент задержания быстро сообразила, что вскоре окажется на длительный срок за решеткой,

поэтому быстро придумала план, как этого избежать. Она умудрилась внезапно схватить колюще-режущий предмет и причинить им себе травму. После чего врачи вынуждены были поместить её на две недели в медицинское учреждение. Лишь после этого она оказалась под стражей. Подобной противоправной деятельностью мошенница стала заниматься, мечтая о яркой и красивой жизни, но ее планам помешали представители Свердловской полиции.

- Жительница Екатеринбурга обратилась в полицию с заявлением о совершенном в отношении нее мошенничестве. Она рассказала, что 21 сентября ей написали в мессенджере от имени силовых структур. Женщине сообщили, что с ней должен связаться представитель Министерства юстиции. И действительно, вскоре ей позвонил неизвестный, который предупредил: в отношении нее якобы замышляется мошенничество – неизвестные пытаются оформить кредит на ее имя. Чтобы предотвратить хищение денег, она должна оказать содействие работникам правоохранительных органов и Центробанка. Затем екатеринбурженке начали звонить лже-сотрудники ФСБ и банка. Используя методы социальной инженерии, они убедили ее оформить «зеркальный», как они пояснили, кредит, и тем самым обезопасить свои средства. Следуя инструкциям мошенников, женщина взяла банковский заем на два млн рублей, обналичила деньги и перевела всю сумму на «безопасные счета». Позже она проанализировала ситуацию и поняла, что стала жертвой мошенников. По факту хищения денежных средств у жительницы Екатеринбурга возбуждено уголовное дело, ведется следствие.
- Верх-Исетский районный суд Екатеринбурга рассмотрит уголовное дело в отношении организованной группы курьеров телефонных мошенников, обманувших 60 человек. Перед судом предстанут 13 мужчин и одна женщина. По версии следствия, они были звеном в мошеннической схеме «Ваш родственник попал в ДТП». Неизвестные лица звонили людям и сообщали, что их близкие якобы попали в дорожную аварию, поэтому нужно передать деньги для лечения пострадавших, чтобы избежать уголовной ответственности. Перед курьерами ставилась задача в кратчайшие сроки приехать к потерпевшим и забрать у них сбережения. Часть денег «бегунки» оставляли себе в качестве вознаграждения. В период с декабря 2021 года по апрель 2022 года преступная группа украла более 11,9 миллиона рублей у 60 обманутых граждан. Организатор мошеннической схемы не установлен, материалы в отношении него выделены в отдельное производство. Группу курьеров, по данным следствия, возглавлял 27-летний екатеринбуржец. В зависимости от роли и степени участия они обвиняются по следующим уголовным статьям: части 1 и 2 статьи 210 УК РФ «Создание и участие в преступном сообществе в целях совместного совершения тяжкого преступления» и часть 4 статьи 159 УК РФ «Мошенничество, организованной группой, в особо крупном размере, с причинением значительного ущерба, группой лиц по предварительному сговору. Правоохранители еще раз напоминают: никаких зеркальных кредитов и безопасных счетов не существует. Представители банков и силовых структур никогда не склоняют граждан к

участию в спецоперациях по поимке преступников, не предлагают им оформить кредиты, не запрашивают данные банковской карты, включая PIN-код.

- В середине 2023 года правоохранительными органами в ряде субъектов нашей страны зафиксированы и пресечены попытки совершения преступлений террористической направленности в отношении административных зданий. Ранее подобные противоправные действия были предотвращены в Нижнем Тагиле и Первоуральске. Имеющиеся в распоряжении специальных служб региона данные об обстоятельствах их совершения свидетельствуют о ряде особенностей. Противоправные деяния исполнителей потенциальных преступлений явились следствием совершенных в отношении них мошеннических действий со стороны третьих лиц. Лица, которые обманным путём подталкивали жителей региона к совершению преступлений, находятся за пределами Российской Федерации. Жертвами «телефонных террористов» как правило являются социально-уязвимые категории граждан или лица, попавшие в трудную жизненную ситуацию, которые легко поддаются внушению. Для достижения своих преступных целей злоумышленники представлялись сотрудниками правоохранительных органов и требовали совершить заведомо сомнительные финансовые операции. В дальнейшем они обманным путём получали данные, которые впоследствии использовали для манипулирования сознаниями жертв. Для возврата денежных средств на счета подвергшихся подобной обработке граждан им предлагалось совершить террористический акт. Комментируя активизацию работы «телефонных террористов» УФСБ России по Свердловской области призывает жителей и гостей Урала быть бдительными, не поддаваться на их провокации и сохранять холодный разум. Рекомендуется также поговорить со своими родными и близкими старшего возраста, предупредив их о существующей угрозе. В очередной раз спецслужба отмечает, что ни сотрудники ФСБ, ни представители иных силовых структур не вправе с использованием телефонной связи требовать от граждан участия в «спецоперациях», связанных с любыми финансовыми инструментами.
- Технологии развивают не только мошенники, но и операторы связи. Уже несколько лет на сетях крупных операторов работают Антифрод (антимошеннические) системы. Для решения проблемы телефонного мошенничества Роскомнадзор начал создание Единой платформы верификации вызовов, которая сможет объединить и маршрутизировать запросы от 2400 Антифрод систем российских операторов. Все работы по объединению запланированы до марта 2024 года. Система «Антифрод» позволяет усиливать контроль за телефонными вызовами в России и выявлять подменные номера. Первую очередь системы запустили в декабре 2022 года. В среднем в сутки она выявляла около 1,5 млн звонков мошенников. В июле 2023 года количество таких звонков выросло на 21% по сравнению с июнем и составило почти 73 млн. Всего с декабря 2022 по июль 2023 года предотвращено 391,3 млн мошеннических звонков. Система в первую очередь вводят блокировку подменных номеров. Но не всегда мошенники могут пользоваться подменой номера, иногда они используют чужие действующие телефонные номера. Мошенники начали

использовать в качестве «подменных» номера тех, кто нагрубил аферистам или попытался пошутить над ними. Подменный номер высветится, когда человеку звонят якобы от имени банка или по любой другой мошеннической схеме. Поэтому юристы предостерегают от долгих и тем более грубых разговоров с телефонными мошенниками. Разговор рекомендуется прекращать сразу, как только вы догадались, что дело нечисто. Также рекомендуется использовать автоматический определитель номера (АОН), установленный на смартфон. С его помощью во многих случаях человек сможет увидеть, кто ему звонит, а сомнительные вызовы будут проходить с пометкой «есть жалобы на спам». Лучше выбрать российский АОН, так как он больше нацелен на отечественный рынок. Приложения, определяющие номер, тоже работают по принципу антифрод-платформы: они точно так же обращаются к базе подменных номеров. Но объем этой базы в несколько раз ниже.

- К новым схемам, которые появились в 2023 году, относится использование искусственного интеллекта. С его помощью мошенники подделывают голоса близких и родственников потенциальной жертвы. Эта схема только набирает обороты, поскольку довольно сложна в исполнении, но в будущем может стать настоящей угрозой.

Заключение

Профилактика мошеннических действий составляет неотъемлемую часть повседневной деятельности. Поскольку все мы погружены так или иначе во взаимоотношения с незнакомыми нам лицами, то должны проявлять разумную бдительность и осторожность. Огромный поток внешней информации может порой сбивать с толку, поэтому знания об угрозах со стороны потенциальных злоумышленников необходимы. Знание методов и форм действий мошенников, правил работы с техническими средствами коммуникаций, возможностей информационных систем и программ помогут всегда оставаться в безопасности.

Необходимо иметь при себе номера телефонов своего территориального отдела полиции, дежурной части ГУ МВД России по Свердловской области **8-343-358-83-38**, номера экстренного вызова **02**, **102**, **112**, номер горячей линии Банка России **8-800-300-3000**, напоминать о них нашим подопечным. Пожилым гражданам особенно важно постоянное внимание и информирование о новых формах и методах действий злоумышленников.

Сведения, изложенные в методических рекомендациях, помогут нам избежать неприятных ситуаций, а порой и трагедий. Важна ваша обратная связь, задавайте свои вопросы, вносите предложения.

Список использованных источников и литературы:

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 12.10.2023) [электронный ресурс]https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения 26.10.2023.).

2. Амеличева Л., Белокрыльцева А. «Бабушки против мошенников», Методическое пособие. БО «Адреса милосердия» Москва, 2019;

3. Антитеррористическая комиссия в Свердловской области [электронный ресурс] https://t.me/antiterror_ural дата публикации 02/08/2023/

4. Информационно-просветительский ресурс Центрального банка Российской Федерации Финансовая культура https://fincult.info/rake/

5.Официальный сайт ГУ МВД России по Свердловской области https://66.мвд.рф

6. Российская газета https://www.rg.ru .

7. Ютюб канал ГУ МВД России по Свердловской области https://www.youtube.com/channel/UC9j3n4EQmtnQ9lbyc-9Tb5Q (дата обращения 26.10.2023.)

Приложение 1: статистика ГУ МВД России по Свердловской области

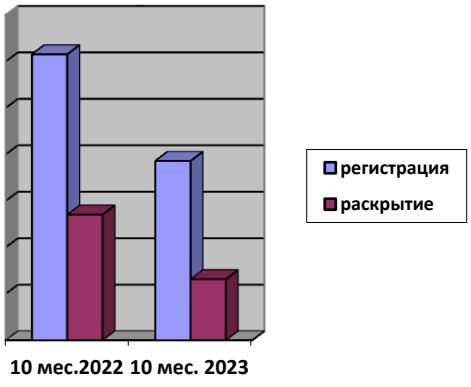
Количество зарегистрированных и раскрытых мошеннических действий контактным способом и с использованием информационно-телекоммуникационных технологий на территории Свердловской области за 10 месяцев 2022/2023 года.

	10 мес. 2022 г. регистрация	10 мес. 2022 г. раскрытие	%	10 мес. 2023 г. регистрация	10 мес. 2023 г. раскрытие	%
Контактные мошенничества	1231	541	39,1	772	263	44,7
Мошенничества с использованием информационных технологий	3884	358	10,8	5889	590	9,5

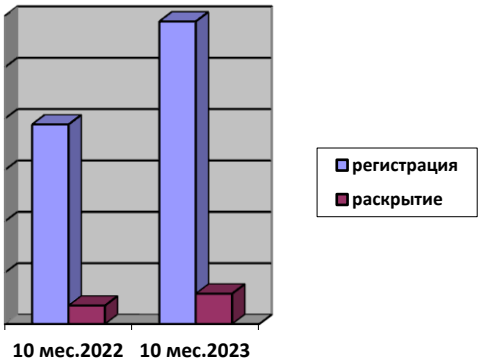
В 17 территориальных органах Свердловской области наблюдается рост зарегистрированных преступлений контактным способом: Кировский район г. Екатеринбурга Орджоникидзевский район г. Екатеринбурга, Артёмовский городской округ, Байкаловский район, Ивдельский городской округ, Камышловский район, Кировградский городской округ, Красноуральский городской округ, Кушвинский городской округ, город Нижний Тагил, Нижнесергинский район, Новолялинский городской округ, Североуральский городской округ, Сухоложский район, Сысертский район, Красноуфимский район, город Лесной.

Самым распространенным видом контактного мошенничества является схема действий злоумышленников, при которой звонят гражданам и сообщают: «родственник попал в ДТП». На втором месте преступления схема, где мошенники под видом социальных работников, проникают в квартиры пожилых граждан и похищают денежные средства.

В тоже время наблюдается рост мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий. По данному виду преступления значительный рост во всех территориальных подразделениях Свердловской области.



Контактные мошенничества



Мошенничества с использованием информационных технологий

Приложение 2: Образцы листовок

ВНИМАНИЕ, МОШЕННИКИ!

ПОМНИ! Мошенники – хорошие **психологи.**
Утром думаешь, что тебя это не коснется,
а вечером пишешь заявление в полицию!

ПОЗВОНИЛ СОТРУДНИК ИЗ БАНКА?

- Уточните причину обращения,
- **ПРЕРВИТЕ ЗВОНОК** и
- обратитесь в офис Вашего банка.

Никогда **НЕ СООБЩАЙТЕ** данные карты **в социальных сетях!**

Никому НЕ СООБЩАЙТЕ:

- код из смс и
- CVV – код с обратной стороны карты!

МВД РОССИИ ПРЕДУПРЕЖДАЕТ

будьте бдительны! звоните 02 или 102

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста!

НЕ ДОВЕРЯЙТЕ,
если Вам звонят и сообщают, что Ваш **родственник или знакомый попал в беду** или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться.
Это ОБМАН!

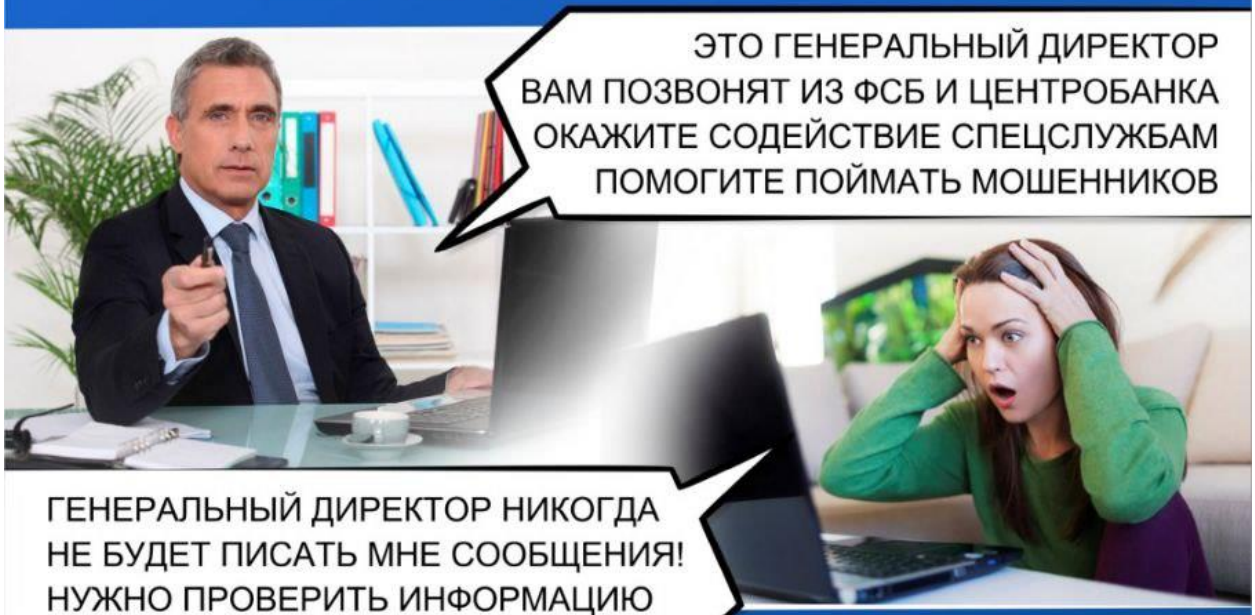
СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ
Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!

Не подписывайте никакие документы!

Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам?
НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!

УМВД России по г. Екатеринбургу предупреждает:

ШЕФ МОЖЕТ ОКАЗАТЬСЯ ФЕЙКОМ!



ВАМ ПОСТУПАЮТ ЭЛЕКТРОННЫЕ ПИСЬМА ИЛИ СООБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ ОТ ЛИЦА ВАШИХ РУКОВОДИТЕЛЕЙ

«НАЧАЛЬНИК» ПРОСИТ ВЫПОЛНЯТЬ ТРЕБОВАНИЯ ПРЕДСТАВИТЕЛЕЙ СИЛОВЫХ СТРУКТУР, КОТОРЫЕ РАССЛЕДУЮТ ХИЩЕНИЯ ДЕНЕГ СО СЧЕТОВ

УТОЧНЯЙТЕ У СВОЕГО РУКОВОДСТВА ДОСТОВЕРНОСТЬ ПОЛУЧЕННОЙ ИНФОРМАЦИИ!
НЕ ВЫПОЛНЯЙТЕ ТРЕБОВАНИЙ НЕИЗВЕСТНЫХ И НЕ ПЕРЕВОДИТЕ ДЕНЬГИ ПО ИХ УКАЗАНИЯМ!

СООБЩАЙТЕ О ФАКТАХ МОШЕННИЧЕСТВА ПО ТЕЛ: 02 (102)