МЕТОДИЧЕСКОЕ ПОСОБИЕ

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА В ОТНОШЕНИИ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

Департамент социального развития
Ханты-Мансийского автономного округа – Югры

Бюджетное учреждение Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА В ОТНОШЕНИИ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

Методическое пособие

Сургут
Бюджетное учреждение Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»
2024

УДК 343.851(079)
ББК 67.408.121.2я81
П84

Под общей редакцией:

И. И. Тимергазина, врио директора бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Ресурсный центр развития социального обслуживания»;

Е. С. Юшковой, канд. филол. наук, начальника отдела социальных технологий бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Ресурсный центр развития социального обслуживания»

Составитель:

М. В. Пикинская, методист отдела социальных технологий бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Ресурсный центр развития социального обслуживания»;

Д. М. Громова, методист отдела социальных технологий бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Ресурсный центр развития социального обслуживания»

П84 Профилактика мошенничества в отношении граждан пожилого возраста : методическое пособие / под общей редакцией И. И. Тимергазина, Е. С. Юшковой; составители М. В. Пикинская, Д. М. Громова. – Сургут : БУ «Ресурсный центр развития социального обслуживания», 2024. – 57 с.

Методическое пособие содержит информационно-методические материалы по предупреждению мошенничества в отношении граждан пожилого возраста, проживающих в Ханты-Мансийском автономном округе – Югре; предназначено для специалистов и руководителей учреждений социального обслуживания, подведомственных Депсоцразвития Югры, а также для широкой общественности.

УДК 343.851(079)
ББК 67.408.121.2я81

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире использование информационно-коммуникационных технологий является неотъемлемой составляющей повседневной жизни. Они перестали быть инструментом, которым владеют лишь «продвинутые» пользователи. Теперь техникой на основе цифровых технологий так или иначе пользуется каждый, независимо от образования и возраста. В связи с этим участились случаи мошенничества с использованием гаджетов.

Анализ социальных и возрастных особенностей граждан, пострадавших от мошенничества, показывает, что этому виду преступлений подвержены все возрастные категории населения. Разумеется, у каждой категории имеются особенности восприятия, связанные с возрастными отличиями, различия в восприятии информации, понимании технологии цифровых процессов, порядка работы банковских учреждений и органов правопорядка. Недостаточные знания граждан являются одной из причин, по которым они становятся жертвами мошенников.

Мошенничество относится к экономическим преступлениям и является уголовно наказуемым (ст. 159 УК РФ). Цель любого мошенничества – выманить денежные средств путем обмана или введения в заблуждение человека любым способом.

Практика показывает, что наиболее сложной категорией в плане защищенности от противоправных действий являются люди пожилого возраста. Им зачастую свойственны забывчивость, доверчивость и нередко беспомощность, что играет на руку мошенникам. Пожилые люди, как правило, используют меньшее количество источников информации, чаще – привычные им телевизор, радио, газеты. Они часто не могут отличить рекламу от информационного выпуска о новейших исследованиях и разработках, не разбираются в банковской сфере, с трудом справляются с гаджетами и привыкли всем доверять. Для данной категории граждан, помимо возрастных рисков, добавляется риск недостаточной информированности о схемах обмана, распознавании мошенников, а значит, повышается вероятность быть обманутыми мошенниками.

В связи с этим с целью профилактики мошенничества должна активнее проводиться разъяснительная и информационно-просветительская работа среди граждан пожилого возраста.

В учреждениях социального обслуживания Ханты-Мансийского автономного округа – Югры постоянно проводится разъяснительная работа по профилактике мошенничества с целью снижения риска совершения мошенничества в отношении пожилых людей (в том числе проживающих в

стационарном учреждении социального обслуживания). Но, учитывая, что проблема мошенничества с использованием методов социальной инженерии остается актуальной, необходимо усилить работу среди граждан пожилого возраста в данном направлении путем проведения обучающих занятий в «Университете третьего возраста» и просветительских мероприятий, консультирования сотрудниками разных ведомственных структур, оказания помощи и поддержки волонтерами.

Методическое пособие «Профилактика мошенничества в отношении граждан пожилого возраста» разработано для специалистов учреждений, подведомственных Депсоцразвития Югры, для применения в работе с пожилыми людьми.

В методическом пособии описаны виды и приемы мошенничества, меры предупреждения мошенничества, действия специалистов по работе с гражданами пожилого возраста, правила для граждан и др.

При разработке методического пособия использовались материалы, размещенные на официальном сайте Департамента региональной безопасности Ханты-Мансийского автономного округа – Югры, иных Интернет-ресурсах.

ГЛАВА 1. АЛГОРИТМ РАБОТЫ СПЕЦИАЛИСТОВ УЧРЕЖДЕНИЙ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ С ГРАЖДАНАМИ ПОЖИЛОГО ВОЗРАСТА ПО ПРОФИЛАКТИКЕ МОШЕННИЧЕСТВА

Мошенничество, согласно определению, данному в ст. 159 Уголовного кодекса Российской Федерации, – это совершенное с корыстной целью путем обмана или злоупотребления доверием противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества, либо совершенное теми же способами противоправное и безвозмездное приобретение права на чужое имущество.

Основой мошеннических схем служит информация о персональных данных, полученная на нелегальном рынке баз данных финансовых учреждений, государственных структур, Интернет-магазинов, центров занятости, салонов сотовой связи, а также от граждан, относящихся с доверием к телефонным звонкам, СМС-сообщениям, информации на сайтах и др. Для совершения своих преступных действий мошенники собирают информацию, которую потом используют в смежных мошеннических схемах.

Профилактика мошенничества в отношении граждан пожилого возраста является важным аспектом благополучия пожилых людей. Соблюдение простых правил гражданами пожилого возраста – это их вклад в безопасность дома, имущества, в свое психическое и физическое здоровье.

С целью недопущения мошенничества, снижения уровня риска махинаций рекомендуется расширить курс обучения пожилых граждан по вопросам профилактики мошенничества в рамках программы обучения граждан старшего поколения «Университет третьего возраста».

1.1. Алгоритм работы специалистов для предотвращения мошенничества в отношении граждан пожилого возраста

Для предотвращения мошенничества в отношении граждан пожилого возраста применяется типовой алгоритм действий специалистов учреждений социального обслуживания. Специалистам учреждений социального обслуживания рекомендуется:

1. Пройти обучение по содержанию мошеннических схем и их предотвращению. Изучить виды и приемы мошенников, психологические зацепки мошенников и правила безопасности, а также основы финансовой грамотности.

2. Подготовить наглядно-дидактические материалы по борьбе с мошенничеством для распространения среди граждан пожилого возраста.

3. Разработать план мероприятий по профилактике мошенничества в отношении граждан пожилого возраста.

4. Провести разъяснительные беседы с пожилыми людьми по темам: распространенные схемы мошенничества, тактика мошенников, правильное реагирование на мошенников, меры безопасности и др.

5. Обучить граждан пожилого возраста основным правилам безопасности (в рамках факультетов «Цифровая грамотность», «Финансовая грамотность», «Безопасность жизнедеятельности» программы обучения граждан старшего поколения «Университет третьего возраста»).

6. Провести практические мероприятия с гражданами пожилого возраста по смоделированным мошенническим схемам для разбора ситуаций и отработки навыков безопасного поведения и адекватного ответа мошенниками.

7. Распространить тематические буклеты и памятки среди граждан пожилого возраста.

1.2. Алгоритм работы специалистов при совершении мошенничества в отношении граждан пожилого возраста

При совершении мошенничества в отношении граждан пожилого возраста, пребывающих в учреждении социального обслуживания, рекомендуется придерживаться следующего алгоритма действий. Специалисту учреждения социального обслуживания следует:

1. Прибыть незамедлительно к получателю социальных услуг, попавшему на мошенническую схему, по его запросу.

2. Сообщить о факте мошенничества руководству учреждения социального обслуживания, в правоохранительные органы, полицию (тел. 02, 102), единую службу спасения (тел. 112).

3. Помочь пострадавшему вспомнить все подробности, действия мошенников, их приметы, время и суть разговора, предварительно оценив причиненный ущерб.

4. Пригласить психолога для работы с пострадавшим, чтобы успокоить и снизить психоэмоциональное напряжение (при необходимости).

5. Оказать помощь гражданину пожилому возраста в обращении в отдел полиции (при составлении заявления).

6. Провести разбор мошеннического действия, выявить ошибки пожилого человека, смоделировать ситуацию «как правильно поступать в подобной мошеннической схеме».

7. Оставаться на связи с пожилым человеком и поддерживать до тех пор, пока не будет полностью выяснена ситуация и определены дальнейшие действия.

1.3. Рекомендации по формированию обучающей программы по профилактике мошенничества в отношении граждан пожилого возраста

В содержание обучающей программы по профилактике мошенничества в отношении пожилых людей рекомендовано включать ниже приведенные темы. Планируемый объем обучающих мероприятий (количество часов и тематика программы) определяется с учетом уровня первичных знаний граждан, желающих пройти обучение, о профилактике мошенничества и востребованности получения навыков борьбы с мошенническими схемами. Для каждого обучающего следует подготовить информационно-дидактический материал (памятки, буклеты, схемы, алгоритмы и т. п.) по мерам безопасности и защиты от мошенничества.

Тема 1. Виды мошенничества

При изучении темы «Виды мошенничества» рекомендуется делать упор на то, что мошенники обманывают людей всех возрастов, при этом пояснить, что в «любимую» категорию мошенников входят пожилые люди, потому что данная категория граждан имеет постоянный гарантированный доход – пенсию. Рассказать о видах мошенничества, об их особенностях. Рассмотреть примеры мошенничества, конкретные случаи, произошедшие с гражданами, и провести их разбор; определить дальнейшие действия и ошибки гражданина. Напомнить о телефонах, по которым необходимо звонить в случае мошенничества.

Тема 2. Приемы мошенничества

При изучении темы «Приемы мошенничества» затронуть весь комплекс преступных схем и ресурсов, которые используют мошенники при совершении мошеннических действий. Подробно рассмотреть методы социальной инженерии, нейролингвистики, гипноза, используемые мошенниками в своих схемах; привести примеры. Провести разбор ситуаций мошенничества в отношении пожилых граждан в части применяемых со стороны аферистов приемов.

Тема 3. Психологические зацепки мошенников

При изучении темы «Психологические зацепки мошенников» разобрать основные психологические манипуляции, которые используются в отношении граждан пожилого возраста для использования их в своих корыстных целях. Рассмотреть примеры мошеннических действий с гражданами в разрезе

используемых психологических манипуляций. Провести разбор ситуаций, произошедших с гражданами, которые попались на психологические уловки мошенников.

Тема 4. Правила защиты от мошенничества

При изучении темы «Правила защиты от мошенничества» рассмотреть меры безопасности, как и в каких случаях руководствоваться правилами защиты от мошенничества, в том числе с привлечением родственников. Рассмотреть примеры профилактики мошенничества в отношении граждан пожилого возраста в комплексе и с учетом видов/приемов мошенничества, психологических зацепок и правил безопасности.

Рекомендации

При подготовке занятий с гражданами пожилого возраста важно учитывать специфику региона, так как местные варианты мошенничества могут отличаться от классического набора мошеннических схем. При разборе мошеннических схем необходимо разбирать и записывать новые способы мошенничества в отношении граждан пожилого возраста.

Также следует учесть при проведении обучающих мероприятий, что среди слушателей может находиться человек, попавший под влияние мошенников, который однако не готов в этом признаться. Поэтому важно подробно разбирать разные случаи мошенничества, информацию в Интернете о мошенниках, с которыми сталкивались слушатели в группе (возможно, эта схема/организация уже оставила за собой следы). Если даже конкретному гражданину и не удастся помочь, зато он будет вооружен на будущее, а другие – предупреждены.

ГЛАВА 2. ВИДЫ МОШЕННИЧЕСТВА

Единой общепринятой классификации мошенничества нет, однако все мошеннические схемы связаны с кражей денежных средств с банковских счетов граждан либо выманиванием у людей денежных средств обманным путем.

В данном пособии рассмотрены основные виды мошенничества, связанные с банковскими картами (счетами), «выигрышем в лотерею», «поимкой преступников», «благотворительностью», телефонными вирусами и т. п.

В последнее время широко распространено мошенничество с использованием социальной инженерии.

Социальная инженерия (social engineering), или «атака на человека», – совокупность психологических и социологических приемов, методов

и технологий, которые позволяют получить конфиденциальную информацию. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, персональным данным, данным карточек, паролям, банковским данным и другой персональной информации с последующим осуществлением мошеннических операций. Обезопасить себя от мошенничества с применением социальной инженерии можно, соблюдая простые меры безопасности и проявляя разумную бдительность.

2.1. Мошенничество с банковскими картами и счетами

Банковская карта, безусловно, удобная и полезная вещь для совершения покупок, оплаты – и крайне соблазнительная для мошеннических действий.

Звонок от неизвестного лица о покупке или продаже товара/услуги

Человеку поступает звонок по объявлению, данному в Интернете или в СМИ, и на той стороне соглашаются на покупку не торгуясь, но с переводом оплаты на карту. Мошенник – «потенциальный покупатель» – просит сообщить номер, срок действия и CVV-код карты и после этого сообщить СМС-код банка о проведенной операции. Если мошеннику не удается получить весь набор информации, то недостающие данные восполняются квалифицированными хакерами. В результате счет банковской карты не пополняется, а опустошается путем перевода наличности на некий электронный кошелек, который немедленно исчезает из сети после вывода средств с него, и тогда найти мошенника практически невозможно.

Звонок от «службы безопасности банка» о подозрительной банковской операции

Мошенник – «сотрудник банка» – уведомляет клиента о сбое в программном обеспечении, который привел к потере средств, либо о попытке взлома или блокировки банковской карты, подозрительных действиях в онлайн-банке. Также может поступить угроза штрафа по надуманному обвинению либо предупреждение о пропущенном платеже по кредиту. Для решения данных проблем мошенник просит человека назвать банковские данные со всеми кодами для восстановления счета и возврата денег.

Звонок по короткому номеру банка об оформлении кредита

Человеку поступает звонок по короткому номеру банка с использованием специальных программ-обманок, которые маскируют настоящий номер звонящего, и абонент видит знакомый ему идентификатор. Мошенники предлагают гражданам оформить кредит на выгодных условиях либо совершить иное действие, с помощью которого мошенники получают доступ к персональным данным гражданина и его счетам.

Звонок от «силовых структур»

Лжесотрудник представляется по Ф.И.О., заявляет о высокой вероятности кражи денежных средств человека для перевода их в иностранное государство, которое действует против России (что является госизменой и карается по закону).

Мошенники, как правило, представляются от имени руководителя организации, в которой работает человек, в мессенджере Телеграм с оповещением работника об утечке его персональных данных и назначении «куратора» по данному вопросу. Человек, доверяя своему руководителю, ничего не подозревая, идет на контакт с мошенником-«куратором», Ф.И.О. которого дал мнимый руководитель в Телеграме. Далее мошенники «от лица» «силовых структур» рассказывают историю о некоем предателе, которого необходимо поймать путем финансовых манипуляций с банковскими счетами человека (ловля на живца). Чтобы вычислить «предателя», убеждают человека перевести средства на некий безопасный счет. По данному вопросу мошенники соединяют с разными лжесотрудникам банка, ЦБ, службы безопасности, при этом не разрешая человеку ни с кем разговаривать и звонить по поводу проводимой «секретной операции». Гражданин, доверяя «службе безопасности», в надежде помочь поймать преступника идет на сделку с мошенниками, выполняя все их поручения. В результате человек передает/перечисляет денежные средства (в т. ч. числе оформленные кредиты) мошенникам.

Звонки от иных «ведомств» и «организаций» (налоговая служба, страховые компании, службы ЖКХ, управляющие компании, риелторы, Госуслуги, Социальный фонд России и др.)

Звонок от «сотрудника Госуслуг»: мошенники сообщают, что на имя гражданина пришло электронное письмо и что необходимо назвать код из СМС, чтобы оно отразилось в личном кабинете на Госуслугах. Получив от человека СМС-код, мошенники получают доступ к аккаунту Госуслуг. В личном кабинете Госуслуг мошенники получают всю информацию о доходах, о транспортных средства, квартирах, налогах, кредитной истории. Они могут оформить займ и произвести много иных мошеннических действий.

Звонок из «пенсионного фонда»: лжесотрудник, обращаясь по имени-отчеству к человеку, сообщает, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда, либо о переплате средств. Убеждает человека, что для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.

Кроме того мошенники уговаривают человека перевести деньги на другую банковскую карту или установить предлагаемый номер мобильного телефона в качестве доверительного, что позволит мошенникам войти в мобильный банк гражданина.

Звонок из «Центробанка»: лжесотрудник предлагает человеку установить на телефон приложение «Банкноты Банка России» для проверки подлинности 5-тысячной купюры. Вместе с приложением скачивается вредоносная программа, которая дает доступ к личному кабинету человека.

Звонок из «поликлиники», «аптеки», «медицинского центра»: мошенники преподносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить звонящему.

Звонок от «оператора сотовой связи»: звонит лжесотрудник сотовой связи с оповещением о завершении срока договора на сотовую связь или перенесении номера на другого оператора, в связи с чем номер будет заблокирован. Для пролонгации договора требуют назвать направленный на номер человека СМС-код. С помощью кода мошенники получают доступ к личным кабинетам банков, Госуслуг, сотовой связи и иным сервисам.

2.2. Мошенничество со счетами мобильных телефонов

Мобильная телефонная связь является наиболее простой в исполнении мошеннической схемой.

«Ошибочный» перевод денег на телефон. Человеку поступает СМС-сообщение или звонок об ошибочном переводе денег на счет его мобильного телефона, и «пострадавший» объясняет, что якобы случайно перевел деньги, и просит вернуть их владельцу. При отказе произвести перевод денег на телефон «владельца» могут поступать угрозы обращения в полицию или оператору связи с требованием блокировки телефона. Вы переводите, после чего такая же сумма списывается с Вашего счета. Чтобы во второй раз списать сумму с Вашего счёта, злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. То есть первый раз вы переводите деньги по его просьбе, а второй раз он получает их по правилам возврата средств.

Блокировка телефона. Бывают случаи, когда в процессе перевода денег человеку за мобильную связь мошенниками запускается программа

блокировки телефона и никакие вызовы недоступны, либо вообще гаснет экран, и телефон не работает. Тогда следует срочно с чужого телефона позвонить оператору связи и в банк, откуда списались деньги, и сообщить о мошенничестве.

2.3. Мошенничество с «попавшим в беду родственником»

Игра на личных мотивах и родственных связях граждан – выигрышная схема для мошенников.

Человеку (матери, отцу, бабушке) поступает звонок о попавшем в беду родственнике (сыне, дочери, внуке) от имени правоохранительных органов или медицинских учреждений: это может быть сообщение о ДТП, хранении оружия или наркотиков, нанесении тяжких телесных повреждений, убийстве. Например, лжесотрудник полиции по телефону уверенным тоном сообщает, что в данной ситуации можно помочь родственнику, но для решения вопроса (закрытия дела) необходима определенная сумма денег, которую следует привезти в определенное место или передать/перевести какому-либо человеку. Обычно это случается среди ночи, чтобы ввести в панику полусонную жертву. Человек переводит озвученную сумму на электронный кошелек или счет мобильного телефона. Метод крайне жестокий, известны случаи инфарктов от подобных «новостей».

2.4. Мошенничество с «выигрышем в лотерею»

Данная мошенническая схема широко применяется в отношении граждан пожилого возраста.

Человеку поступает звонок от якобы ведущего популярной радиостанции, который поздравляет с крупным выигрышем в лотерею, организованной радиостанцией или оператором мобильной связи. Мошенник убеждает в том, что для получения приза (телефона, ноутбука или даже автомобиля), необходимо в течение минуты дозвониться на радиостанцию по указанному номеру телефона. Перезвонившему абоненту отвечает сотрудник «призового отдела» и грамотно убеждает в «честности» акции (никаких взносов, переигровок и т. д.), просит представиться и назвать год рождения, подробно объясняет условия получения приза, причем для его получения требуется осуществить «незначительный» предварительный перевод денежных средств или предоставить персональные данные, данные карты, полученный код из СМС.

2.5. Мошенничество с короткими номерами мобильной связи

Мошенничество с короткими номерами мобильной связи – малозатратный для преступников прием совершения махинаций.

Человеку поступает звонок либо приходит СМС-сообщение якобы от сотрудника службы технической поддержки оператора мобильной связи с обоснованием: предложение подключить новую эксклюзивную услугу; для перерегистрации во избежание отключения связи из-за технического сбоя; для улучшения качества связи; для защиты от спам-рассылки; для принятия участия в акции от сотового оператора.

Мошенник предлагается набрать под диктовку код или СМС, которое «подключит новую услугу», «улучшит качество связи» и т. п. На самом деле происходит следующее: предложенный код является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только он набирается, счет человека обнуляется (никакая услуга не подключается).

2.6. Мошенничество со «штрафными санкциями»

Махинации со штрафными санкциями – наиболее распространенный прием у мошенников.

Человеку поступает звонок от лжесотрудника службы технической поддержки оператора мобильной связи. Мошенник сообщает, что произошло нарушение условий договора (например, абонент сменил тарифный план, не оповестив оператора; не внес своевременно оплату; воспользовался услугами роуминга без предупреждения и т. п.). Якобы чтобы предотвратить отключение номера, мошенник предлагает перевести на свой номер сумму штрафа и набрать код; перевести средства на указанный номер и т.п. Мошенник обещает, что данные действия помогут доказать невиновность гражданина и при этом сохранить свой номер.

2.7. Интернет-попрошайничество

Интернет-попрошайничество – достаточно новый и очень изощренный вид мошенничества.

Благотворительные акции. В Интернете появляются объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего сайта, меняют реквизиты для перечисления денег.

Рекламные предложения. Мошенники проводят рассылку фальшивых рекламных предложений и ложных ссылок в мессенджерах, на Интернет-ресурсах на предзаказ товаров со скидкой для получения доступа к банковским картам и счетам клиентов. После оплаты такие товары либо не доставляются, либо оказываются поддельными.

Суперскидки, акции в мессенджерах. Мошенники размещают объявления о суперскидках в мессенджерах, включая закрытые чаты. Переходя по ссылке, пользователи скачивают вредоносный APK-файл, замаскированный под приложение для получения промокодов или скидок. После его установки мошенники получают доступ к паролям, одноразовым кодам и другой конфиденциальной информации, и могут управлять банковскими счетами без ведома жертвы.

Для того чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, необходимо перезвонить в указанную организацию и уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать – передавать деньги или нет.

2.8. Мошенничество с Интернет-ресурсами (фишинговые атаки)

Зная номер телефона человека, мошенники делают разные комбинации махинаций, включая совершение фишинговых атак[1].

Злоумышленники подделывают популярные сайты (к примеру, органов власти и различных ведомств), а также подделывают сайты известных магазинов, маркеплейсов, туристических компаний, авиакомпаний и др. Имитируя Интернет-ресурсы популярных компаний, мошенники рассчитывают, что пользователи не заметят подделку и оставят на поддельной фальшивой странице важную информацию: личные или финансовые данные, логин и пароль, контактные сведения (номер телефона и электронную почту), а также оплатят покупку путевок, авиабилетов и иных услуг.

Распознать фишиговый сайт можно по нескольким признакам: адрес сайта может отличаться от настоящего лишь парой символов; в адресной строке отсутствует «https» и значок закрытого замка; дизайн сайта скопирован некачественно, в текстах допущены ошибки; у сайта мало страниц или даже только одна – для ввода данных карты.

Зачастую мошенники создают сайт, замаскированный под Госуслуги. Несмотря на то что внешне он очень похож на настоящий, при внимательном

[1] Фишинговые атаки – вид интернет-мошенничества, цель которого – получение идентификационных данных пользователей (в том числе паролей, номеров карт), кража или повреждение конфиденциальных данных путем обмана людей.

рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена. Настоящий сайт «Госуслуги», а также официальные сайты финансовых организаций в популярных поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

2.9. Мошенничество с использованием телефонных вирусов

С развитием IT-технологий участились случаи мошенничества с использованием телефонных и компьютерных вирусов (в т. ч. вирусов в программном обеспечении)

Ссылка в СМС-сообщении. Человек получает СМС-сообщение о том, что ему надо пройти по указанной ссылке в некий мессенджер для получения/прочтения важного сообщения. При переходе по данной ссылке в смартфон внедряется вирус программного обеспечения, благодаря которому мошенники получают полный контроль над гаджетом – происходит кража данных, денежных средств.

Скачивание мобильного контента. Человек при скачивании мобильного контента получает предупреждение через СМС-сообщение: «Вы собираетесь отправить сообщение на короткий номер. Для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений.

2.10. Мошенничество по месту жительства человека

Представители «газовой службы» или «водоснабжения»: лжесотрудник приходит домой к пожилому человеку якобы для проведения осмотра счетчиков или сверки показаний. Пенсионеры не задумываясь впускают мошенников в квартиру. После осмотра приборов злоумышленники сообщают, что нужно заменить какое-либо оборудование и уверяют в необходимости покупки этого оборудования у них, запугивая возможной утечкой газа или прорыва водопровода. Взволнованные пенсионеры соглашаются на все, что им предлагают аферисты, вследствие чего остаются обманутыми и лишенными денежных средств. По такой схеме мошенники часто обманывают пожилых людей, продавая и другие товары (медицинские аппараты, пластиковые окна и т. д.).

Представители «службы ренты»: под видом ухода за пожилым человеком мошенники заключают договор ренты и разрабатывают недобросовестную схему завладения квартирой пожилого человека – сразу или

после его смерти, пользуясь тем, что одиноким пенсионерам нужны деньги, помощь по дому и уход. Однако люди пожилого возраста порой теряют бдительности и не разбираются в договорах, в связи с чем могут получит не то, что ожидали. На словах мошенники проговаривают одни условия ренты, а на подпись подсовывают договор с другими условиями – пенсионер ожидает помощь и уход, но не получает их. Также мошенники могут в последний момент подменить договор ренты договором купли-продажи или дарения квартиры, в результате человек переписывает квартиру на аферистов, а сам остается на улице. Затем мошенники продают квартиру, и пострадавшими оказываются и пенсионер, и покупатель квартиры.

ГЛАВА 3. ПРИЕМЫ МОШЕННИКОВ

Для совершения обмана мошенники в свои махинации включают целый комплекс различных ресурсов/процессов/действий: регистрацию юридических лиц, аренду офисов, наем сотрудников, производство какого-либо товара и его агрессивную рекламу, создание фейковых сайтов и др.

Приемы мошеннических схем основаны на неожиданности, обещании «всего и сразу», напористости, запугивании, требовании немедленного принятия решения (срочности), имитации заботы и т. п. Мошенники в свои изощренные схемы включают методы социальной инженерии, нейролингвистики, гипноза: психологическое давление и манипулирование, выведение человека из равновесия, приведение его в состояние страха, стресса, либо же завоевание доверия, сочувствие, налаживание эмоционального контакта и др.

Рассмотрим более подробно приемы мошенников, используемые в отношении пожилых людей.

3.1. Срочность принятия решения

Суть мошеннического приема: мошенники торопят пожилого человека требуют принять решение срочно, быстро, чтобы он не успел опомниться и подумать над сложившейся ситуацией и адекватным принятием решения; не дают времени на прочтение договора (иных документов), не разрешают посоветоваться с друзьями и родными.

Действия мошенников сопровождаются такими формулировками: «срочно», «немедленно», «только сейчас», «последний день», «осталось последнее место», «если вы успеете первым ответить на вопрос, то…», «до конца акции осталось совсем немного», «только для вас индивидуальное

предложение», «а то не останется», «перестанет действовать скидка», «будет не так выгодно» и т. п.

3.2. Фактор неожиданности

Суть мошеннического приема: мошенники стараются звонить внезапно, чтобы создать эффект неожиданности, сообщают об «экстренных ситуациях», когда человеку сложнее адекватно реагировать на информацию (ночью или раним утром).

Действия мошенников сопровождаются ночным звонком с сообщением ложной информации о том, что близкий родственник (сын, муж) сбил человека или попал в аварию и что срочно нужны деньги для откупа или проведения срочной операции. Говорят от имени полицейского (если «авария») или от имени врача (если «попал в больницу»). Человек, ошеломленный плохой новостью, переводит на указанный счет денежные средства (или срочно начитает занимать деньги у знакомых, оформлять кредит), чтобы на родственника не завели уголовное дело / сделали сложную срочную операцию. Мошенники также выводят человека из равновесия неожиданными сообщениями о смертельной болезни родственника, срочности сложной операции (рак), о заблокированной банковской карте, с которой якобы сейчас выводят денежные средства и др.

3.3. Завышенные (нереальные) обещания

Суть мошеннического приема: мошенники по телефону предлагают разные услуги, которые могут заинтересовать пожилого человека. Для этого они нажимают на «болевые точки» всех пожилых людей – небольшие пенсии, хронические болезни, одиночество, несбывшаяся мечта, долг государства и др.

Действия мошенников включают основные «услуги», связанные с завышенными обещаниями: «волшебные» таблетки, мази, «лечебные» напитки, исцеляющие все болезни (за минимальную стоимость); подарки (бесплатно); приборы медицинского назначения, излечивающие от «всех» болезней; высокая доходность банковских счетов (от 50 до 100 %) и оформление беспроцентного кредита; путевки в санатории / дома отдыха / пансионаты («пенсионерам практически бесплатно»); участие в беспроигрышной лотерее и крупном выигрыше (оплата только доставки, пересылки или налога); прибавка к пенсии; бытовая техника «по исключительным ценам» и т. п.

3.4. Напористость

Суть мошеннического приема: мошенники с самого начала ставят целью не отпустить свою жертву под любым предлогом, поэтому ни на минутку не оставляют ее наедине с собой (родственниками, знакомыми, коллегами) и энергично обрабатывают и «ведут» до момента, пока они не заберут деньги: не дают отвлечься от разговора, прервать разговор, положить трубку под предлогом «секретности проводимой операции», «защиты информации» или «серьезности предложений». В то же время, удерживая человека на телефоне, узнавая информацию о его банковских счетах, мошенники стараются расположить его проникновенными разговорами, расспросами о жизненных ситуациях, проблемах.

Действия мошенников направлены на убеждение человека в важности «проводимой операции по поимке преступника» и необходимости перевода денежных средств на «безопасный банковский счет». При этом аферисты сопровождают человека до банкомата для снятия денег (или банка для взятия кредита) для проведения «закрытой операции по поимке преступника». Чтобы создать наиболее комфортные условия для жертвы и побыстрее забрать деньги, мошенники предлагают подвезти человека до банка на машине или оплатить такси. Человек, находясь под воздействием слов мошенников, снимает деньги, переводит на счет, предоставленный мошенниками. Далее мошенники убеждают жертву в дальнейшем ее сопровождении и возврате денежных средств после поимки преступника.

3.5. Запугивание

Суть мошеннического приема: мошенники звонят по телефону и ошарашивают человека какой-то неприятной новостью, вводят в состояние стресса, безысходности, запугивая его, чтобы в состоянии страха отключить критическое и логическое мышление, чтобы человек принял решение, которое нужно мошенникам. Далее мошенники подсказывают выход из ситуации, решение которой требует денежных переводов, оплат, покупок.

Действия мошенников направлены на:

запугивание человека выдуманными штрафами и санкциями (например, «пропустил срок поверки счетчиков», «договор расторгнут, срочно перезвоните по этому номеру или пройдите по ссылке», «карта заблокирована, перезвоните по этому номеру» и т. п.);

пробуждение чувства страха за родных (например, «внук попал в аварию», «на вашей дочери сглаз», «у вас плохие анализы – обнаружен рак» и т. п.).

3.6. Имитация заботы

Суть мошеннического приема: мошенники, чтобы завоевать доверие пожилых людей, по телефону представляются обычными людьми, приятными в общении, доброжелательными, коммуникабельными. Данные приемы используют аферисты, представляющиеся, как правило, продавцами разного рода товаров и услуг для здоровья, правильного питания. В этом случае их крайне тяжело заподозрить в обмане, потому то они правдоподобно и с энтузиазмом рассказывают о предлагаемых продуктах, товарах. Если мошенник чувствует, что гражданин сомневается или не хочет расстаться с деньгами (купить товар, получить услугу), то в действие вступают приемы запугивания, обещаний «всего и сразу», напористости, неожиданности. Мошенники – хорошие актеры и психологи, в своих действиях для получения максимального результата, они используют разные коммуникативные приемы, нейролингвистическое программирование, гипноз.

Действия мошенников «добродетельны», направлены на «заботу о ближнем»: они предлагают БАД, лекарственные препараты, медицинские приборы с «большой выгодой», «понимая, что у пенсионера небольшой доход». При этом продавцы товара якобы сами пользовались этими «исцеляющими продуктами» или товарами, которые помогли вылечиться за короткий срок. Гражданин проникается «открытостью» и «внимательностью» продавца, а также «результативностью» предлагаемого продукта, не чувствуя подвоха и плохого умысла, с радостью покупает товар-пустышку, переводя деньги мошеннику.

ГЛАВА 4. ПСИХОЛОГИЧЕСКИЕ ЗАЦЕПКИ МОШЕННИКОВ

Мошенники используют психологические зацепки и «болевые точки», чтобы привлечь побольше жертв в свои сети; пожилые люди являются самым «жирным уловом» в их махинациях.

Какие психологические зацепки дают преступникам привлекать большое число пенсионеров в мошеннические схемы?

4.1. Доверчивость пожилых людей

Граждане пожилого возраста – это люди, которые, как правило, воспитывались с детства в условиях другой эпохи – советской, в которой было доверительное отношение к информации в газете, на радио, на телевидении как основным инструментам связи с миром. Пожилые люди, особенно проживающие в селах и небольших городах, зачастую имеют большие

сложности в пользовании гаджетами, чтобы быть достаточно просвещенными в вопросах безопасности, знать о возможном мошенничестве, следить за видами мошеннических схем и способах их предотвращения. Поэтому мошенники активно используют рекламу в газетах, на радио и телевидении, рассчитывая на людей старшего поколения.

4.2. Ожидание вознаграждения от государства

Граждане пожилого возраста, долгое время проработавшие на благо государства, ожидают вознаграждения за их вклад в развитие страны, таких как надбавка к пенсии, почетные звания, получение квартиры, ветеранские награды, выгодные банковские счета и т. п. Поэтому мошенники обращаются к пожилым людям с предложениями якобы от государства, на которые те могут повестись, и заманивают в финансовые пирамиды, обещают надбавки к пенсии, награды, получение квартир и др.

4.3. Желание быть здоровым

Граждане пожилого возраста, как правило, имеют хронические заболевания или целый «букет» заболеваний. Они максимально сосредоточены на своем здоровье, хотят быть активными и здоровыми, в связи с чем и принимают за «чистую монету» обещания о действии лекарственных средств, БАД, медицинских приборов и т. п., предложенных мошенниками.

4.4. Тревожность

Пожилые люди в большей степени предрасположены к тревожности как в биологическом, так и в социальном плане, связанной с уходом на пенсию, ухудшением состояния здоровья, ощущением бесполезности, зависимости и беспомощности перед окружающим миром. Такие люди часто попадаются на крючок к мошенникам, которые умеют использовать их страхи в своих целях.

4.5. Одиночество

Пожилой человек по ряду обстоятельств может проживать один, и тогда это становится хорошей приманкой для мошенников, потому что в одиночестве человеку не с кем поговорить, а востребованность в коммуникациях и добром слове воспринимается очень высока Порой одиноко проживающий пожилой человек стесняется сказать родным, знакомым, что попался на удочку мошенников. Эти чувства являются

непреодолимой преградой в общении и мешают поделиться с родными своими трудностями, поэтому пострадавший предпочитает сам выпутываться из долговой ямы, куда попал по вине мошенников. Поэтому мошенники всячески этим пользуются при заманивании одиноких пожилых людей в свои «сети»: они улыбаются, разговаривают внимательно, уважительно, обязательно поинтересуются здоровьем, посочувствуют – и быстро добиваются полного расположения пожилого человека. А дальше уже могут предлагать ему все, что угодно: от «волшебных пилюль» до ренты на «выгодных условиях».

4.6. Сложное финансовое положение

Большинство пожилых людей живут скромно и, как правило, экономят на всем: в магазинах ищут товары со скидками, выбирают магазины, где основные продукты немного дешевле, даже если для этого приходится далеко ехать. Поэтому для пенсионеров слова «скидка», «акция», «распродажа» становятся ключевыми, и мошенники активно используют их, предлагая «выгодные» инвестиции, дорогие вещи/товары/продукты «за полцены». Здесь срабатывает краткосрочность действия акции: «скидка» действует только сегодня (несколько часов). А позже пожилой человек разберется, что купленный товар – китайская дешевка, за которую он заплатил намного дороже, к тому же совсем ему не нужная.

4.7. Подражание

Пожилые люди могут быть не только доверчивыми и открытыми, но и наоборот – подозрительными. В этом случае мошенникам очень помогает ссылка на то, что данный товар/услугу купили другие пожилые граждане и очень довольны покупкой: мошенники приводят якобы конкретные случаи таких приобретений «тетеньки из соседнего подъезда», чье здоровье «улучшилось в разы». При этом мошенники показывают ссылку, переходя по которой пожилой человек может сам убедиться в эффективности того или иного товара/услуги. И тогда гражданин, забыв о своих сомнениях, приобретает у мошенников товар/услугу.

4.8. Тяжелая жизненная ситуация

В тяжелой жизненной ситуации могут оказаться люди разных возрастов. Однако для пожилого человека такая ситуация оказывается наиболее критичной: проблемы в семье, смерь близкого человека, пожар, инвалидность

и т. п. Мошенники под каждую жизненную ситуацию, возникшую у пожилого человека, подбирают соответствующие схемы махинаций.

4.9. Вера в чудеса

Зачастую пожилой человек перед лицом болезней и смерти задумывается о духовности, верит в чудеса излечения от серьезных болезней и продления жизни. На этой почве возникает ни на чем не основанная вера в медицинские «чудо»-препараты, «волшебные» приборы, травки, гадания, снятие порчи, иные альтернативные методы лечения. Такие махинации, как правила, проворачивают и так называемые экстрасенсы, колдуны, знахари.

ГЛАВА 5. ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСТВА

5.1. Правила защиты от мошенничества для граждан пожилого возраста)

Пожилые граждане являются основной мишенью для мошенников, потому что они доверчивы и не знают всех нюансов работы банковских структур и других организаций, Интернет-сервисов. Чтобы обезопасить пожилых людей от подозрительных звонков, напоминайте им об основных правилах безопасности:

1) никому не сообщайте реквизиты паспорта и банковских карт (код SVV с обратной стороны карты, коды из СМС, данные для входа в онлайн-банк);

2) используйте только официальные сервисы банков, платежных систем и торговых площадок для перевода денег;

3) звоните в банки и государственные структуры только по их официальным номерам;

4) не перезванивайте по незнакомым номерам, даже если вам поступил звонок, который был сразу же сброшен; сбросьте звонок и перезвоните сами на официальный номер той организации, от которой якобы поступил первичный вызов (например, звонок из банка о блокировке карты или других проблемах с ней);

5) не звоните по номеру, с которого отправлен СМС: вполне возможно, что в этом случае с вашего телефона будет автоматически снята крупная сумма;

6) не соглашайтесь на получение какой-либо выплаты, а поищите информацию о ней в других официальных источниках;

7) заблокируйте банковскую карту и запросите ее перевыпуск, если потеряли карту или сообщили подозрительному человеку ее номер.

8) разговаривайте очень осторожно при звонках с человеком, звонящим из незнакомого номера; не используйте в разговоре с мошенниками фразы: «да», «нет», «согласен», «подтверждаю» и т. п.;

9) не сообщайте персональную информацию о себе;

10) блокируйте подозрительные и рекламные номера;

11) договоритесь с родственниками и близкими о создании контрольного вопроса (слова), чтобы при звонке/СМС-сообщении удостовериться, что звонит не мошенник, не робот;

12) не реагируйте ни на какие ссылки в незнакомых сообщениях, ссылки для скачивания стороннего программного обеспечения или перехода на какие-либо веб-страницы с целью получения, (например, выигрыша в лотерее, особенно, если ни в каком конкурсе вы не участвовали);

13) не переводите деньги по сообщениям и по звонкам от незнакомых номеров, поступивших якобы от лица близких родственников о попадании в сложную ситуацию (авария, пожар, болезнь, полиция, кража и др.);

14) не переводите полученные денежные средства на ваш счет самостоятельно, если вам случайно перевели деньги (например, на мобильный телефон), в этом случае необходимо обратиться в банк с заявлением об ошибочном зачислении;

15) задавайте уточняющие вопросы якобы близкому родственнику или знакомому, который попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела и ему нужны деньги для урегулирования дела: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т. е. задавать вопросы, ответы на которые знаете только вы оба;

16) задавайте утоняющие вопросы полицейскому, если он вам звонит, чтобы сообщить о неприятной ситуации, совершенной вашими знакомыми/родственниками: из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда;

17) не открывайте двери незнакомым людям, что бы они ни предлагали, что бы ни обещали, чем бы ни пугали. Если незнакомцы за дверью настаивают, можно позвонить в полицию;

18) повесьте на видном месте список телефонов коммунальных, социальных, аварийных служб, полиции, районной поликлиники, газовой службы, горячей линии банка и мобильного оператора, чтобы в случае сомнений самим звонить туда; запишите рядом со списком телефонных

номеров завершающую разговор фразу, например: «Спасибо за информацию, я вам перезвоню», чтобы пожилой человек, на которого будет оказано сильнейшее психологическое давление, не забыл эти слова и смог повесить трубку;

19) делайте все нужные покупки в проверенных магазинах, где обозначена цена, есть гарантия качества и не подошедший товар можно вернуть;

20) не занимайтесь самолечением и самостоятельно, под влиянием рекламы или чьих-то советов, не покупайте медицинские препараты и приборы. Не бывает лекарств и приборов, которые способны вылечить все болезни, а тем более – старость. Обещать это могут только мошенники;

21) не открывайте микрокредиты, не обращайтесь за микрозаймами: это начало кабалы, из которой трудно выбраться;

22) принимайте участие в акциях, конкурсах, лотереях и викторинах только в присутствии доверенных лиц (родных, близких), потому что для этого требуется заполнить анкету, указать свои паспортные данные и расписаться. Недобросовестные люди могут воспользоваться этим для заключения кредитного договора;

23) не ведитесь на предложения что-то выиграть, бесплатно получить приз или подарок. Мошенники завлекают обещаниями, а сами выманивают деньги. Бесплатных товаров не бывает, как и конкурсов с простыми вопросами и ценными призами;

24) советуйтесь с родными и близкими при принятии серьезных решений, обдумав все как следует;

25) не подписывайте договоры и другие документы, не прочитав их, даже если менеджер торопит. Если договор подписан, нельзя допускать замены документа или каких-то его страниц;

26) входите на сайт самостоятельно «вручную», а не по ссылкам, это наиболее безопасный способ, потому что фишинговые письма перенаправляют получателя на вредоносный сайт или мошенническую версию сайта банка, а некоторые из них предназначены для сбора вашего имени пользователя, пароля и другой личной информации.

5.2. Правила защиты от мошенничества (для родственников пожилых людей)

Родственники являются самыми близкими людьми для пожилых граждан и обязаны предостеречь своих доверчивых и малоинформированных родных от мошеннических действий. Для этого рекомендуются следующие

правила защиты от мошенников для родственников, в первую очередь, родственников граждан престарелого возраста, требующих особой защиты:

1) чаще звоните, приходите в гости к пожилым родственникам и спрашивайте, как у них дела. *(Тогда они скорее послушают вас, чем попадутся на уловки аферистов);*

2) рассказы о мошенниках помогают плохо: новые схемы появляются каждый день и бабушки/дедушки не всегда их распознают. *(Не стоит и запирать пенсионера дома – он не заключенный);*

3) почистите бабушкин почтовый ящик и установите на него замок. Уберите «хлам» с балкона и поставьте новую входную дверь. *(Так аферисты не догадаются, что в квартире живет пенсионер);*

4) убедите пожилого родственника получать деньги на банковскую карту, а не наличными у почтальона;

5) привяжите бабушкину/дедушкину банковскую карту к отдельному номеру и заблокируйте на нем исходящие СМС;

6) запомните (запишите) и сотрите трехзначный код на обороте банковской карты пенсионера и установите лимит на снятие наличных;

7) убедите пожилого родственника спрятать паспорт подальше (если есть возможность, уберите в сейф в его квартире) или уберите сами (когда документ понадобится, вы его предоставите или сообщите код от сейфа).

8) контролируйте звонки и расходы пожилого родственника через приложения банков и мобильных операторов;

9) установите в квартире пенсионера видеоглазок (работает как звонок, фотографирует посетителей), внешнюю камеру или сигнализацию. Сигнализации бывают с веб-камерами, датчиками движения и брелоками с тревожной кнопкой. Если что-то случится, вам поступит звонок.

4.2. Средства защиты от мошенничества

Аппаратные средства защиты от телефонных мошенников

Службы безопасности банков активно используют аппаратные средства защиты от мошенников, в том числе систему кибербезопасности с использованием искусственного интеллекта. Например, в базу данных ведущих банков включены известные действующие мошеннические колл-центры и более 150 преступных схем, и в случае подозрения о мошеннической операции на экране онлайн-банкинга появляется красный транспарант и операция блокируется.

Определители номеров мошенников

В Интернете существует достаточно много сервисов для того, чтобы определить если не владельца конкретного телефонного номера, то, по

крайней мере, город или страну, откуда поступил звонок. Большая часть таких сообщений отправляются из-за границы и мест заключения.

Чтобы определить номер конкретного владельца телефона (город или страну, откуда совершен звонок) в Интернете существует достаточно много сервисов. Самый проверенный способ не попасть к телефонным мошенникам – это произвести звонок в проверенную службу безопасности или колл-центр банка, зайти на официальный сайт той организации, откуда якобы поступил звонок, и проверить информацию.

Страхование банковских карт, счетов, вкладов

Основными целями системы страхования вкладов являются: защита прав и законных интересов вкладчиков банков Российской Федерации; укрепление доверия к банковской системе Российской Федерации и стимулирование привлечения денежных средств в банковскую систему Российской Федерации. Страховка компенсирует потерю денег на картах и счетах банка по вине мошенников. В полис также входит защита от грабежа при снятии денег в банкомате.

Установка двухфакторной аутентификации (входа)

Двухфакторная аутентификация – это дополнительный уровень безопасности аккаунта человека, который гарантирует, что доступ в аккаунту человека сможет получить только сам человек, даже если пароль известен еще кому-то. Аутентификация по телефону – это метод двухфакторной аутентификация премиум-класса, обеспечивающий надежное подтверждение личности с помощью кода, который передается на телефон в виде текстового сообщения или голосового вызова по запросу получателя. Иначе говоря, двухфакторная аутентификация является проверкой подлинности человека, процесса или устройства.

Установка антивирусных программ на гаджеты

Антивирусные программы помогают защититься от фишинговых сайтов и опасных сетей. Если программа заподозрит угрозу, то пришлет уведомление, что на этой веб-странице нельзя вводить персональные данные или что стоит подключиться к другому Wi-Fi. Антивирус на современном смартфоне играет важную роль в защите данных и обеспечении безопасности устройства.

Подключение информирования от банка при совершении операций

Информированность банка о совершенных платежах (уведомления) увеличивают безопасность денежных средств.

Контрольный вопрос

Контрольный вопрос – это форма проверки подлинности пользователя, которая подтверждает его личность на основе личных знаний. Эти вопросы обычно служат вторичным методом аутентификации, часто используемым при восстановлении пароля или проверке учетной записи.

Запрет на операции с недвижимостью и кредиты

Эта мера – эффективный способ защиты своей недвижимости от мошеннических действий. После наложения запрета никто без ведома и согласия собственника не сможет продать или подарить такой объект, сдать его в аренду или отдать в залог.

Подать заявление о несовершении сделок без личного участия можно бесплатно в любом офисе МФЦ или в электронном виде через личный кабинет на Госуслугах. Чтобы установить самозапрет на кредиты, достаточно заполнить шаблонное заявление на Госуслугах или в МФЦ. Устанавливаются и отменятся самозапреты без ограничений и бесплатно.

ПРИЛОЖЕНИЕ

Департамент социального развития
Ханты-Мансийского автономного округа – Югры

Бюджетное учреждение
Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»

ОСНОВЫ БЕЗОПАСНОЙ ЖИЗНИ ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

ЭЛЕКТРОННОЕ МЕТОДИЧЕСКОЕ ПОСОБИЕ

Бюджетное учреждение
Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»
Сургут, 2024

Дорогие граждане!

Представляем Вашему вниманию электронное методическое пособие, адресованное людям старшего возраста с большим жизненным опытом.

На первый взгляд кажется, что они знают о жизни все и сами могут научить кого угодно. Но в реальности именно представители старшего поколения чаще всего становятся жертвами мошенников. Наверное, каждый может вспомнить случаи, когда вам или вашим близким предлагали «волшебные таблетки», сковородки и кастрюли «в подарок», обещали большие скидки на товары и услуги и т. д. Так действуют мошенники, цель которых – получить ваши деньги любой ценой. Для этого они используют любые средства: от уговоров и обещаний до запугивания.

Как показывает практика, наказать виновных, добиться справедливости и вернуть утраченные средства практически невозможно. Лучше предотвратить угрозу: предупрежден – значит вооружен.

КОРОТКО О МОШЕННИЧЕСТВЕ

Граждане пожилого возраста – самые уязвимые жертвы мошенников

Жертвой мошенников может стать кто угодно, 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. Есть целая категория аферистов, которые специализируются на пенсионерах.

Мошенничество 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 (ст. 159 УК РФ).

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 своих 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 пожилые люди сами называют данные для перевода денег.

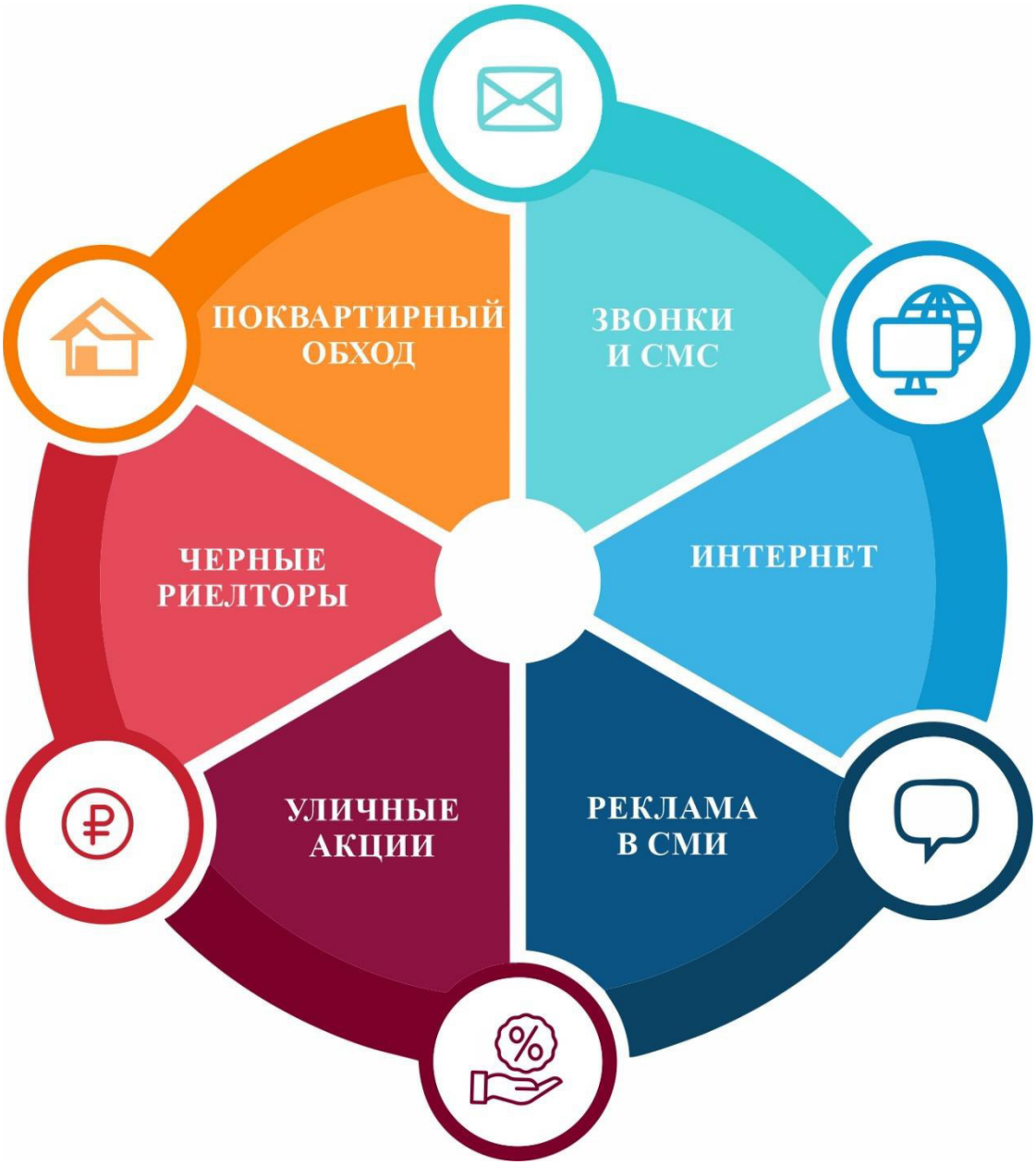
Чаще всего пенсионеров обманывают с помощью электронных платежей или используют их персональные данные.

Мошенничество с электронными платежами: человек теряет деньги через банковские карты, виртуальные кошельки. Например, если ему звонят якобы из банка, спрашивают данные карты и воруют деньги со счета (ст. 159.3 УК РФ).

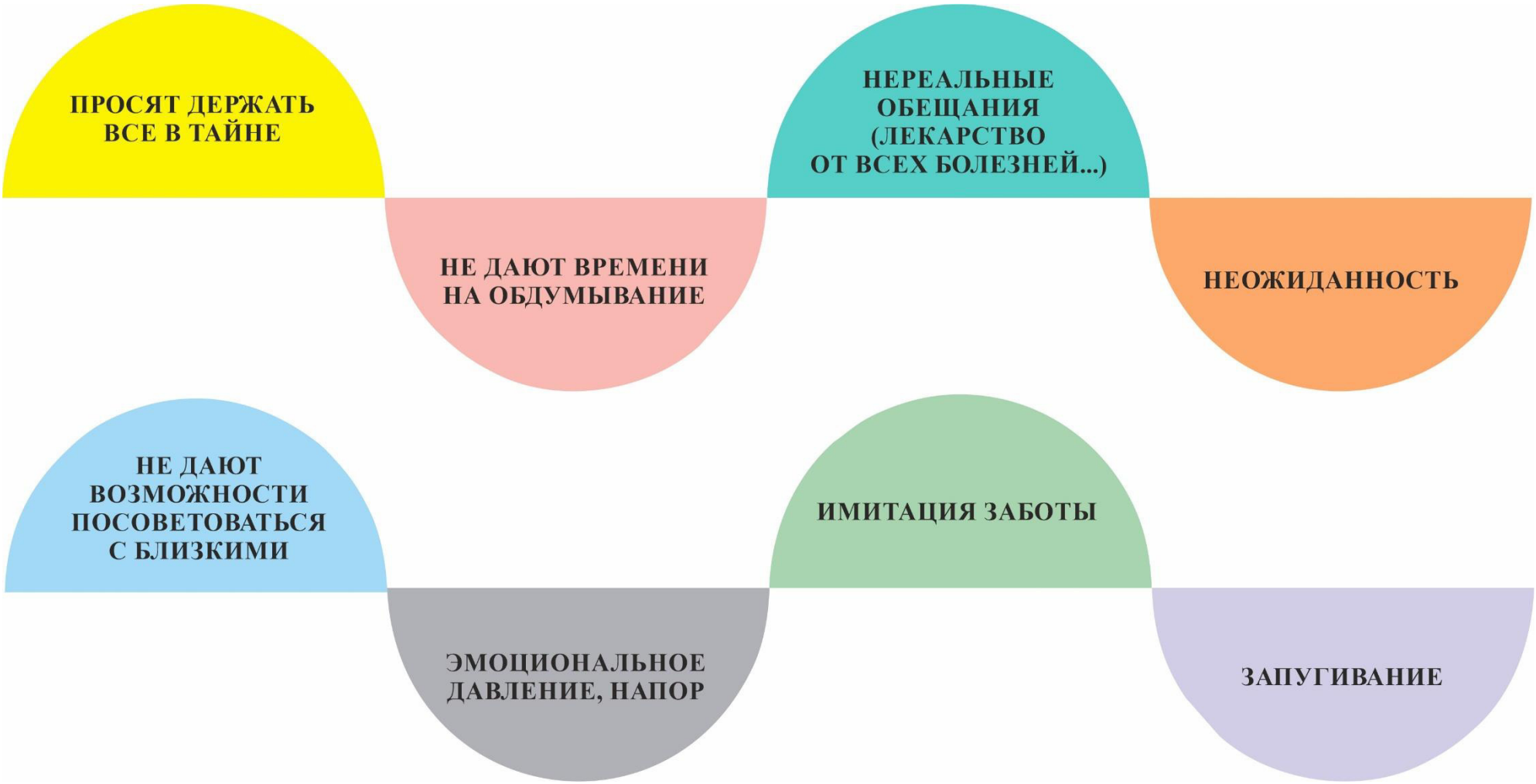
Мошенничество с персональными данными: персональные данные похищают или изменяют, чтобы получить права на имущество. Например, оформляют за пенсионера электронную подпись и сами подписывают договор купли-продажи его квартиры (ст. 159.6 УК РФ).

В настоящее время можно легко и без особых проблем установить «запрет на действия с недвижимостью без личного участия» собственника, обратившись в АУ «Многофункциональный центр Югры» (филиал по месту жительства).

ВИДЫ МОШЕННИЧЕСТВА



ОСНОВНЫЕ ПРИЕМЫ МОШЕННИКОВ



ВЫ В ЗОНЕ РИСКА, если:

верите в чудеса

слишком доверчивые

испытываете одиночество

желаете вернуть былое здоровье

испытываете чувство тревожности

оказались в сложной жизненной ситуации

находитесь в тяжелом материальном положении

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

- БУДЬТЕ БДИТЕЛЬНЫ
- СОВЕТУЙТЕСЬ С БЛИЗКИМИ
- ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ
- НЕ СТЕСНЯЙТЕСЬ ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ И ИНФОРМАЦИЕЙ В ПОЛИЦИЮ, АДМИНИСТРАЦИЮ И ДРУГИЕ СЛУЖБЫ
- НЕ ОТКРЫВАЙТЕ ДВЕРЬ НЕЗНАКОМЫМ, НЕ РАССКАЗЫВАЙТЕ О СЕБЕ ПОСТОРОННИМ ЛЮДЯМ
- НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЫМИ ЛЮДЬМИ ПО ТЕЛЕФОНУ
- НЕ ДАВАЙТЕ ПОСТОРОННИМ СВОИ Ф.И.О., АДРЕС, ДАННЫЕ ПАСПОРТА И БАНКОВСКИХ КАРТ
- НЕ ЗАНИМАЙТЕСЬ САМОЛЕЧЕНИЕМ, ВСЕ ЛЕКАРСТВЕННЫЕ ПРЕПАРАТЫ И МЕДИЦИНСКИЕ ПРИБОРЫ ПРИОБРЕТАЙТЕ В АПТЕКЕ ПО НАЗНАЧЕНИЮ ВРАЧА
- НЕ ПОКУПАЙТЕ ТОВАРЫ С РУК, НЕ ВЕРЬТЕ РЕКЛАМЕ И ОБЕЩАНИЯМ
- НЕ ОФОРМЛЯЙТЕ НА СВОЕ ИМЯ НИКАКИЕ БАНКОВСКИЕ КАРТЫ, КРОМЕ ПЕНСИОННОЙ
- НЕ БЕРИТЕ КРЕДИТЫ И МИКРОЗАЙМЫ
- НЕ ПОДПИСЫВАЙТЕ НИКАКИХ ДОКУМЕНТОВ, ПРЕДВАРИТЕЛЬНО НЕ ПРОЧИТАВ ИХ И НЕ ПОСОВЕТОВАВШИСЬ С БЛИЗКИМИ
- НИКОМУ НЕ СООБЩАЙТЕ ПИН-КОД, CVV-КОД И ДРУГИЕ ДАННЫЕ СВОЕЙ БАНКОВСКОЙ КАРТЫ
- НЕ ПРИНИМАЙТЕ ПОСПЕШНЫХ РЕШЕНИЙ

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО

ПО 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…»

«Ваша карта заблокирована, для разблокировки отправьте в ответ …»

Что нужно мошенникам: чтобы гражданин отправил деньги или данные карты через СМС.

Что не нужно делать: блокировать 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: напоминания о записи к врачу, уведомления о зачислении пенсии и списаниях по карте.

Что делать: когда гражданин пожилого возраста оформляет в банке карту, можно привязать ее к отдельному номеру телефона. Можно настроить смартфон так, чтобы он принимал СМС на обе карты, а отвечать можно было с одной – не привязанной к счету, или купить для нее отдельный телефон. Пенсионер не будет проверять его постоянно, а у кодов подтверждения короткий срок действия.

Пример из жизни. 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 и без внучки не попалась бы на развод.


НЕ ГОВОРИ
НИКОГДА И НИКОМУ
коды из СМС
трехзначный код на оборотной стороне карты (CVV/CVC)
PIN-код
пароли/логины к банковскому приложению и онлайн-банку
кодовое слово
персональные данные
ЗВОНЯТ
из банка, полиции или другой организации?
УБЕДИТЕСЬ,
что звонят не телефонные мошенники!
Банк России
Финансовая культура

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА?

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

КАК ЗАЩИТИТЬ СВОИ ФИНАНСЫ

Узнай больше на **fincult.info**

ПО ТЕЛЕФОНУ

Что говорят:

«Мама/папа/бабушка/дедушка, я попал в беду! Нужны деньги на лечение/взятку/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 сбил человека, нужны деньги для пострадавшего»

«Вам положены компенсации/выплаты/надбавки/перечисления из бюджета. Нужно только оплатить комиссию»

«Это из поликлиники. У вас плохой диагноз – нужны лекарства и «волшебные» медицинские приборы, у нас они в наличии»

«Поучаствуйте в беспроигрышной лотерее»

«Вчера к вам приезжал курьер с доставкой, у нас строгая отчетность, и для нее необходимо продиктовать цифры из СМС-сообщения»

Что нужно мошенникам: данные карты для перевода денег (номер, срок действия и CVV – трехзначный код на обратной стороне карты). Граждане сами диктуют информацию по телефону.

Что не нужно делать: отказываться от банковских карт. Деньги в банке защищены лучше, чем наличные под матрасом.

Что делать: стереть с обратной стороны карты трехзначный код. Картой можно будет платить в магазинах, снимать с нее деньги и пополнять счет. Но без кода человек не переведет аферистам деньги, ничего не купит в сомнительном телемагазине и не сделает ставку в онлайн-лотерее. Для этого придется найти, где он записан,

или позвонить тому, у кого из родственников он сохранен, и спросить код. А родственник как раз и спросит, зачем он нужен.

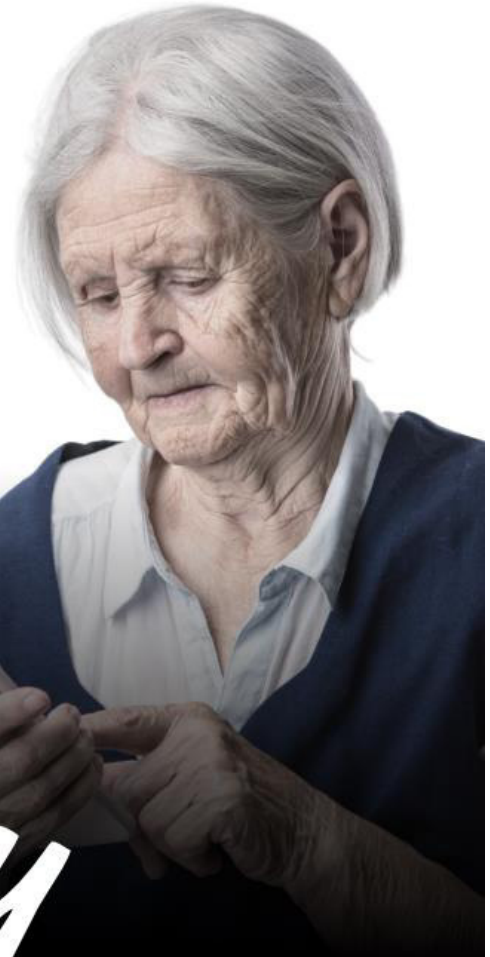
Некоторые мошенники звонят и убеждают принести деньги наличными. Лучше отказаться от наличных в повседневной жизни, а снятие с карты ограничить несколькими тысячами рублей. Это можно сделать в мобильном приложении или в отделении банка, если прийти туда с пожилым родственником. Когда пенсионер не сможет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

Также не нужно принимать доставки, которые вы не заказывали (цветы, пицца и т. д.).

Пример из жизни. Дедушке 74 лет позвонили и сказали, что его сын сбил человека. Пострадавший якобы в порядке, но за молчание просит 20 000 руб. Дедушка пошел к банкомату, но тот не работал. Тогда он позвонил внучке и спросил, где еще есть банкомат, – она и распознала обман. Если бы банкомат работал, дедушка лишился бы денег. Еще в этом случае помогло бы ограничение на снятие крупных сумм.

Как распознать мошенника?

- **Просят** данные банковской карты, пароли и коды из СМС
- **Предлагают** перевести деньги на «безопасный счет»
- **Гарантируют** супердоход от инвестиций
- **Представляются** якобы сотрудниками банка или полиции
- **Пугают** взломом Госуслуг



Клади трубку

Без разговоров.
Это мошенники!

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

В КВАРТИРАХ

Что говорят:

«Мы из социальной службы, вам положена консультация»

«Мы из ЖЭУ, нужно осуществить поверку/проверку счетчиков»

«Мы из оконной фирмы, давайте отрегулируем окна»

«В доме тараканы и клопы, требуется санобработка»

«Для пенсионеров у нас техника/лекарства/посуда со скидкой»

«Вам положено бесплатное медицинское обследование на дому»

«Подпишите петицию за справедливость. Надпись «кредитный договор» – это просто форма такая…»

Что нужно мошенникам: вынудить подписать кредитный договор, навязать 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 бабушка/дедушка, приведите в порядок почтовый ящик и входную дверь, переведите пенсию на карту и уберите лишнее с балкона. Еще можно приклеить на дверь наклейку, что объект охраняется.

В старых домах почтовые ящики часто без замков, и из них легко достать содержимое. Из платежных извещений мошенники 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 человек. Еще в документах бывает информация о льготах. Выход – установить замок на почтовый ящик и следить, чтобы там не скапливалась корреспонденция.

Еще два возможных признака, что в квартире живет пожилой человек: много вещей на балконе и обшарпанная дверь. Убедите родных не хранить на балконе «старье» и не сушить там половики. И попросите родных поставить хотя бы недорогую железную дверь. Внешне она не будет сильно отличаться от дорогих.

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).

Мошенники не любят места, где есть камеры и в любой момент может появиться полиция. Можно купить муляжи камер и наклейки с надписью «ведется видеонаблюдение». Они яркие и бросаются в глаза («охраняется полицией», «ведется видеонаблюдение»). Также можно повесить в подъезде плакат с телефоном участкового и графиком приема.

Пример из жизни. Бабушка 83 лет шла по улице, а рядом женщина упала на землю. Бабушка подошла к ней, а та сказала: «Я ясновидящая. Мне было видение, что с вашим самым дорогим человеком случится беда. От этого мне стало плохо. Покажите мне фото, и я сниму порчу». Бабушка пригласила ее в квартиру и дала фото своей дочери. Мошенница сказала, что ей нужны все бабушкины деньги, чтобы снять сглаз. Но у пенсионерки была только карта. Аферистка дала номер своей карты и попросила перевести все, что есть, но никому об этом не рассказывать, а то процедура не подействует. Мошенница ушла, а бабушка не удержалась и позвонила дочери – сообщить про порчу. Денег мошенница не дождалась. Если бы мошенница увидела в подъезде наклейки о видеонаблюдении, возможно, у нее нашлись бы другие дела. Смотреть в полиции видеозаписи своих подвигов преступники не любят.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

1 **ПРОВЕРЬТЕ СРОК ПОВЕРКИ СЧЕТЧИКОВ:**

- **В ВЕРХНЕЙ ЧАСТИ ЕПД**
- **В ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ ПРИБОРА**
- **ПРИ ЛИЧНОМ ПОСЕЩЕНИИ ЦЕНТРА ГОСУСЛУГ «МОИ ДОКУМЕНТЫ»**

Если срок поверки не наступил, то проверять и заменять счетчик нет необходимости. Если вас уверяют в обратном – скорее всего, это мошенники.

Если подошел срок поверки, выберите аккредитованную организацию или управляющую компанию с соответствующим разрешением, или обратитесь в организацию, которая установила вам счетчики.

2 **УТОЧНИТЕ У ЗВОНЯЩЕГО НАЗВАНИЕ ОРГАНИЗАЦИИ, ОБЯЗАТЕЛЬНО ЗАПИШИТЕ ЕГО И СВЕРЬТЕ ДАННЫЕ С «ЧЕРНЫМ СПИСКОМ» НЕДОБРОСОВЕСТНЫХ ПОСТАВЩИКОВ УСЛУГ НА САЙТЕ ФАС fas.gov.ru**

3 **ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, ОБРАТИТЕСЬ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ**

В МЕДИЦИНСКИХ И ТОРГОВЫХ ЦЕНТРАХ

Что говорят:

«Для вас есть заем 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»

Что нужно мошенникам: вынудить подписать кабальный договор купли-продажи, кредитный договор или «развести» на большие траты.

Что делать. От такого мошенничества труднее всего защититься. Фирмы аферистов часто официально зарегистрированы и даже платят налоги. Почти всегда они подписывают с пенсионером договор, а при его наличии нет оснований для возбуждения уголовного дела. В этом случае 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. Главное – не носить с собой паспорт: без него невозможно заключать договоры. Можно просто положить его подальше, рядом с документами на квартиру, например.

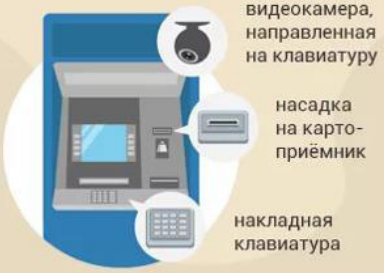
Пример из жизни. В торговом центре женщине предложили полежать на ортопедическом чудо-матрасе. Он стоил 30 000 руб., и ее убедили купить его в кредит. Оказалось, ставка – 10% ежемесячно. Женщина уже год ходит по судам, чтобы расторгнуть кабальный договор. Если бы у нее не было с собой паспорта, она бы не оформила кредит. Паспортные данные пенсионеры редко помнят.

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

МОШЕННИКИ ПРЕДЛАГАЮТ КОМПЕНСАЦИИ ЗА ЛЕКАРСТВА И БАДЫ

Как не стать жертвой мошенников, снимая деньги в банкомате?

Пользуйтесь банкоматами в фойе банков, крупных ТРЦ



Проверяйте, нет ли у банкомата подозрительных деталей

Прикрывайте клавиатуру рукой, когда набираете PIN-код

Сохраняйте чеки, чтобы свериться с историей платежей на Kaspi.kz

Никогда никому не сообщайте PIN-код, CVV2 и срок действия карты

Сделайте репост, расскажите друзьям!

Схема мошенничества с банковской картой в кафе, барах, магазинах

Клиент отдает карту для оплаты в руки официанту (бармену, продавцу)

Работник-мошенник уносит карту и фотографирует ее реквизиты

Спустя время он совершает онлайн-покупки, а с карты клиента списываются суммы

Как предотвратить:

Не передавать карту третьим лицам (в том числе фото карты)

Не показывать CVV-код

Попросить принести POS-терминал или пройти к кассе для оплаты

Держать закрытым доступ для покупок в интернете

Не игнорировать сообщения от банка о списании денег

Сделайте репост, поделитесь с друзьями!

ПАМЯТКА ДЛЯ РОДСТВЕННИКОВ ПОЖИЛЫХ ЛЮДЕЙ

КАК ЗАЩИТИТЬ ПОЖИЛОГО РОДСТВЕННИКА ОТ МОШЕННИКОВ

1. Почаще звоните, приходите в гости к пожилым родственникам и спрашивайте, как у них дела. *(Тогда они скорее послушают вас, чем попадутся на уловки аферистов.)*

2. Рассказы о мошенниках помогают плохо: новые схемы появляются каждый день и бабушки/дедушки не всегда их распознают. *(Но не стоит и запирать пожилого человека дома: он не заключенный.)*

3. Почистите бабушкин/дедушкин почтовый ящик и установите на него замок. Уберите лишние вещи с балкона и поставьте новую входную дверь. *(Так аферисты не догадаются, что в квартире живет одинокий пожилой человек.)*

4. Убедите пожилого родственника получать пенсию на банковскую карту, а не наличными у почтальона.

5. Привяжите банковскую карту пожилого родственника к отдельному номеру и заблокируйте на нем исходящие СМС.

6. Запомните (запишите) и сотрите трехзначный код на обороте банковской карты пожилого родственника. Установите лимит на снятие наличных.

7. Убедите пожилого родственника держать паспорт подальше (если есть возможность – уберите в сейф в его квартире). Когда документ понадобится, пусть он позвонит вам и спросит, где находится его паспорт или код от сейфа.

8. Контролируйте звонки и расходы пожилого родственника через приложения банков и мобильных операторов.

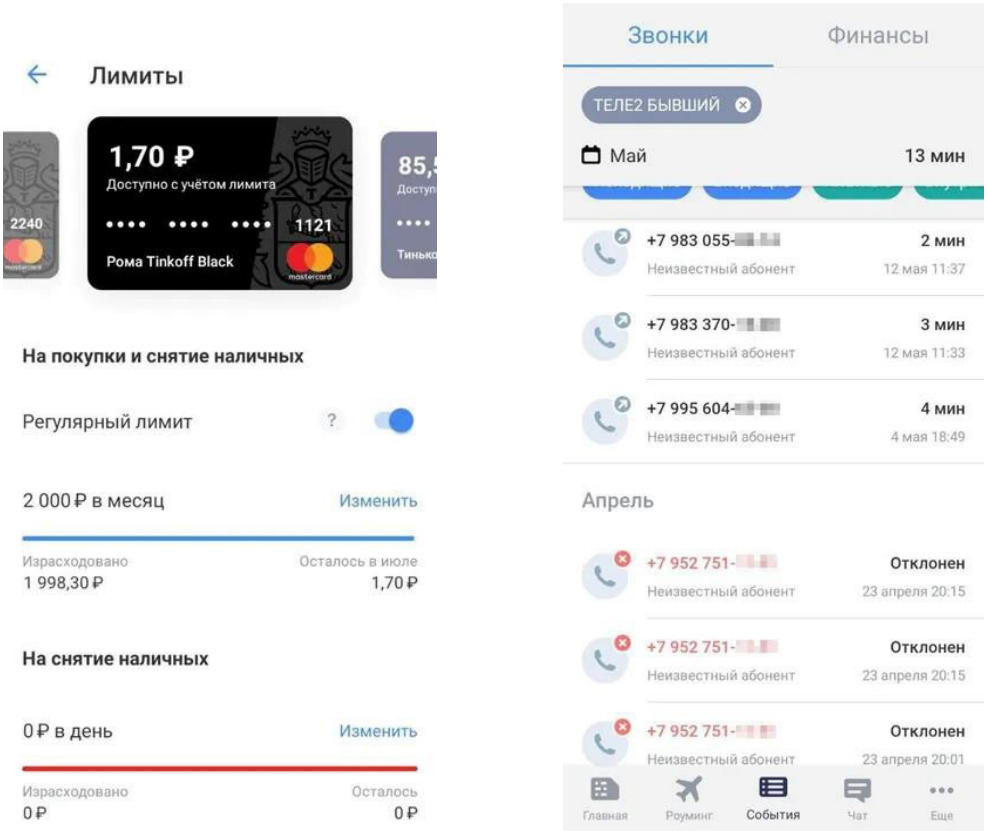
9. Установите в квартире пожилого родственника видеоглазок или сигнализацию. Сигнализации бывают с веб-камерами, датчиками движения и брелоками с тревожной кнопкой. Если что-то случится, вам поступит звонок.


Как телефонные мошенники используют для обмана WhatsApp
Входящий вызов
+7 99* *** *** **
1
Мошенник звонит с иностранного номера
Я из техподдержки
2
Представляется сотрудником банка
3
Предлагает перейти в WhatsApp «для безопасности»
4
Отправляет фото поддельных удостоверений
5
Запугивает, что у жертвы пытаются похитить средства
«безопасный счет»
6
Убеждает перевести их на «безопасный счет» и исчезает
Обратите внимание
Техподдержка банков не общается через WhatsApp
Банки Казахстана не звонят с номеров других стран
Сделайте репост, поделитесь с друзьями!

ПРОГРАММЫ И ТЕХНИКА ДЛЯ ЗАЩИТЫ

Специальные технические средства и программы помогают защитить пожилых людей. Самое эффективное средство – обычный мобильный телефон. Средство, при помощи которого совершают мошенничество, можно использовать и для защиты от него. Чем чаще вы звоните родственникам и чем больше знаете о них, тем меньше вероятность, что они попадут в беду. Но есть еще удобные мобильные приложения, сигнализации и видеоглазки.

Приложения банков и мобильных операторов можно установить на свой смартфон (например, приложение «Т-Мобайл» от Т-Банка). Так вы будете контролировать траты пожилого родственника и фиксировать звонки с незнакомых номеров. Если пожилая бабушка звонила только подругам и родственникам, а потом стала часто набирать номера телефонов неизвестных людей, стоит насторожиться.



В приложениях многих банков можно установить лимит на платежи в течение месяца. Если понадобится, его легко можно увеличить в любой момент

Автономную GSM-сигнализацию можно установить и настроить самостоятельно. В комплекте идут датчики открытия двери, веб-камера или брелок с тревожной кнопкой. В сигнализацию ставят сим-карту и задают номера родственников. Когда срабатывает датчик или кнопка, по этим номерам идет звонок.

Датчики будут срабатывать каждый раз, когда пожилой человек откроет дверь. Убедиться, что к бабушке просто пришла подруга, поможет веб-камера с передачей звука. Если увидите мошенников, позвоните бабушке и вызовите полицию.

Еще одно полезное устройство – брелок с тревожной кнопкой. Пожилой родственник сможет нажимать его каждый раз, когда к нему стучатся посторонние. Он подействует, даже если человек находится в подъезде или на улице, в 10-15 метрах от квартиры. И поможет, если ему станет плохо: проще нажать одну кнопку на брелоке, чем звонить вам по мобильному.

Видеоглазок фотографирует посетителей или снимает их на видео. Он исполняет таже функции дверного звонка, а фотографию посетителя может отправлять вам на телефон (если подключен к Интернету через Wi-Fi).

В ЗАВЕРШЕНИЕ…

Если Вам звонят с неизвестного номера, и Вы понимаете, что это не Ваши близкие, – **КЛАДИТЕ ТРУБКУ!**

Если Вам предлагают продиктовать данные банковской карты, пароли, коды из СМС, перевести деньги на «безопасный счет», представляются сотрудниками банка, полиции, ФСБ, пугают взломом Госуслуг – **КЛАДИТЕ ТРУБКУ!**

Если Вас уговаривают заключить «подозрительный» договор в торговом центре, приглашают пройти обследование прямо сейчас быстро и недорого, предлагают огромные скидки и акции – **ЗАКАНЧИВАЙТЕ РАЗГОВОР И УХОДИТЕ!**

Не принимайте поспешных решений, не делайте ничего, не посоветовавшись с близкими!

ПОЛЕЗНЫЕ ССЫЛКИ

1. Интернет-ресурс Департамента региональной безопасности ХМАО – Югры: https://deprb.admhmao.ru/profilaktika-moshennichestva/

2. Интернет-ресурсы Банка России, Минцифры России, МВД России, финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности, содержащих информационно-разъяснительные материалы по профилактике дистанционных преступлений:

МВД России:
https://мвд.рф/Videoarhiv/Socialnaja_reklama
https://мвд.рф/mvd/structure1/Upravlenija/убк
https://t.me/cyberpolice_rus

Банк России:
https://cbr.ru/protection_rights/finprosvet

Банк России г. Тюмень
https://disk.yandex.ru/d/aE-X_tMBixtXLg
https://disk.yandex.ru/d/Xn5YAs2ItvY5sw

Минцифры России:
https://www.gosuslugi.ru/cybersecurity
https://киберзож.рф/
https://выучисвоюроль.рф
https://готовкцифре.рф

3. Интернет-ресурсы финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности:

https://www.sberbank.ru/ru/person/kibrary
https://kaspersky.ru/resource-center
https://kids.kaspersky.ru/
https://rocit.ru

4. Памятки по профилактике мошенничества https://clck.ru/3ErjQC *(ссылку необходимо копировать и вставить в поисковую строку браузера)*

5. Благотворительный фонд помощи пожилым людям и инвалидам «Старость в радость» https://starikam.org/news/gor_liniya/

ВАЖНЫЕ ТЕЛЕФОНЫ

Общий телефон МЧС	112
Социальная защита	
Поликлиника	
Управляющая компания/ЖЭК	
Пенсионный фонд	
Участковый (полиция)	
Районная газовая служба	
Аварийная служба	
Банк	

Телефон горячей линии помощи пожилым людям: +7 (985) 862-95-02

с 10 до 18 по рабочим дням
(звонок платный, по тарифу вашего оператора, поэтому достаточно набрать номер, услышать гудок и положить трубку – координатор перезвонит вам и разговор будет бесплатным)

Распечатайте и запишите сюда все необходимые номера, а также внесите их в список контактов мобильного телефона!

Примечание: указанный номер принадлежит благотворительному фонду «Старость в радость», который помогает одиноким, малоимущим гражданам пожилого возраста и инвалидам по всей России https://starikam.org/.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Профилактика мошенничества: Департамент региональной безопасности Ханты-Мансийского автономного округа – Югры. – URL : https://deprb.admhmao.ru/profilaktika-moshennichestva/ (дата обращения: 15.11.2024).

2. Меры по профилактике мошенничества среди граждан. – URL : https://ako.ru/deyatelnost/mery-po-profilaktike-moshennichestva-sredi-grazhdan/obshchaya-informatsiya.php (дата обращения: 15.11.2024).

3. Методические рекомендации о предупреждении наиболее распространенных видов мошенничества. – URL : https://novo-sibirsk.ru/news/255231/ (дата обращения: 15.11.2024).

4. Рекомендации по защите от мошенников. – URL : https://chr.sledcom.ru/Rekomendacii-po-zashhite-ot-moshennikov (дата обращения: 15.11.2024).

5. Профилактика мошенничеств с использованием средств сотовой связи и Интернет-ресурсов. – URL : https://adm.gov86.org/399/688/795/3110/ (дата обращения: 15.11.2024).

Департамент социального развития
Ханты-Мансийского автономного округа – Югры

Бюджетное учреждение Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА В ОТНОШЕНИИ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА: МЕТОДИЧЕСКОЕ ПОСОБИЕ

Под общей редакцией:
И. И. Тимергазина, Е. С. Юшковой

Составители:
М. В. Пикинская, Д. М. Громова

Ответственный редактор Е. С. Юшкова
Оформление А. В. Кудрявцева

Бюджетное учреждение Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»,
628418, Тюменская обл., ХМАО – Югра, г. Сургут,
ул. Лермонтова, д. 3/1,
т./ф.: 8(3462) 550-558;
e-mail: DSRRC@admhmao.ru;
official sate: rcsur.ru