

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

**Психологические аспекты противодействия
мошенничеству: как защитить себя и свою семью**
Методические рекомендации

2025

ГКУ СОН СО «Организационно-методический центр социальной помощи»

Психологические аспекты противодействия мошенничеству: как защитить себя и свою семью/ методические рекомендации – Екатеринбург. – 2025. – 58 с.

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

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. Разобраны психологические способы действий злоумышленников, показана методика их противоправной деятельности. Определены технологические и психологические уязвимости каждого человека. Подробно освещены способы психологической защиты и техники саморегуляции эмоционального состояния. Постоянное нахождение в осознанности – залог защиты от манипулятивного воздействия.

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

Консультант Е.В. Полупанов начальник УБК ГУ МВД России по Свердловской области полковник полиции.

Консультант М.Г. Перцель, главный внештатный психотерапевт Министерства здравоохранения Свердловской области.

В разработке принимала участие группа психологов комплексных центров социального обслуживания населения, подведомственных Министерству социальной политики Свердловской области.

А.В. Вавилов, ГАУСО СО «КЦСОН Артинского района»;

Е.В. Ларичева, ГАУСО СО «КЦСОН Чкаловского района города Екатеринбурга»;

Н.Н. Камышникова, ГАУСО СО «КЦСОН города Серова»;

Н.В. Козырева, ГАУСО СО КЦСОН Тагилстроевского района города Нижний Тагил;

Е.С. Коннова, ГАУСО СО «КЦСОН Ленинского района города Нижний Тагил»;

Г.Г. Полеводова, ГАУСО СО «КЦСОН Талицкого района»;

В.В. Прахт, ГАУСО СО «КЦСОН «Золотая осень» города Нижний Тагил»;

О.Н. Суханова, ГАУСО СО «КЦСОН Ленинского района города Нижний Тагил»;

И.И. Сухоносова, ГАУСО СО «КЦСОН города Асбеста».

СОДЕРЖАНИЕ

Введение	4
Глава 1 Принятые меры на государственном уровне	5
Глава 2 Наиболее распространенные способы действий злоумышленников	8
Глава 3 Психологический разбор преступных схем	16
Глава 4 Информационный след	17
Глава 5 Контрмеры каждого человека	19
Глава 6 Почему пожилые люди часто оказываются жертвами мошеннических действий	20
Глава 7 Подростки и молодежь в зоне риска	22
Глава 8 Вербовка для совершения экстремистских действий	24
Глава 9 Психологический аспект	27
Глава 10 Наличие когнитивных искажений	29
Глава 11 Фундаментальные методы действий мошенников	31
Глава 12 Как определить человека, оказавшегося под воздействием мошенников	34
Глава 13 Способы психологической защиты, как обезопасить себя	36
Глава 14 Как защитить своих близких от воздействий мошенников	37
Глава 15 Рекомендации для защиты себя и своих близких от чужого эмоционального воздействия	40
Глава 16 Минимизация риска стать жертвой мошенничества	43
Глава 17 Противодействие манипулятивному воздействию	45
Глава 18 Техники саморегуляции эмоционального состояния	47
Заключение	52
Список использованных источников	53
Список рекомендуемой литературы	54
Приложение 1: Макет памятки	55
Приложение 2: Образцы листовок	56

Введение

Граждане России за 11 месяцев 2024 года потеряли 168 млрд рублей в результате дистанционных мошенничеств. Всего за 11 месяцев 2024 года зарегистрировано более 702 тыс. IT-преступлений, что на 14,3% больше, чем за 11 месяцев 2023 года. Вместе с тем удалось сократить прирост мошенничеств с 44% в 2023 году до 9,2% в 2024 году. Министр внутренних дел России Владимир Александрович Колокольцев на заседании коллегии МВД России по вопросу киберпреступности отметил, что с 2020 года количество посягательств с использованием информационных технологий увеличилось на треть. Доля дистанционных деяний в общем массиве сейчас приближается к 40%. В 2023 году от них пострадало полмиллиона человек. В первой половине 2024 года жертвами различных уловок преступников стали более 40 тысяч граждан преклонного возраста.

«За последние пять лет число противоправных деяний в киберпространстве увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и составляет около 40%. А по тяжким и особо тяжким составам этот показатель уже приблизился к 60%», - сказал Владимир Александрович Колокольцев на заседании Общественного совета при МВД РФ в сентябре 2024 года.

В Свердловской области за 12 месяцев 2024 года зарегистрировано около 45 тысяч преступлений, из них более 17 тысяч в сфере информационных технологий это мошенничества, кражи, завладение чужим имуществом и т.п. (за аналогичный период прошлого года около 14 тысяч). Около 7 тысяч потерпевших, из которых практически каждый третий пенсионер. Сумма хищений возросла на треть и составила более 4,2 миллиарда рублей.

Глава 1 Принятые меры на государственном уровне

Совершенствование законодательства

Правительство Российской Федерации утвердило «Концепцию государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий» (распоряжение от 30 декабря 2024 года №4154-р).

Проводится постоянная работа по совершенствованию законодательства борьбы с мошенниками. С 25 июля 2024 года вступили в силу поправки, согласно которым в определенных случаях банк отправителя должен будет вернуть полную сумму украденных средств в течение 30 дней после получения заявления от клиента. Речь идёт о переводе денег на банковские счета посредников, которые получают деньги от жертвы обмана и переводят их по цепочке мошенникам.

Кроме того, банки и платежные системы обязали проверять подозрительные операции и приостанавливать явно мошеннические действия между счетами физических лиц, даже если имеется согласие клиента. Кредитные организации смогут замораживать такие операции на 2 дня. Если клиент принял решение не под давлением мошенников и не изменил его через двое суток, деньги перечислят автоматически.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

На портале «Госуслуги» создан раздел «Кибербезопасность — это просто!» Интернет-мошенники регулярно изобретают новые схемы обмана. Однако соблюдая простые правила кибергигиены, им можно противостоять. В разделе опубликованы полезные советы и памятки гражданам защиты от киберугроз и ограждения от них себя и своей семьи [1].

Антифрод система Роскомнадзора

Создана в 2022 году, 99.6% номерной ёмкости российских операторов связи подключились к системе блокировки звонков с подменных номеров «Антифрод». Чтобы в России блокировались все звонки с подменных номеров, в 2024 году к системе присоединились еще более 600 операторов. По итогам 12 месяцев 2024 года система не пропустила более 757 млн звонков с фальшивых номеров. Эти меры необходимы для того, чтобы защитить людей от мошенников, использующих технологию подмены номера для обмана и вымогательства. Заблокированы 6,2 млн сим-карт операторов сотовой связи, оформленных с нарушением [2].

Центральный банк России

Банк России формирует базу данных «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента» на основе сведений, которые предоставляют банки и другие участники информационного обмена. Установлено время, в течение которого кредитные организации вносят реквизиты злоумышленников, поступившие из базы данных регулятора, в собственные системы противодействия подозрительным операциям. Это позволит уменьшить количество новых переводов на счета мошенников. С 22 октября 2024 года для крупных банков и значимых кредитных организаций этот срок составит два часа, а с 1 января 2025 года — один час. В отношении остальных банков установлен срок в три часа. Кроме того, Банк России уточнил требования к порядку предоставления банками сведений о возможных мошеннических операциях, в том числе для информационного обмена с правоохранительными органами. Теперь при запросе регулятора банк должен установить, совершалась операция без добровольного согласия клиента или нет, и в течение одного рабочего дня ответить Банку России, признает ли такой перевод мошенническим. Этот подход важен в случае, когда пострадавший не стал обращаться в свой банк, а сразу подал заявление в полицию.

Сведения о компаниях с признаками нелегальной деятельности, в том числе финансовых пирамид, вносятся на платформу «Знай своего клиента», это позволяет банкам оперативно учитывать степень рисков своих клиентов и их контрагентов при проведении операций. Чтобы предупредить граждан и снизить риски этот список обновляется ежедневно. Для пресечения нелегальной деятельности регулятор направляет информацию обо всех выявленных фактах в правоохранительные органы, ФАС России и иные.

Мероприятия Свердловской области

Губернатор Свердловской области Е.В. Куйвашев 15.03.2024 года утвердил «План-график мероприятий по профилактике хищений денежных средств граждан, совершенных с использованием информационно-телекоммуникационных технологий на территории Свердловской области, на 2024 год».

В учреждениях социальной защиты населения Свердловской области подготовлены планы совместной работы с территориальными отделами полиции ГУ МВД России по Свердловской области. Проводится широкий спектр профилактических мероприятий. Указанием Первого заместителя Министра социальной политики Свердловской области Е.Д. Шаповалова предписано руководителям организаций социального обслуживания **обеспечить подписку на госаблик ГКУ СОН СО «ОМЦСП» в социальной сети ВКонтакте**

(<https://vk.com/omcspso>). В еженедельной рубрике «**#БезопасныйВзгляд.**» систематически размещается актуальная информация, которая анализируется, согласуется с ГУ МВД России по Свердловской области, и рекомендуется для использования в практической работе по профилактике противоправных действий в отношении граждан. Представляются новые способы действий мошенников, а также меры противодействия.

Глава 2 Наиболее распространенные способы действий злоумышленников

Для противостояния киберугрозам, в структуре МВД России создано Управление по борьбе с противоправным использованием информационно-коммуникационных технологий. Постоянно анализируются все виды дистанционных хищений, которые применяют злоумышленники. Начальник подразделения генерал-майор полиции Филипп Николаевич Немов рассказал об актуальных мошеннических схемах, откуда может исходить угроза и как ей противостоять [3].

Схема 1. Ваш номер нужно подтвердить

Простейший обман, который чаще всего срабатывает. Идет звонок якобы от оператора сотовой связи. Мошенники пугают, что действующий договор на оказание услуг связи заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет собеседник. Достаточно продиктовать код из смс. На самом деле цель одна - получить доступ к аккаунту человека на Госуслугах. Следующий шаг - перейти по присланной ссылке, где нужно ввести еще один код. Таким образом человек не продлевает договор, который на самом деле является бессрочным,

а предоставляет данные для входа в личный кабинет на портале "Госуслуги" и всю информацию о себе, которая там хранится. Есть и другая цель, которую преследуют мошенники, представляясь оператором связи. Тот же звонок, но теперь с предложением по смене тарифного плана, подключения новых опций, замены sim-карты, либо тестирования нового оборудования. Чтобы это сделать, абонента просят продиктовать код из смс. С помощью этого кода злоумышленник получает доступ

к личному кабинету пользователя на сайте оператора мобильной связи. А уже там он настраивает переадресацию сообщений и звонков с номера жертвы на свой. Это делается для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.

Что в таком случае советуют делать киберполицейские. Вы можете обновить персональные данные, обратившись за услугой лично, - в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс). Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, размещенном на официальном сайте.

Схема 2. Предложения от лжеброкеров

Аферисты предлагают вам выгодно вложить свои средства, обещая процент гораздо выше, чем у банков. С потенциальными инвесторами они связываются через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое: нужно лишь открыть "брокерский" счет и инвестировать от 10 тысяч рублей. Доход - не меньше миллиона. Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюте. Как только у "инвестора" возникает желание вывести деньги со счета, начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить "страховку". Или ежедневное размещение валюты в "европейской ячейке" либо найти поручителя, чтобы можно было "обналичить" средства. В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы. Вариант этой мошеннической схемы - участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают при помощи писем на электронную почту. Мошенники, оформляя сообщение, копируют визуальный стиль банка, для убедительности используя те же корпоративные цвета, логотип и другие элементы. Для участия в "выгодной" кампании предлагается перейти по ссылке. После вам предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации, а также дадут доступ к специальному приложению. А уже там понадобится ввести данные своей банковской карты - с нее аферисты потом и спишут деньги.

Как отличить мошенников от реальных брокеров. Проверьте сайт инвесткомпания или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России. Откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица либо через электронный кошелек.

Схема 3. Вам предлагают выгодную работу

Аферисты размещают лжевакансии на популярных сайтах объявлений. Зарплата привлекательная, условия работы заманчивые. Но нужно пройти собеседование с будущим работодателем, и мошенники предлагают сделать это онлайн по видеозвонку.

Собеседование с будущим работодателем - волнительная процедура. Во время онлайн-встречи мошенники пользуются растерянностью соискателей и крадут личные данные. Под видом будущего работодателя они проводят собеседование,

где просят кандидата заполнить анкету прямо во время эфира. Один из ее пунктов - номер карты и другие финансовые данные. Такая информация им нужна якобы для перечисления зарплаты в будущем. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия. Понятно, что вместо пополнений с банковской карты соискателя в будущем происходят списания, а ни о какой работе речи не идет.

Находясь в поиске работы, человек может попасть в мошеннический сценарий, как подставное лицо, задействованное в нелегальных схемах по выводу средств

с банковских карт. Так можно не только потерять деньги, но и нарушить закон. Часто человек даже не осознает, что вовлечен в преступную схему. Ведь объявление

о работе, на которую он устраивается, не выглядит подозрительно.

Чего нельзя делать при трудоустройстве онлайн. Внимательно изучайте предложение от будущего работодателя и отзывы о нем. Не поддавайтесь на обещания легкого заработка с минимальной затратой собственного времени. При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное - следите за данными, доступ к которым предлагает предоставить работодатель.

Схема 4. Друг просит о помощи

Еще одна тактика кибермошенников - рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники заходят и дальше - играют на чувствах человека и сообщают, что его родственник попал

в беду. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это делает искусственный интеллект. Аферисты взламывают аккаунт пользователя. Скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана. Существует и другой сценарий - просьба проголосовать за детей в конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

Как понять, что родственник фальшивый. Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным.

Схема 5. Оплата услуг по фейковому QR-коду

Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Правда, вместо прогулки с ветерком и заряженного аккумулятора телефона можно получить пустой банковский счет. Дело в том, что такой QR-код может вести не на официальный сайт сервиса, а на поддельный ресурс, через который аферисты крадут деньги и данные карты.

Как платить, чтобы не потерять средства. Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 6. Звонки из банка

Наряду с лживыми угрозами об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операции по ней - появились и новые сценарии. Мошенники под видом специалистов техподдержки банков предлагают установить на смартфон приложение для поиска вирусов. Это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным.

Банковские работники никогда не обзванивают клиентов с предложениями что-то установить. Это можно сделать самостоятельно, обратиться за помощью к проверенным специалистам или в офис банка лично. **При подозрении можно самостоятельно выявить шпионские программы в смартфоне. Набрать комбинацию *#21# и нажать кнопку вызова, после чего на экране устройства появится информация о переадресации. Если во всех пунктах будет стоять отметка «Не переадресовано» или «Отключено», то смартфон в порядке.**

Еще один популярный сценарий - помощь в сохранении денежных средств. Аферисты под видом сотрудников Банка России сообщают человеку, что кто-то пытается похитить деньги со счета. Чтобы их спасти, надо перевести средства на «безопасный» счет в ЦБ РФ. По легенде это временная мера - на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве или в банковской ячейке.

Как проверить совершается ли звонок из банка. Пользуйтесь только официальными ресурсами финансовых организаций. Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации. Там же вы можете скачать официальные банковские приложения. Можно обратиться на **номер горячей линии Банка России 8-800-300-3000.**

Схема 7. Представляются госслужащими, руководителями организаций

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, налоговой, портала «Госуслуги». Самая распространенная уловка - предложение получить какую-либо госвыплату. Схема классическая: вы нам данные карты, мы вам - деньги. Есть и другой сценарий. Например, звонок от следователя или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Может в мессенджере прийти сообщение от якобы руководителя с указанием помочь правоохранительным органам в расследовании утечки персональных данных, начислений заработной платы и т. п. Строго указано держать это в тайне. Такие сообщения могут поступать либо рано утром, либо вечером, когда человек расслаблен, не находится в активном бодром состоянии.

Что следует сделать: не верить таким звонкам вообще. Поскольку ведомства не наделены полномочиями по аресту денежных средств и никогда не оказывают платных услуг по телефону или в мессенджерах. Не постесняйтесь и спросить у начальника проводится ли на самом деле какая-то проверка.

Схема 8. Отбирают не только деньги, но и квартиры.

Эта схема рассчитана на пожилых людей. И длится несколько недель. Сначала жертве сообщают, что кто-то пытается незаконно переоформить на себя их собственность, а правоохранительные органы уже расследуют это дело. «Следователь» по телефону просит пожилого человека проявить гражданскую ответственность и помочь органам в поимке преступников. Для этого надо лишь побыть в качестве наживки. А именно - опередить злоумышленников и самостоятельно продать квартиру.

Примечательно, что у телефонных аферистов в этот момент появляются офлайн-сообщники. Они приходят под видом риелторов, которые срочно продают недвижимость. Как правило, по заниженной стоимости, чтобы ускорить сделку. А после нее мошенники просят (а точнее, требуют) перевести всю выручку на «безопасный счет». Якобы до окончания следственных действий. На этом звонки и визиты прекращаются.

Жертв держат на связи постоянно и запрещают общаться с родственниками. Как итог - по данным московской прокуратуры, только за семь месяцев 2024 года мошенники лишили 11 пожилых москвичей их квартир. Общий ущерб оценивается в 156 млн рублей. Похожие истории зафиксированы и в других регионах. Случаи с потерпевшими известными лицами постоянно освещаются в средствах массовой информации.

На практике часто злоумышленники используют многоходовые комбинации из этих схем, работают группой, передавая потерпевшего от одного «специалиста» к другому. Преступление порою длится дни, а то и месяцы. У них есть свои

подразделения. Сотрудники одного из них осуществляют «холодный обзвон». Поняв же, что человек подвержен вовлечению в их схему, они передают его другому участнику преступной группы колл-центра, так называемому клоузеру или реализатору, который выводит потерпевшего на финал, когда тот переводит денежные средства на счета, подконтрольные злоумышленникам.

Начинающие сотрудники колл-центров, совершающие «холодный обзвон», действуют по заданному алгоритму – по скрипту (им запрещено проявлять инициативу в разговоре), то есть по определённому плану ведению разговора, который разработан психологами, социальными инженерами. Причём зачастую злоумышленники намеренно вкладывают в алгоритм разговора логическую ошибку. Они могут «ошибиться», скажем, в названии учреждения, структуры. Для чего? Если человек замечает эту ошибку, значит, уровень критического мышления у него

на должном уровне и вести с ним дальнейшие разговоры бесполезно. К счастью, немало людей обладает таким критическим мышлением, знают мошеннические схемы и, соответственно, на них не попадаются. Если же мошенники понимают, что критическое мышление у человека не сработало, они продолжают втягивать его

в мошенническую схему. Держать в голове все известные схемы не обязательно, тем более что их огромное количество и мошенники придумывают всё новые и новые ухищрения. Главное – не утратить критическое мышление. Необходимо помнить

о маркерах, ключевых словах, свидетельствующих о том, что вы имеете дело со злоумышленниками:

- *звонок от лица, представляющегося сотрудником МВД, ФСБ, Центробанка, Финмониторинга, Роскомнадзора;*
- *попытка поставить вас в ситуацию быстрого принятия решения (всё пропало, деньги утекают, но мы вам поможем),*
- *настойчивое предложение перевести деньги на «резервный/безопасный счёт» или сообщить код из СМС.*

Эти маркеры – сигнал о необходимости перепроверки информации и включить повышенное внимание. Есть и обратная сторона - люди, обладающие критическим мышлением, иногда пытаются троллить позвонивших им мошенников. Но этого делать не стоит. Есть риск, что это будет использовано против вас. Чем больше слов вы «отдадите» мошенникам, тем у них будет больше возможностей задействовать их в создании дипфейков. Конечно, искусственный интеллект пока ещё может не всё, но смодифицировать ваш голос он сможет. И потом этим голосом мошенники с определёнными целями могут позвонить вашим родственникам, знакомым. Могут отомстить и по-другому, внести телефон в базу подменных номеров. И как

будто

с вашего номера пойдут звонки другим абонентам, потенциальным потерпевшим. Помните, что вы для этих злоумышленников один из миллионов, и они к таким вещам относятся хладнокровно.

Единственно верный вариант – прервать разговор!

Разберём конкретный случай. В Управление МВД России по городу Екатеринбург^у летом 2024 года поступило заявление от заведующего отдела одного из институтов УрО РАН о том, что неизвестные обманым путем убедили его перевести на указанные ими счета 2 миллиона 770 тысяч рублей сбережений. По факту хищения денежных средств следственным подразделением УМВД по городу Екатеринбург^у возбуждено уголовное дело по признакам преступления, предусмотренного ч. 4 ст. 159 Уголовного кодекса РФ "Мошенничество в особо крупном размере".

Потерпевший под давлением профессионально организованной группы лжесиловиков и «банковских работников» согласился выполнить их указания и обналичил со счетов все свои сбережения и перевел наличные на счета злоумышленников. Его передавали друг другу пять исполнителей по хорошо отработанной, тщательно отрегулированной преступной схеме. Как пояснил заявитель, ему через мессенджер поступило сообщение от **«коллеги по работе» (1)**, в котором было указано, что в Институте проводится бухгалтерская проверка, якобы, у некоторых сотрудников было обнаружено несоответствие в начислении заработной платы, и он также находится в списке этих сотрудников, а проверкой по данному факту занимаются «сотрудники ФСБ», и с ним в ближайшее время должен связаться "представитель службы безопасности". Затем с потерпевшим также через мессенджер связался **«сотрудник ФСБ» (2)** и пояснил, что через банковские счета собеседника проводились переводы денежных средств на счета лиц, которые «финансируют терроризм», и рассказал, что несколько сотрудников Института также оказались в такой щекотливой ситуации, и его коллеги сейчас проходят такую же проверку. После звонивший поинтересовался у заявителя, действительно ли он совершал указанные переводы. В ответ растерянный ученый пояснил, что никаких переводов не совершал. Затем лжесиловик сообщил потерпевшему, что с ним свяжется «сотрудник Росфинмониторинга», чтобы вывести денежные средства собеседника из «подозрения». После потерпевшему позвонила **«специалист Росфинмониторинга» (3)** и поинтересовалась о наличии у него банковских счетов, когда он в последний раз совершал денежные операции, делал ли крупные переводы и так далее. Затем неизвестная пояснила, что с мужчиной свяжется «следователь ГУВД». Далее заявителю позвонил **«следователь» (4)** и сообщил, либо мужчина будет с ними сотрудничать, либо становится подозреваемым в «финансировании терроризма». Затем звонивший добавил, что в его распоряжении имеется доверенность на использование банковских счетов собеседника, которую последний, якобы, выдал на имя лица,

который находится в федеральном розыске, таким образом, мужчина становится соучастником разыскиваемого преступника, если откажется от сотрудничества. В дальнейшем потерпевшему позвонил «*сотрудник службы безопасности ЦБ РФ*» (5) и пояснил, что для снятия с себя подозрений необходимо «обновить», принадлежащие ему счета, а для этого, по словам звонившего, нужно ездить по банковским организациям, закрывать там счета и поэтапно переводить снятые с этих счетов денежные средства на новые счета по реквизитам, которые ему продиктуют. После совершения всех операций, когда звонки прекратились, потерпевший понял, что он стал жертвой кибермошенников [4], [5].

Глава 3 Психологический разбор преступных схем

Если мы будем рассматривать схемы 1 и 2, то наиболее подвержены воздействию мошенников финансовые потребители (сотрудники учреждений, одиноко проживающие граждане с доверчивым поведением, а также склонные основываться на первом впечатлении). Принадлежащие к этим психотипам люди не проводят достаточный анализ ситуации и не распознают ловушки мошенников. К менее восприимчивым относятся люди тревожного типа поведения, при котором степень доверия зависит от эмоционального состояния, а также людей недоверчивого типа, которые проявляют склонность проверять информацию и чаще обращают внимание на поступающую информацию.

Не менее важный фактор в воздействии внешних признаков мошенников на потенциальных жертв — это экономическая образованность. Финансово грамотные люди, склонные к критическому мышлению и анализу, внимательные к особенностям речи, языку тела и жестам собеседника, менее подвержены манипулятивным воздействиям. Они способны проявлять осторожность при принятии финансовых решений и проверять информацию перед тем, как довериться кому-либо.

По схемам 3 и 4 часто жертвами мошенников становятся тревожные и эмоциональные люди. На таких проще всего надавить при помощи грозного тона, жестких требований. Люди теряются и начинают следовать тому, что говорят по телефону. (особенно по схеме 4 пожилые, одинокие люди).

Также легко поддаются воздействию со стороны мошенников ведомые люди, привыкшие отталкиваться от какого-то ориентира. Если мошенник использует техники воздействия, демонстрируя некий авторитет, то таких людей легко ввести в заблуждение. Те, кто привык к жесткой дисциплине, тоже часто становятся жертвами мошенников.

По схемам 5, 6 и 7 воздействию подвержены люди пенсионного возраста с низкой самооценкой, не имеющие личных границ, добрые, наивные, не владеющие информацией о структуре социальной сферы, с низкой финансовой грамотностью.

По схеме 8 люди пожилого возраста с психотипами: флегматик и меланхолик, эти две крайности достаточно зависимы от мнения окружающих, особенно меланхолик. Меланхолия и зарождается в том, что у человека сильно занижена самооценка, и чтобы человеку ее поднять он нуждается во мнении о нем практически каждого человека, с которым он сталкивается. Это и делает его зависимым.

С возрастом эти психотипы усиливаются, возникает излишняя доверчивость, особенно если пожилой человек мало общается и прослеживается низкий уровень социализации.

Глава 4 Информационный след

Возникает вывод, что злоумышленники хорошо осведомлены о нас. Каковы же источники их информации. Бывают утечки из банков, микрофинансовых организаций, каких-то иных учреждений – это пресловутый человеческий фактор. Второй способ – хакерские атаки, в результате которых персональные данные уходят в сеть.

Немаловажный фактор, позволяющий злоумышленникам получить доступ к нашим данным, – информационные следы, которые мы оставляем. Человек должен понимать, что социальная сеть – это открытый источник. И если он делится подробностями личной жизни, злоумышленники этим непременно воспользуются. Даже круг общения человека – большой аналитический пласт для мошенников. Кроме того, мы, сами того не осознавая, оставляем информационную «тень» - нас фиксируют камеры видеонаблюдения, мы заходим со своих профилей на различные сайты, публикуем свои фотографии. Информационная «тень» тоже анализируется злоумышленниками. Они ведут серьезную аналитическую работу.

Мы указываем в профилях своих родственников, друзей, фотографируем свои дома, машины, рассказываем, как провели отпуск, делимся рабочими моментами. В совокупности всё это позволяет мошенникам составить по нам так называемое информационное досье.

Понятно, что интернет, социальные сети прочно вошли в нашу жизнь, но мы должны знать, как и в каких целях используют их злоумышленники, и не транслировать в общем доступе какую-то глубоко личную информацию. Сюда же относится и схема так называемых «спящих клиентов». Бывает, что человек, зарегистрировав на себя номер телефона, в силу каких-то обстоятельств перестаёт им пользоваться. Возможно, человек забывает, что он привязал его к социальным сетям, маркетплейсам, различным сервисам, банковским картам. Через определённое время оператор сотовой связи его блокирует, и номерная ёмкость переходит в руки нового владельца. Злоумышленники этим пользуются и вычисляют такие номера. Внезапно выясняется, что на человека взяли кредит. Потом начинаем разбираться, а «старый» номер был привязан к банковскому счёту. По данным специалистов, которые исследовали данную уязвимость, из 100 сим-карт почти половина (43%) номеров ранее уже использовалась для регистрации

в сервисах. Только для 6% номеров ранее созданные аккаунты были заблокированы. Чаще всего возможность восстановления доступа отмечена к социальным сетям и маркетплейсам. Аккаунт на портале «Госуслуги» позволит злоумышленнику

оформить кредиты в микрофинансовых организациях или кредитные карты. Получение доступа к аккаунту гражданина на маркетплейсах предоставляет возможность приобретения товаров в рассрочку. Аккаунт в социальных сетях может быть использован для вредоносных рассылок или получения персональных данных гражданина. Чтобы исключить такие риски, необходимо к своим телефонным номерам относиться так же аккуратно, как к паспорту или водительским правам, поддерживать доступ к своим номерам, а при утрате или замене обязательно перенести учётные записи на новый номер. Если перестали пользоваться номером телефона, то следует обратиться в банк – отвязать его от счёта и очистить от всех приложений [6], [7].

Дело не просто в доверчивости пострадавших, а в том, что сами технологии манипуляции сознанием людей стали более изощренными. Преступники, как правило, хорошо осведомлены о жертве. Они обращаются по имени-отчеству. Представляются официальными лицами. Предоставляют подтверждения, переключают на других важных профессионалов. То есть у человека создается иллюзия, что он общается с наделенными властью людьми, а сам он - беззащитная жертва обстоятельств. Телефонные аферисты всё чаще представляются полицейскими, офицерами ФСБ и непосредственным начальством. Такое количество обманутых людей говорит не только о наивности пострадавших, а также об изощрённых способам, к которым прибегают преступники. Почему такое происходит, как мы можем допускать, казалось бы, очевидные ошибки?

Глава 5 Контрмеры каждого человека

При анализе действий потерпевших речь идет не только об интеллекте или образованности — здесь задействован сложный коктейль личностных особенностей и жизненного опыта. Помимо критического мышления важна эмоциональная устойчивость, адекватная самооценка (уверенность в себе, невосприимчивость

к давлению, манипуляциям, угрожающим компетентности или безопасности). Имеет значение также уровень осведомлённости о современных видах мошенничества. Некоторые люди склонны к определённым когнитивным искажениям, которые делают их более уязвимыми перед злоумышленником. Яркий пример — «иллюзия контроля», то есть уверенность в том, что человек может контролировать события, которые на самом деле не подвластны его воле.

Переживание тревоги в какой-то жизненной ситуации, а также общая тревожность могут снижать концентрацию внимания и способность критически мыслить. Человек меньше присматривается к деталям, способен пропустить «красные флажки» и легче поддаётся манипуляциям. В состоянии тревоги люди более чувствительны к эмоциональному давлению. Мошенники используют это, вызывая чувство страха, вины, жалости, чтобы заставить жертву действовать импульсивно. Находящийся в стрессовой ситуации человек, как правило, более эмоционален, менее склонен сомневаться и пропускает существенные детали. Это особенно актуально для тех, кто ищет быстрое решение своих проблем.

Всё сказанное подчёркивает важность заботы о своём психическом здоровье. В сложные моменты жизненно необходимо обращаться за поддержкой к профессионалам.

Итак, если вы чувствуете сильную тревогу или стресс, постарайтесь не отвечать на звонки с незнакомых номеров, не вступать в беседы с незнакомцами на улице

и особенно не совершать поспешных шагов, когда вам предлагают «быстрое решение» проблемы. Следует насторожиться, взять паузу и попросить помощи у компетентных людей или своих близких. Важно перепроверить информацию: позвонить в банк, если речь идёт о действиях с деньгами, либо в полицию, если звонит якобы сотрудник правоохранительных органов [8].

Глава 6 Почему пожилые люди часто оказываются жертвами мошеннических действий

Уязвимость пожилых людей можно объяснить их опытом жизни в эпоху, когда не было необходимости шифровать, запоминать и активно использовать информацию в таких объемах, как сегодня. Кроме того, пенсионеры часто сталкиваются с трудностями в освоении новых технологий, не успевая за быстрыми изменениями. Особенности социального положения граждан пожилого

возраста

и инвалидов:

- одиноко проживающие;
- плохо разбираются в современных технологиях;
- недостаточная информированности;
- низкий уровень финансовой грамотности;
- маломобильные;
- испытывают трудности финансового характера;
- проблемы со здоровьем.

Преступников привлекает привычка пожилых людей хранить деньги наличными, а также возможность быстро получить доступ к их банковским картам, мобильным телефонам или компьютерам. Старшее поколение часто хранит деньги на «черный день», и сумма неприкосновенного запаса иногда достигает внушительных размеров.

Социальное положение пожилых людей формирует привычки и психологические особенности, которые в своих целях используют мошенники.

Психологические особенности пожилых людей и инвалидов:

- внушаемость;
- доброта;
- сердобольность;
- доверчивость;
- замедленность мыслительных процессов;
- снижение скорости реакции на возникшую ситуацию;
- ощущение беспомощности, несамостоятельности;
- забывчивость (сложности в запоминании известных схем обмана);
- повышенная тревожность.

Используя различные схемы преступных действий, мошенники создают у жертвы чувство опасности, применяют эффект неожиданности. Пользуясь тем, что пожилой человек при телефонном звонке или получении СМС сообщения от незнакомца начнет паниковать, волноваться и теряет способность рассуждать

логически. Злоумышленники с легкостью получают доступ к личным данным гражданина.

Граждане старше 70 лет, вдовцы старше 65 лет, одинокие женщины старше 50 лет. Эти группы людей чаще становятся мишенью мошенников по сравнению с другими категориями населения.

Городские пожилые люди, как правило, имеют лучший доступ к интернету и современным технологиям, что позволяет им быть более информированными и поддерживать контакт с родственниками и друзьями. В сельских районах доступ к технологиям может быть ограничен из-за недостаточной инфраструктуры. Информационное окружение, доступность среды и услуг делает городских жителей мишенью для мошенников чаще, чем деревенских. Это связано с тем, что городские пожилые люди чаще взаимодействуют с цифровыми сервисами, такими как интернет-банкинг, социальные сети и онлайн-магазины, что увеличивает их вероятность стать мишенью для кибермошенников. Благодаря большей активности в цифровом пространстве, они подвергаются большему количеству фишинговых атак, поддельных сайтов и телефонных звонков от злоумышленников, выдающих себя за сотрудников банков или других организаций.

Кроме того, городская жизнь требует большей мобильности и использования технологий, что может привести к снижению бдительности и критического мышления, особенно если человек сталкивается с новыми для него цифровыми угрозами. Мошенники, зная об этом, нацеливаются на городских пожилых людей, используя их доверие к технологиям и службам, с которыми они взаимодействуют ежедневно.

Практические способы обезопасить пожилых людей.

1. Почистите бабушкин почтовый ящик и установите на него замок. Уберите хлам с балкона и поставьте новую входную дверь. Так аферистам будет сложнее догадаться, что в квартире живет пенсионер.

2. Убедите пожилого родственника получать деньги на банковскую карту, а не наличными у почтальона.

3. Привяжите бабушкину банковскую карту к отдельному номеру и заблокируйте на нем исходящие смс.

4. Запомните и сотрите трехзначный код на обороте банковской карты пенсионера, установите лимит на снятие наличных.

5. Проверяйте звонки и расходы пенсионера через приложения банков и мобильных операторов. Не ругайте и не говорите, что отслеживаете.

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

Глава 7 Подростки и молодежь в зоне риска

Молодые люди понимают повестку времени и наслышаны о тех же телефонных мошенниках, но всё равно становятся жертвами преступников. Они при этом не считают себя жертвами, а скорее наоборот, решившимися на поступок «героями», пусть и в негативном смысле.

По установленным данным мошенники используют природный агрессивный потенциал подростков и молодёжи. У них велико естественное желание, которое необходимо для взросления, противопоставлять себя всем окружающим. Их неудовлетворённость миром используют в негативном контексте. Поэтому довольно легко внушить идею о каком-то сопротивлении, что якобы то, что он сейчас делает, будет высоко оценено. Это попытка заявить о себе, проявиться, доказать сверстникам, что, мол, я могу совершить такой «подвиг», пусть и негативный. У них ещё и неустойчивая философия, неустойчивые позиции. К тому же подростки не несут такую уголовную ответственность, как взрослые. Несовершеннолетние не знают законов, поэтому могут легко согласиться на преступление, не осознавая последствий. Определённые проблемы в семье или отсутствие доверия к родителям ведут к тому, что эти подростки после звонка мошенника не спешат поделиться информацией с родными, а просто верят человеку по телефону. На молодёжь после 20 лет могут давить через финансовые интересы, когда обещают лёгкие деньги и полную анонимность. А фактор устрашения, запугивания якобы проблемами с правоохранительными органами может подействовать абсолютно на все категории граждан.

Очень опасная тактика телефонных мошенников может охватить всех, у кого имеются банковские карты. В последнее время именно этот сценарий становится популярным, а его жертвами становятся студенты и школьники. Дропперы (от английского drop - бросать, капать) - подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт. Абсолютное большинство нынешней молодёжи постоянно находятся в интернете и там все чаще стали сталкиваться с предложениями легкого заработка. Обычно предлагающие представляются работодателями и рекламируют легкую, а главное, высокооплачиваемую работу. При этом схема получения денег действительно не требует особых знаний или усилий. Подростку в интернете предлагают заработать деньги следующим образом: он получит проценты за перевод со своей банковской карты поступивших на нее сумм на чужие банковские счета.

Еще один вариант возможного предложения - попросить молодого человека продать свою банковскую карту для таких же операций. Он получит деньги сразу и весьма солидную сумму. Оба предложения выглядят крайне заманчиво.

Поначалу чаще всего этим занимались студенты, а сегодня большинство дропперов - школьники, у которых есть оформленная родителями карта банка.

Правда, школьнику не говорят, что, как только он соглашается на один из предложенных вариантов, он становится соучастником незаконной схемы по отмыванию денежных средств. Ведь с помощью его банковской карты будут переводиться деньги, добытые преступным путем. Также детям никто не скажет, что зачастую обещанных процентов или суммы за продажу банковской карты они могут и не получить. И жаловаться не стоит. Об этом детям расскажут сами мошенники.

И доходчиво разъяснят, что они стали участниками преступления, начнут шантажировать, угрожая сообщить обо всем в полицию.

Обманутых детей просто запугивают, объясняя, что они приняли участие в мошенничестве и отмывании денег. О чем узнает не только полиция, но и школа, друзья и родители. В результате человек остается без обещанных денег и с серьезными проблемами. В случае причинения кому-то имущественного ущерба на родителей ребенка может быть возложена обязанность по возмещению причиненного вреда.

Следует объяснить простую истину - не вступать в диалог с незнакомцами в интернете, поскольку последние обладают специальными навыками и способностями психологического воздействия на человека. Мошенники годами оттачивают свое «мастерство», навыки по обману людей, а значит, нет никаких гарантий того, что в ходе общения им не удастся склонить ребенка к «сотрудничеству».

Владелец карты также попадет в общий банковский «черный список», и - надолго. Затем последует блокировка банковских приложений, останется возможность использования только наличных денежных средств. Он может быть привлечен к ответственности, в том числе и уголовной. Пройдет несколько лет, а у вчерашнего школьника, если он обратится в банк возникнут проблемы. Кроме того, очень вероятная судимость сделает для него недостижимыми очень многие профессии. Также злоумышленники могут продолжить склонять его к дальнейшей преступной деятельности, в том числе и к экстремистской. [9].

Глава 8 Вербовка для совершения экстремистских действий

Вербовщики активно используют социальные сети и мессенджеры. Злоумышленники внимательно изучают аккаунты, посты, комментарии и, найдя подходящего кандидата, вступают с ним в диалог. Оценив сильные и слабые стороны собеседника, определив темы, волнующие его больше всего, вербовщик всеми силами старается вызвать доверие и интерес, чтоб собеседнику хотелось продолжать общение.

В своей враждебной деятельности вербовщики ориентируются на молодых людей, которые зачастую не имеют большого жизненного опыта, твердой жизненной позиции, ищут поддержку в Интернете, а также находятся в проблемных или кризисных обстоятельствах. Нередко для совершения диверсий и террористических актов злоумышленники используют материальную заинтересованность. Опытный вербовщик, изучая аккаунты, вычисляют людей, нуждающихся в денежных средствах.

Им могут просто без всякой идеологической подводки предложить финансовые средства за определенные действия, например, бросить бутылку с «зажигательной смесью» в госучреждение, выйти на одиночный пикет, перевезти компоненты взрывчатых веществ, запрещенных к обороту и т.д.

В процессе вовлечения могут предложить исполнить мелкое поручение за денежное вознаграждение расплатившись по безналичному расчёту или криптовалюте с целью проверки степени пригодности к последующему совершению настоящего преступления.

Если вербовщикам не удастся склонить жертву к совершению противоправных действий на идеологической или финансовой основе, в ход могут пойти компрометирующие материалы, например, личного характера, которыми человек когда-то с кем-то поделился, пусть и в закрытой переписке.

Вербовкой занимаются специально обученные, хорошо подготовленные люди, владеющие психологическими приемами - техникой манипуляций, внушением. Поэтому противостоять им довольно сложно, необходимо вовремя распознать вербовщика и минимизировать общение с ним.

Признаки вербовщика:

- ведет дружественную переписку;
- хвалит, делает комплименты, поддерживает и демонстрирует заботу к собеседнику;
- проявляет чрезмерную заинтересованность к личности собеседника и его проблемам, имитирует помощь;
- оценивает психологические и физические качества, интересуется материальным положением;

- внушает, что вводит собеседника в некое секретное «сообщество», которое занимается исполнением «очень важных дел», члены сообщества - люди избранные;

- всегда имеет заранее подготовленные ответы на любые вопросы.

Характеристика лиц, попадающих под влияние вербовщиков.

Вербовщикам легче всего взаимодействовать и вовлекать в преступную деятельность следующую категорию лиц:

- сторонники оппозиционных движений, приверженцы радикальных взглядов и идеологий;

- зависимые граждане (наркоманы, игроманы, алкоголики, «закладчики», и др.), готовые совершить преступления против общественной безопасности и правопорядка, представителей государственной власти по идеологическим мотивам или за денежное вознаграждение;

- жертвы мошеннических действий, ошибочно полагающие, что совершение преступления приведет к возврату похищенных денежных средств;

- лица, находящиеся в неустойчивом психоэмоциональном состоянии (стресс, разочарование, одиночество, безденежье, депрессия);

- подростки, чем младше человек, тем более он подвержен влиянию извне, воспринимая свое окружение и интернет, как обучающую среду;

- молодые люди, не определившиеся со своей самоидентичностью, с гипертрофированным желанием выделиться из толпы, из «серой массы», быть причастными к значимому и «секретному» обществу, движению;

- пожилые одинокие люди, которые из-за своей доверчивости и неумения или невозможности критически мыслить выполняют какие-либо поручения или задания, не понимая, что их просто используют.

Способы противодействия вербовкам.

Противодействовать вербовщикам можно такими же способами, как и мошенникам. При этом необходимо помнить, что, следуя указаниям мошенников можно лишиться денежных средств, поставить под угрозу финансовое благополучие собственной семьи. А следуя указаниям вербовщиков можно поставить под угрозу безопасность страны, лишиться свободы, а то и жизни.

Для того, чтобы не привлекать к себе внимание вербовщиков (или мошенников) в сети Интернет необходимо придерживаться и соблюдать простые правила:

- не размещать на личных страницах социальных сетей и аккаунтах мессенджеров информацию о месте жительства, работе, учебе, свои личные данные и данные родственников;

- ограничить доступ к личным фотографиям, записям, оставив доступ только кругу хорошо знакомых людей;

- не вступать в переписку с незнакомыми людьми, особенно настороженно относиться к тем, кто проявляет чрезмерную активность и интерес, а также предлагает легкий и быстрый способ заработка за короткое время;

- на любое предложение о легком заработке, решении проблем отвечать отрицательно и прервать дальнейшую переписку;

- при малейшем подозрении на вербовку прекратить общение, воспользовавшись опцией «черный список», «заблокировать», «пожаловаться» в случае, если незнакомое лицо продолжает «атаку» сообщениями;

- не отправлять фото документов, удостоверяющих личность (паспорт, ИНН, водительские права), не записывать и не отправлять видеообращения по готовому сценарию собеседника;

- воздержаться от спорных и неоднозначных мнений в общедоступных форумах, группах, чатах (вербовщики привлекают внимание людей к темам, вызывающие споры и сами активно «подливают масло в огонь»);

- выработать в себе навык «наблюдателя», критически мыслить, не поддаваться угрозам, проверять и перепроверять информацию;

- не передавать третьим лицам данные банковских карт, счетов, сведений из личного кабинета налогоплательщика, на портале госуслуг;

- не переводить денежные средства на неизвестные счета банковских карт, в том числе не пополнять счета абонентских номеров телефонов по чьей-либо просьбе, чтобы в последующем не стать жертвой мошенников, которые также склоняют потерпевших на совершение преступлений экстремистской направленности;

- если вы стали жертвой вербовки, в том числе вам начали поступать угрозы и запугивания, обратиться за помощью к родным и близким, если же ситуация выглядит угрожающей, существует опасность для жизни, то необходимо обратиться в правоохранительные органы [10], [11].

Глава 9 Психологический аспект

Преступники играют на таких составляющих:

- слабости человека (некомпетентность, неопытность, невнимательность);
- природные инстинкты (страх, жадность, желание безопасности);
- положительные качества человека (доброта, доверие, благодарность).

Хорошо организованные преступные структуры превратились в одно из направлений криминального бизнеса. Социальная инженерия — в контексте информационной безопасности — психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Это способ психологического манипулирования человеком путём внушения, создания атмосферы доверия, применения специфических уловок и хитростей, за счет которых человек оказывается под влиянием мошенников. Совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного «мошенничества» отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества. Технологии социальной инженерии обкатываются на большом количестве людей, что позволяет постоянно совершенствовать формы и методы, находить уязвимости в электронных сервисах и, к сожалению, оставаться эффективными.

Социальная инженерия стала «работой» для преступников. Они организуют высокотехнологичные контактные центры, создают каналы связи с подменой номеров, команды программистов пишут специальные скрипты для общения операторов со своими потенциальными жертвами. Отрабатывают новые схемы на пилотных проектах, четко структурируют категории лиц для преступной обработки, ведут персональный сбор данных. Проводят психологические и социальные исследования. Разрабатывают стратегии развития и выманивают все, до чего могут дотянуться (деньги со счетов, кредиты, займы, вклады, инвестиции, недвижимость).

Вот этот напор и слаженность мошенников, а также техники внушения, которые они используют, выбивают у человека почву из-под ног. Он уже не может мыслить критически, он не решается обратиться за помощью, потому что, как ему угрожают, это будет иметь фатальные последствия.

Такие состояния и природные качества делают нас подверженными действиям мошенников:

- Стресс из-за общей усталости и перегруженности организма, что снижает концентрацию нашего внимания. В таком состоянии есть склонность к быстрым и необдуманным решениям, а также затруднения с оценками рисков. Усталость

сильно влияет на способность к познавательным процессам. Утомление мешает контролировать своё финансовое поведение и распознавать обман.

- Склонность к анализу, рационализм.
- Суеверность.
- Инфантильность.
- Дефицит общения.
- Доверчивость, ведомость и внушаемость.
- Высокая тревожность.
- Азартность.
- Плохая осведомлённость о работе финансовой системы.
- Нахождение в тяжёлом материальном положении.
- Рассеянность и невнимание к деталям.
- Неудовлетворенность своим материальным положением.
- Низкая собственная самооценка, в совокупности с чувством собственной неполноценности, эмоциональной неустойчивости, неуверенности в себе, впечатлительности.

Особенности мышления человека, делающие его более подверженным атакам злоумышленников:

- Отсутствие навыков системного критического мышления и самоконтроля.
- Медленный темп психической активности.
- Отсутствие гибкости мышления.
- Инертность и стремление действовать по шаблонам и стереотипам.
- Наивный оптимизм.

Глава 10 Наличие когнитивных искажений.

Когнитивные искажения - это систематические ошибки в восприятии и мышлении, вызванные убеждениями и социальными стереотипами, эмоциональными состояниями и особенностями обработки информации нашим мозгом. Этих искажений около 200 (иллюзорная корреляция, феномен «дверь в лицо», эффект сверхуверенности, стереотипизация, эффект ложной уникальности, эгоцентрическое искажение, подчинение авторитету, эффект Даннинга-Крюгера, эффект иллюзии правды, вера в справедливый мир, эффект роли, конформность, ошибка выжившего, эффект текущего момента, эффект третьего лица и другие). Они вшиты в наше мышление на подсознательном уровне. Мы их не замечаем, так как последствия в повседневной жизни не так значимы.

На бытовом уровне потери от ошибок не так страшны. Конечно, для каждой ловушки сознания разработаны свои противоядия. Но применить их возможно только, если действовать сознательно и осознанно. Должно быть время, чтобы применить знания о том, как бороться с когнитивными искажениями.

Состояние депрессии, пониженное настроение также влияет на когнитивные функции. Снижается внимание, память, способность логически мыслить. Также затруднено воспринимание манипуляций и обманов. В состоянии депрессии может возникать чувство собственной ущербности, вины, подсознательное желание наказания.

Это знают преступники, и поэтому они удерживают сознание под своим контролем. Требуют, чтобы мы всегда оставались на связи, торопят, стимулируют чувство страха, неуверенности в себе. В результате, даже зная о феномене когнитивных искажений, человек не может этим знанием воспользоваться.

Рассмотрим некоторые из них:

Конформность. Склонность индивида менять свое поведение под влиянием окружающих. Вшито у человека в подсознание, мы не хотим отличаться от окружающих, испытываем потребность соответствовать ожиданиям. Отсутствие у человека собственного мнения. Конформист готов выполнять требования любого, кто имеет над ним власть, а также требования, продиктованные обществом. Такие люди всегда следуют за большинством и не любят выделяться из толпы. Именно на это давят мошенники, когда рассказывают о необходимости, важности той ситуации, в которую погружают жертву. Говорят, что сейчас всех обманывают, поэтому надо быть заодно со всеми. И используют страх быть обманутыми, чтобы нас обманывая добиться от нас лояльности к себе. И в моменте стресса наша природная конформность приводит к увеличению степени доверия к человеку, с которым мы разговариваем.

Подчинение авторитету. Это тенденция оценивать мнение авторитетных людей выше, чем собственное, и в большей степени полагаться на него. Инстинкт, заложенный в нас эволюцией. Сталкиваясь с представителями власти, рефлекторно

начинаем следовать их инструкциям, подчиняемся указаниям авторитетных для нас людей. Поэтому мошенники часто представляются официальными лицами (представителями МВД, ФСБ, Следственного комитета, Центробанка). Мы и не замечаем, как начинаем со всей серьёзностью выполнять то, что нам говорит «представитель власти».

Вера в справедливый мир. Мнение, что мир устроен справедливо, а значит нас не обманут. Люди хотят верить в мир, где добродетель вознаграждается, а зло наказывается. Мы верим, что большинство населения хорошие и справедливые люди как мы. Подсознательно считаем, что и другие не хотят нанести нам вред. Человек доверяет другим людям просто потому, что нам трудно сжиться с мыслью, что от человека можно ожидать негативных действий просто так. На это и давят мошенники. «Ну не будем же мы вас обманывать, вы же такой замечательный и законопослушный человек». Именно лжецы любят повторять, что они не лгут.

Эффект третьего лица. Наши мысли о том, что любая вредная информация, плохие новости, реклама воздействуют на нас меньше, чем на всех остальных. Мы склонны думать, что мы особенные и отличаемся от большинства, причём в лучшую сторону. То есть мы за себя спокойны, но не спокойны за наших близких. Как будто у нас есть особенный иммунитет, а у других нет. Уж мы то точно способны отличить правду от лжи, манипуляцию от реальности. Этой нашей самоуверенностью и пользуются злоумышленники.

Стереотипизация. В психологии этот термин означает принятие события, человека при следовании своим убеждениям и опыту. При таком явлении происходит присваивание знакомых свойств характера. На самом деле мы просто переоцениваем себя и недооцениваем других.

Неосведомленность о том, как мошенники вводят человека в состояние, когда он перестаёт контролировать ситуацию, являются основной причиной попадания под их влияние. *Знание основных психологических способов, которые используют злоумышленники возможно будет одним из основных способов защиты.*

Глава 11 Фундаментальные методы действий мошенников

Взаимность. Мягкое воздействие, которое создает ситуацию взаимности. У человека ощущение, что ему оказали услугу и он должен ответить тем же. Это распространённый приём манипуляции, когда манипулируют чувством вины или долженствования.

Благорасположение. Люди склонны больше верить тому, кто приятен и нравится. Пускают в ход своё обаяние и пытаются максимально соответствовать ожиданиям. «Ведь такой замечательный человек не может нам навредить!» Но это работает эффект благорасположения.

Эмоциональные триггеры. Максимально интенсивное, эмоциональное, прямолинейное воздействие. Притворяются близкими родственниками, которые попали в беду. Эта ошеломляющая новость сразу снижает у человека критическую оценку ситуации.

Страх неизбежности. Создают эмоциональное давление тем, что случится что-то непоправимое. Деньги нельзя будет вернуть, преступника невозможно будет поймать, наказание будет неизбежным и т.д. поэтому действовать надо немедленно и выполнять все указания злоумышленников.

Авторитет. Притворяются сотрудниками авторитетных структур или активно ссылаются на них. А затем говорят о необходимости тех или иных действий. Всячески подчеркивают свою экспертность, значимость, власть над человеком или над ситуацией. Проблему решить можно только с ним или никто больше не поможет.

Последовательность. Создание ложных логических цепочек из чего-то знакомого и необычного. Любой человек когда-то общался с оператором банка (знакомое), но преподносится ситуация якобы списания с банковской карты денежных средств (не знакомое). При этом псевдооператор действует по специальному протоколу, разработанному именно для таких случаев. Ситуация запутывается так, что человек уже не понимает, что правда, а что ложь. И мошенник пытается играть на отсутствии логических противоречий в своей аргументации. Но эта логическая непротиворечивость не исключает того, что нас обманывают.

Социальное доказательство. Мошенник настаивает, что все люди в данной ситуации поступают так, как нужно по инструкции, придуманной мошенником. Поступай так и всё окончится благополучно. Но ведь мы не знаем, как поступают все и послушно следуем инструкциям (вводим пин-коды, говорим пароли и т.д.).

Эффект дефицита. Создаётся нехватка какого-либо ресурса. Это пробуждает ощущение, что надо спешить, действовать быстро. Принимать решение, пока якобы есть такая возможность. А то акция закончится или ваше место займёт кто-то другой.

Из этих способов вытекают две основные стратегии воздействия: эмоциональный шок и перегрузка:

Эмоциональный шок создаётся неожиданным и резким погружением в стрессовую ситуацию. Например, информация о распоряжении, об аресте банковских счетов или о краже денег. На этом этапе главное – вывести из состояния равновесия, вызвать шок и тотальную растерянность. Добиться, чтобы человек запаниковал. Создаётся ситуация спешки. Чрезвычайно мощный эмоциональный стимул. Когда мы боимся опоздать что-то сделать, то мы действуем стереотипно или по инструкции. Рациональное мышление при этом отключается и нет возможности распознать несостыковки в словах и действиях мошенников. А также попросить совета и помощи у друзей и близких или у специалистов, которые разбираются в подобной ситуации.

Тогда принимаются успокаивать и внушать, что на том конце провода находится спаситель, который вошёл в положение и готов помочь всем, чем может. Предлагается быстрое решение проблемы, от которой нельзя отказываться. При этом общаются с пониманием и сочувствием, а это снижает соответствующие психологические барьеры.

Стратегия перегрузки, когда необходимо осмыслить большое количество информации. Происходит многозадачность в моменте. Человек сам не может снизить темп выполняемых параллельных действий, которые задаёт злоумышленник, диктуя их напрямую. Чем больше делается в моменте разных дел, тем ему проще мошеннику добиться желаемого. Зачастую от перегрузки человек впадает в состояние психологического транса, пытаясь учесть множество факторов. Но при этом не видит, что на самом деле происходит у него буквально под самым носом. Срабатывает так называемый феномен «невидимой обезьяны». (Например, фактически передаёт свой пароль для доступа к сайту «Госуслуг»).

Часто эти две стратегии комбинируют и вызывают эмоциональный шок, одновременно создавая перегрузку внимания [12].

Пример такой стратегии «обработки» человека:

1. Мошенник начинает разговор, аккуратно нарушает личные границы, а потом перегружает восприятие. Особенно это легко удаётся, если злоумышленник заблаговременно собрал достаточное количество деталей личной информации из различных открытых источников о жертве. Также собирается информация о должностном лице, которым представляется злоумышленник. Он вбрасывает её детали одну за другой (фамилии, имена, должности, звания, адреса, наименования учреждений и т.п.) и побуждает в психике человека множество ассоциаций. Тем самым внимание оказывается отвлечено на продумывание всех этих несущественных деталей. В мышлении человека создается существенная **перегрузка**.

2. Затем неожиданно начинает директивно или даже устрашающе доносить шокирующую информацию. Его задача напугать, чем сильнее, тем лучше.

Шокирующая информация о близких, деньги со счёта вот-вот пропадут, случится трагическое событие наподобие теракта и тому подобное. Появляется **всплеск негативных эмоций**.

3. Человек впадает в состояние паники, внутренней причиной которой является желание решить проблему, которую он уже воспринял как достоверную, не имея возможности оценить её критически и проверить. Он **стремится вернуться в комфортное стабильное состояние**.

4. Мошенник продолжает давить – сделай то, что просят и тогда всё наладится. Эмоционально загоняет сознание в ловушку и показывает якобы единственно правильный выход, который разрешит «ужасную» ситуацию. Путь возврата в стабильность – это **выполнение действий, предлагаемых злоумышленником**.

5. При это он не прерывает связь с человеком, ведёт его по телефону до совершения необходимых действий. Запугивает, что если связь прервётся, то это будет иметь фатальные последствия. Он регулирует эмоциональное состояние стресса жертвы, действуя очень логично и грамотно. Либо успокаивает и подбадривает, либо наоборот добавляет новые вводные и заостряет риски, которые сам и придумывает. В итоге человек отдаёт деньги курьеру, переводит средства на «безопасные счета», оплачивает несуществующие услуги или товары и тому подобное. **Результат обмана достигнут!**

Глава 12 Как определить человека, оказавшегося под воздействием мошенников

1. Поведение человека начинает меняться после общения с кем-то по телефону, он-лайн, в мессенджере или непосредственно в личном контакте.
2. Мошенники пугают потерей близких, денежных средств, серьёзными проблемами с правоохранительными органами, обнародованием какой-либо чувствительной информации и тому подобное. После резкого приступа страха обычно возникает растерянность и дезориентация, что можно заметить в поведении близкого человека.
3. Заставляют действовать поспешно. Задача злоумышленников состоит в том, чтобы не смогли расценить их требования с рациональной точки зрения, взвесить все за и против последствий сложившейся ситуации. Особенно важно в этот момент взять паузу и внимательно проанализировать все обстоятельства дела.
4. Предлагают большую и легко доступную выгоду. Игра на желании человека «сорвать большой куш». Простота и гарантированность решения вызывают состояние эйфории, что приводит к снижению самоконтроля и адекватности.
5. Манипуляторы могут намекать на то, что человек делает что-то недостаточно хорошо или уже совершил серьёзные ошибки. Это позволяет вызвать чувство неудовлетворённости или неуверенности. После чего может существенно усилиться влияние злоумышленника.
6. Создают чувство зависимости, заставляют ощущать себя им обязанными, выступают в роли «доброего спасителя». В результате может возникнуть чувство, что человек буквально должен мошеннику и уже трудно не подчиниться требованиям.
7. Желая увеличить уязвимость, манипуляторы просят никому не рассказывать о том, что происходит. Это нельзя обсуждать ни с кем, так как поставит всю «операцию» под угрозу. Случится что-то ужасное и все пострадают. В ход идут истории про секретные задания, специальные службы, двойных агентов и прочее. Сценарии вроде бы безумные, но человек может этого не заметить. Человека подробно инструктируют как отвечать на вопросы друзей и близких. Чтобы ни в коем случае не провалить «задание», не подвергнуться риску, не потерять время и т.п. иногда даются «специальные задания», которые имеют прямую цель изолировать человека от родных и близких. Добиться, чтобы человек никак не пересекался с теми, кто может заметить одержимость, трансовое состояние и неадекватность действий.
8. Пытаются внушить мысли, идеи, желания, которые противоречат собственным убеждениям. Это делается под воздействием сильного эмоционального напора, многократного повторения, часто через прямые угрозы.

9. Ощущение потери контроля над своими действиями, мошенники пытаются контролировать, держать на коротком поводке постоянного аудио или зрительного контакта.

10. Ощущение давления и тревоги при взаимодействии со злоумышленниками. Несмотря на то, что они говорят о нахождении на стороне жертвы обмана. Это ощущение труднообъяснимо, но оно постоянно присутствует.

Глава 13 Способы психологической защиты, как обезопасить себя

Помнить, что из любой ситуации всегда есть выход. Даже если по какой-либо причине человек не прервал разговор, дал возможность втянуть себя в беседу – все равно он на любом этапе сможет остановиться.

1. **Время.** Не реагировать сразу, а взять паузу. Если есть хотя бы малейшие подозрения, то эта пауза позволит прийти в себя и проверить информацию. Лучше подстраховаться и удостовериться в безопасности, лишний раз показаться смешным и некомпетентным, зато обрести уверенность в себе. Даже, если мы ошибёмся в подозрительности – это лучше, чем пропустить атаку мошенников.

2. **Критическое мышление.** Вырабатывать привычку изучать и анализировать, получаемую информацию, задавать себе вопросы и проверять достоверность источников или утверждений. Не доверять информации от незнакомых людей. Особенно поступающей неожиданно в режиме реального времени. Не предоставлять свои личные данные и финансовую информацию. Всегда тщательно проверять надёжность компаний и организаций, с которыми планируется ведение каких-либо дел. Читать отзывы, проверять репутацию, наводить справки. Осторожно относиться к слишком заманчивым предложениям. Не верить обещаниям быстрого и лёгкого получения денег.

3. **Знать преступные схемы мошенников.** К сожалению, в настоящее время приходится знать методы, которыми злоумышленники могут манипулировать нашим сознанием. Следить за новостями, делиться этой информацией с близкими и знакомыми. Зная трюки и уловки мошенников можно сэкономить своё время и деньги.

4. **Помнить о социальных навыках.** К большому сожалению, желание незнакомых людей оказать помощь и проявить заботу в помощи заработать деньги зачастую несёт корыстные мотивы. По какой причине обращаются именно к нам, в чём интерес и какие могут быть последствия? Нужно учиться задавать вопросы, слушать ответы на них и рассматривать не одно объяснение почему человек отреагировал так, а не иначе, а разные мотивы возможных его действий.

5. **Обсуждать поступающую информация** с критически настроенными друзьями, родными, близкими, в чьём мнении есть уверенность. Всегда есть право прерваться и позвонить другу за советом. Услышать сторонний, не предвзятый взгляд на события, другой подход к оценке предложений и просьб.

6. **Золотое правило защиты от манипуляций.** Не бояться сказать нет, если что-то кажется неправильным или вызывает внутренний дискомфорт. Приучить себя чётко отделять свои интересы от интересов окружающих. Каждый раз проверять истинную природу своих намерений, точно ли мы сами этого хотим или кто-то другой навязывает нам эти желания?

Глава 14 Как защитить своих близких от воздействий мошенников

- Обращать внимание на необычные действия или поступки со стороны близких. Если он взволнован, проявляет скрытность, признаки нахождения в трансе (отсутствующий взгляд, заторможенность, замедленная реакция на слова), то попытаться понять, что происходит, с кем он находится на связи. Разговаривает по телефону, появились знакомые, с которыми надо срочно что-то решить. Жертвы мошенников обычно чувствуют себя напряженно и ведут себя нервно, так как схемы социальной инженерии предполагают моделирование проблемной ситуации для жертвы.

- Спешка и суета сопутствует погружению в мошеннические действия и являются эффектом дефицита времени. Эмоциональный стресс может проявляться учащенным дыханием, покраснением кожи, потливостью, дрожью, изменением тона голоса или глухим или наоборот слишком звонким, резкими движениями.

- Мошенники постоянно пытаются выключить жертву из общения с близкими. Угрожают применением насилия, потерей денег, увольнением с работы, правовыми последствиями и т. д. жертва будет стараться не смотреть в глаза. Избегать ответов на конкретные вопросы, говорить невпопад странные вещи или давать односложные ответы заученными фразами, как по инструкции. Человеку поступают периодические звонки, сообщения в мессенджерах, для ответа на которые он может уединиться и реагирует необычно резко.

Если подозрения начинают подтверждаться, то нужно попытаться войти с человеком в психологический контакт. Использовать успокаивающий, сочувствующий тон голоса, предложить вместе попить чаю. Быть внимательным, открытым, помочь человеку восстановить его чувство безопасности, что он для близких важен и ценен. Как можно быстрее вывести человека из-под влияния мошенников – это поможет ему быстрее восстановиться и почувствовать себя увереннее. Минимизировать последствия случившегося. Выход человека из тоннеля, в который его ввёл мошенник может оказаться ещё одним шоком и нести тяжёлые последствия. Он пытается осмыслить что случилось, как он вообще мог попасть в такую ситуацию. Помочь связаться с компетентными органами, службой поддержки банка, финансовых организаций. Не сердиться на человека. Оказать ему поддержку, возможно оказать помощь специалиста психолога.

Первый шаг: попробуйте переключить его внимание на что-то другое. Если у вас получится, и он сможет погрузиться в какую-то другую деятельность, то, вероятно, все благополучно. Бывают случаи, когда человек находится в неадекватном состоянии, ведет себя словно загипнотизированный. В этом случае могут помочь простые физические действия: нужно вернуть его в реальный мир, -

что-то сделать, что-то рассмотреть, в чем-то разобраться. Хорошо помогают дыхательные упражнения: буквально можно сказать, что стало душно и надо глубоко подышать, и сделать это вместе с ним - вдох-выдох и т. д. Простые физические действия, внимание к обстановке и нормализация дыхания - самые простые инструменты, которые помогают нам вернуться в реальность, если человек оказался под гипнотическим воздействием. В простонародье в таких случаях «околдованности» говорят: «Ущипните меня!» Как раз про это - выйти из забытья в реальный мир.

Ещё рекомендуется финансово обезопасить старших. Многие пожилые люди хранят крупные суммы «под подушкой», они всегда под рукой. Но это и повышает риск – мошенникам тоже легче добраться до них. Поэтому правоохранители рекомендуют использовать долгосрочные вклады или накопительные счета, которые предлагают банки. Это помогает снизить риск преступления.

С точки зрения психологии рекомендуется проследить не только за финансовой грамотностью, но и за эмоциональным состоянием. И тут лучше не ждать того, что какие-то переживания станут сильными настолько, что справиться с ними без посторонней помощи будет невозможно. Лучше найти регулярный и полезный способ разгружать себя: массаж, спорт, прогулка по лесу и другие средства. Ещё не помешает время от времени советоваться со специалистом. Вполне нормально «сверять» с психологом свое эмоциональное состояние и стремиться улучшить качество жизни.

Также помогает развитие проактивности. То есть умение не реагировать на что-то реактивно и импульсивно, а взять паузу на осмысление. Фактор спешки – главное, на что давят мошенники. Они будут подговаривать, что действовать надо быстро, иначе всё пропало. Но на самом деле, лучше действовать спокойно и не торопясь. Тут может помочь привычка советоваться с близкими в подобных ситуациях. Например, договориться с родственником о том, что кто бы ни позвонил, он перезванивает и говорит, что предлагают. Прямо выучить фразу «я сейчас посоветуюсь с сыном, перезвоните через 30 минут».

Мошенничество может коснуться каждого. Дело не в психологии жертвы, а в нашей общей человеческой психологии. Если вы знаете ее законы, то знаете, как манипулировать человеком. На этих же механизмах выстраиваются, например и «информационные войны». Так что, ни высокий уровень IQ, ни уровень образования, ни даже опыт работы в крупнейших финансовых организациях не даст гарантии защиты от манипуляций. Только знание конкретных схем мошенничества и того, как в том или ином случае себя вести.

Эти схемы основаны на природных инстинктах - страхе, неуверенности, потребности в безопасности. И, что самое отвратительное, на таких прекрасных качествах, как доброта, доверие, благодарность. Мошенники создают ситуацию, когда человек чувствует себя не только зависимым от преступников, но и испытывает к ним благодарность за то, что они его «спасают».

Более подверженным манипуляции делает человека общая усталость, хронический стресс и перегруженность внимания. Состояние депрессии также влияет на наши когнитивные функции: снижаются внимание, память, способность критически мыслить. Еще повлиять на нашу восприимчивость к мошенническим схемам могут низкая самооценка, наше чувство неполноценности, робость, стеснительность.

Глава 15 Рекомендации для защиты себя и своих близких от чужого эмоционального воздействия

Принцип пяти «НЕ».

- Не отвечать на звонки с незнакомых номеров,
- Не заводить телефонных разговоров с неизвестными лицами,
- Не вступать в переписку с незнакомыми людьми,
- Не переходить по ссылкам из непроверенных источников,
- Не устанавливать приложения по рекомендации неизвестных лиц.

Взять за правило.

• Прежде, чем принять какое-либо решение — обязательно дайте себе время всё хорошо обдумать. Обратитесь к родственникам, друзьям, коллегам, осмыслите ситуацию. Не совершайте необдуманных действий и всегда проверяйте полученную информацию.

• Задавайте уточняющие вопросы. Например: «Зачем мне это нужно?», «Вы на самом деле считаете, что это правильно?», «Вы думаете, это разумный поступок?». Обычно манипулятор «складывает оружие», поскольку не знает ответы на прямые вопросы.

• Верьте своей интуиции: если подсознательно чья-то компания вам неприятна, следует прислушаться к внутреннему голосу. Прислушивайтесь к своим чувствам

и телесным ощущениям.

• Наблюдайте за эмоциями, мимикой, особенностями поведения манипулятора и наверняка заметите несоответствие.

• Опасайтесь малознакомых людей, которые демонстрируют чрезмерную доброжелательность, привязанность, стремление понять, обещание решить большинство проблем.

Для того, чтобы выйти из-под контроля манипулятора, можно использовать следующие упражнения.

«Мои пальцы»

Упражнение поможет быстро успокоиться, переключить внимание и отвлечься.

- Посмотрите на свои руки, пусть они лежат расслаблено и спокойно.
- Начните большим пальцем, начиная с указательного, касаться всех остальных и считайте от 1 до 4.
- Затем начинайте с мизинца и считайте от 5 до 8.
- Потом переходите ко второй руке и сделайте тоже самое, только считать начинайте с 8 в обратном порядке.
- Полностью сконцентрируйтесь только на своих руках, на правильном порядке и счёте.

Повторите столько раз, сколько вам потребуется

«Скорая помощь»

- Сделайте глубокий вдох и медленный-медленный выдох через рот (10 раз).
- Посмотрите по сторонам.
- Осмотрись вокруг, и отметьте 5 вещей, которые видите прямо сейчас.
- Теперь отметьте 5 звуков, которые слышите.
- Теперь отметьте 5 ощущений в теле, например, локти касаются стола, движение воздуха в районе лица, ноги стоят на полу и т.п.
- Попробуйте ощутить всё это одновременно.
- Оцените свое состояние от 0 до 10.

Один из лучших и наиболее доступных инструментов, которые можно использовать для уменьшения стресса, — это связь с нашим дыханием. Кроме того, с помощью дыхательных упражнений можно избавиться от приступа тревоги и надвигающейся волны беспокойства. Во время стрессовой реакции дыхание становится легким и поверхностным. Когда это происходит, важно привлечь внимание к дыханию, чтобы помочь перефокусировать ум.

«Дыхание животом»

Приложите ладони к животу и начинайте медленно вдыхать и выдыхать, считая до 10. Сконцентрируйтесь на дыхании: глубокий вдох, а затем выдох в 2 раза длиннее вдоха. Несколько раз быстро втяните воздух носом, после чего сделайте продолжительный выдох ртом.

«Дыхание через ноздри»

Сядьте прямо, на пол или на стул. Правой рукой аккуратно согните указательный и средний пальцы в ладонь. Мягко закройте правую ноздрю большим пальцем и вдохните через левую ноздрю. Закройте вашу левую ноздрю при помощи безымянного пальца и выдохните через правую ноздрю. Затем произведите вдох через вашу правую ноздрю. Закройте правую ноздрю и затем выдохните через левую ноздрю. После этого сделайте вдох через левую ноздрю. Продолжайте эту схему в течение 10 кругов.

«Аутогенные тренировки»

Аутогенные тренировки помогают снять психологическое напряжение, избавляют от тревожности, повышают работоспособность и улучшают настроение.

Заняв удобную позицию, расслабившись и закрыв глаза, следует произносить следующие фразы:

- я совершенно расслаблен и спокоен;
- все части моего тела расслаблены и наполнены теплом;
- мое сердце бьется ровно и спокойно;
- из моей головы исчезают все неприятные мысли;
- я люблю жизнь и живу в гармонии с этим миром;
- я избавляюсь от тревожности и страха;
- я уверен в себе и могу справиться с любой проблемой.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью. Применение предложенных способов и приемов помогут уберечь себя и своих близких от преступных действий злоумышленников.

«Остановите поток мыслей».

Один из популярных способов, чтобы выбросить лишние мысли из головы, это хлопнуть в ладоши и крикнуть: «Стоп! Я подумаю об этом потом!».

Можно носить резинку на запястье и щелкать себя ей (или просто ущипнуть себя). Используйте подобные раздражители, чтобы остановить круговорот мыслей и отложить проблему на потом, на определенное время. Затем постарайтесь переключить свое внимание на какой-либо необычный предмет или занятие.

Разместите в квартире на видном месте на уровне глаз яркое изображение, картину или просто лист бумаги красного цвета. Приучите себя при стрессовой ситуации во время общения с незнакомцами обратить внимание

на это изображение. Рядом разместите памятку, как уберечься от мошенников с телефонами экстренных служб, родственников, знакомых. (приложение 1). Такую же памятку можно разместить у входной двери, возле телефонного аппарата.

Глава 16 Минимизация риска стать жертвой мошенничества

Во-первых, поможет знание о возможных схемах мошенничества. Главное, что надо помнить: если кто-то, кем бы он ни представлялся и какую бы историю ни рассказывал, спрашивает у вас по телефону код из СМС, трехзначный код с обратной стороны карты или просит куда-то перевести деньги, - это однозначно мошенник. Важно не просто знать, а написать правила безопасности, сделать себе и своим родственникам памятки.

Дело в том, что в состоянии высокой тревоги мы можем растеряться, забыть, что нужно хранить в секрете, или, чувствуя себя неуверенно, поддаться на авторитетные требования мошенников, и тогда памятка очень пригодится в качестве «опоры».

Во-вторых, всегда берите паузу перед тем, как принять какое-то решение, предпринять важное действие. Даже если эта пауза будет длиться всего минуту, есть возможность сориентироваться, что тут вообще происходит, не подозрительно ли всё это. Вспомните самый надежный способ – немедленно прекратить разговор и закрыть дверь или положить трубку. Мошенники настаивают на немедленном принятии решения, быстрых действиях, дают пошаговую инструкцию, и, после преодоления первых сомнений и совершения первых шагов, человек дальше совершает действия по инерции. Очень важно после поступления первой информации взять паузу, и это касается любых видов мошенничества – такая рекомендация универсальна. Никогда не принимайте решения, находясь под влиянием сильных чувств: тревоги, восторга («Ого, какое выгодное предложение!»), возмущения. Дайте себе возможность обдумать, проверить информацию, посоветоваться.

В-третьих, по возможности привлеките к разговору кого-то ещё (родственника, коллегу, соседа по лестничной клетке). С большой долей вероятности другой человек будет менее эмоционально затронут (не его же деньгам угрожает опасность) и сохранит более критический взгляд на происходящее. Дублируйте ему то, что говорит и просит сделать звонящий, вам будет проще с такой поддержкой разобраться в ситуации и устоять перед давлением (или обаянием) мошенника. Также рекомендуется повысить свою финансовую грамотность и изменить отношение к личным данным, в особенности к телефону. В наши дни телефон уже фактически является новой формой кошелька. Поэтому относиться к нему стоит соответствующе. Не передавать данные незнакомым людям, не переходить по сомнительным ссылкам, не устанавливать сомнительных приложений и вообще соблюдать осторожность.

Позвонив потенциальной жертве, мошенник сначала нагнетает напряжение, вызывает чувство тревоги, паники. Как только человек замешкался, и на минуту поверил в происходящее, то тут подключается вполне естественная реакция -

он теряется, испытывает страх за своих близких, за свои сбережения. В таком состоянии люди естественным образом ищут опору, спасителя, которым и выступает злоумышленник. Жертве внушается, что нужно выполнить всего несколько операций, сообщить некоторые данные и все, деньги будут спасены! Плюс, стоит повысить уверенность в себе, научиться вести диалог на равных со всеми. Это поможет перехватить инициативу в диалоге с мошенником и не стать ведомым.

Это, как если бы вы вдруг поняли, что заблудились в лесу: скоро совсем стемнеет, вы не понимаете, что делать, к тому же увидели следы диких животных. Нарастет тревога... И вдруг появляется лесник, он уверенно заявляет, что ничего страшного не происходит, все хорошо. Нужно всего лишь дойти до той березы, перебраться через овраг, через двести метров повернуть налево, потом пройти прямо с полкилометра к деревне. И вы, скорее всего, выполните советы лесника, потому что он знает лес, знает, что делать, и он действует в целях вашей безопасности.

Глава 17 Противодействие манипулятивному воздействию

Манипулятивное общение часто оставляет эмоциональный отклик. Формулы внушения могут быть, например, такими: «Ты сможешь это сделать», «Это в твоих силах», «Вы добьетесь успеха!» и т. п. Внушение может быть и негативным: «Вам не справиться с этим», «У вас будут большие трудности», «Вы вряд ли уложитесь в отведенное время» и т. п. Внушение отличается от заражения тем, что в первом случае инициатор влияния сам находится в одном состоянии, а у адресата (чаще – адресатов) влияния производит другое. Заражение подразумевает, что инициатор сам находится в том состоянии, которое он воспроизводит в других людях. К числу личностных факторов, обеспечивающих эффективность – внушения и заражения, а также пробуждения импульса к подражанию, формирования благосклонности целевой персоны и просьбы относится таинственный «личный магнетизм», «обаяние», «харизма» и др.

Мониторинг – это сплошное наблюдение явления в его полной динамике; сканирование, прослеживание. Мониторинг необходим для того, чтобы выявить эмоциональные признаки начинающейся манипуляции. Некоторые изменения в эмоциональном состоянии адресата являются достоверными признаками того, что манипулятор начал свою «работу» с его эмоциональными струнами.

К числу таких признаков относятся:

- дисбаланс – противоречивость эмоций, например, сочетание гордости и обиды, радости и недоверия, умиления и тревоги, или, например, «когда одновременно смешно и неприятно», и т. п.;

- «странность» эмоций, например, вспышка ярости в момент обсуждения несущественных подробностей плана действий; безотчетный страх в процессе мирного обсуждения объема будущих действий и т. п.;

- повторяемость эмоций, например, систематическое возникновение одних и тех же эмоций при встрече с определенным человеком, чувства вины, профессиональной некомпетентности, унижения, протеста и т. п.;

- резкий всплеск эмоций, который не кажется оправданным объективными характеристиками ситуации;

- «странность» эмоций также объясняется тем, что задета одна или несколько наших чувствительных струн, причем столь искусно, что нам даже не удалось заметить, когда и как это было сделано;

- повторяемость эмоций может свидетельствовать о том, что данный манипулятор постоянно играет на одной и той же нашей струне, которая с готовностью начинает звучать при его появлении;

- резкий всплеск эмоций – это, пожалуй, самая важная характеристика, которая должна быть проанализирована в первую очередь. Однако парадокс состоит в том, что при возникновении интенсивной реакции мы забываем о мониторинге. Поэтому тот индикатор, который легче всего заметить, оказывается

самым трудным для практического применения. Вместо того, чтобы использовать собственную эмоцию, как важный информационный сигнал, мы отдаемся во власть этой эмоции.

В настоящее время разработано много различных способов саморегуляции: релаксационная тренировка, аутогенная тренировка, реактивная релаксация, медитация и др. Частные способы регуляции эмоционального состояния (например, использование дыхательных упражнений, психическая регуляция, использование «защитных механизмов», изменение направленности сознания) в основном укладываются в три глобальных способа.

- Посредством другой эмоции. Первый способ регуляции предполагает сознательные усилия, направленные на активацию другой эмоции, противоположной той, которую человек переживает и хочет устранить.

- Когнитивная регуляция. Второй способ связан с использованием внимания и мышления для подавления нежелательной эмоции или установления контроля над ней. Это переключение сознания на события и деятельность, вызывающие у человека интерес, положительные эмоциональные переживания.

- Моторная регуляция. Третий способ предполагает использование физической активности как канала разрядки возникшего эмоционального напряжения.

Глава 18 Техники саморегуляции эмоционального состояния

В ситуации манипулятивного воздействия человек может описывать свое состояние следующими словами: «Я вышел из себя...», «я потерял душевное равновесие», «я забыл обо всем». С точки зрения телесных практик можно сказать, что человек потерял равновесие, потерял ощущение своего Центра. Стал нецентрированным. Центрирование – это способность устанавливать контакт со своей природной сущностью, что позволяет иметь эмоциональную стабильность и спонтанно проявляться в разных жизненных ситуациях.

Центрирование через практики внимательности. Практика центрирования является практикой предупреждения и купирования стрессовой реакции. Если научиться центрироваться в момент распознавания «сигналов угрозы», а именно сразу после того, как заметишь маленькое волнение или небольшую тревогу – а не тогда, когда уже внутреннее напряжение зашкаливает и готов пуститься во все тяжкие. Если это практиковать достаточно долго, то есть центрироваться по триста раз на дню, то в какой-то момент тело само запоминает это состояние и уже удерживает его без постоянных ментальных напоминаний.

Короткая версия центрирования. Ощутить, как стопы (или подошвы обуви) касаются пола. Выпрямить позвоночник, мысленно потянуться головой к небу. Расслабить язык и нижнюю челюсть. Ощутить свое дыхание, сделать естественный вдох животом и грудной клеткой.

Длинная версия центрирования. Устремитесь вверх, вытянув позвоночник, займите достойную позу. Вдохните и направьте долгий выдох вниз вперед, ослабив напряжение в грудной клетке. Почувствуйте свой язык, по возможности ослабьте напряжение в челюстях. Раздвиньте мысленно границы вашего личного пространства, заполнив комнату во всех направлениях. Почувствуйте себя комфортно в этом пространстве

Улыбка Будды. Упражнение «Улыбка Будды» позволит вам легко приходиться в состояние душевного равновесия. Успокойтесь и постарайтесь ни о чем не думать. Полностью расслабьте мышцы лица и представьте, как они наливаются тяжестью

и теплом, а затем, потеряв упругость, как бы «стекают» вниз в приятной истоме. Сосредоточьтесь на уголках ваших губ. Представьте, как губы начинают слегка раздвигаться в стороны, образуя легкую улыбку. Не прилагайте мышечных усилий. Вы почувствуете, как ваши губы сами растягиваются в едва уловимую улыбку, а во всем теле появится ощущение зарождающейся радости.

Техника дыхания через живот. Дыхание способно не только приносить живительный кислород в организм, но и помогать нам в критических ситуациях. С помощью глубоких вдохов и медленных выдохов человек быстрее успокаивается, избавляется от панических атак, сохраняет ясность ума. Глубоко

вдохните через нос, раскрывая легкие и диафрагму. Выдыхайте медленно, ртом. Семь таких вдохов-выдохов способны привести ваш организм в состояние покоя, снизить частоту сердечных сокращений и тем самым стабилизировать давление.

Управляемая визуализация. Закройте глаза, расслабьтесь и представляйте себе приятные моменты из жизни, запоминающиеся образы городов, строений, лица близких родственников, детей, домашних животных – все то, что способно вас обрадовать и поднять настроение. При этом медленно вдыхаете воздух через нос и так же медленно выдыхайте его. Вскоре вы найдете необходимый ритм и полностью расслабитесь.

Практическое задание. Отработка техники преобразования негативных чувств в позитивные действия как способа выхода из негативных состояний, вызванных чужим влиянием. Сначала нужно осознать, что чувство раздражения и гнев являются источником очень сильной энергии. Каждый день эта энергия, неуловимая и неукротимая, причиняет бесчисленные разрушения вокруг и внутри захлестываемого ею человека. Но важно понимать, что сама по себе энергия нейтральна. Та же самая энергия, которая разрушает, может и созидать. Не следует пытаться подавлять ее. Это неразумно, так как на это требуется еще более сильная энергия. Затраты слишком велики. Они опустошают, они разрушают человека. Необходимо научиться трансформировать ее разрушающее начало в созидательное. Вы можете преобразовать агрессивную энергию, направив ее на иной объект и придав ей иную форму проявления.

Следующее упражнение необходимо выполнять, когда вы испытываете какие-то агрессивные чувства или близки к тому, чтобы испытать их. Выберите какой-то проект или деятельность, в который вы хотели бы «поддать пару». Теперь отложите проект в сторону и обратитесь к своим агрессивным чувствам. Ощутите их силу, эффект, оказываемый ими на ваше тело и, возможно, причиняемое ими страдание. Дайте им место в своем сознании, наблюдайте за ними без каких-либо оценок, без навешивания ярлыков. Теперь осознайте, что все эти чувства представляют собой драгоценную энергию, которая находится в вашем распоряжении и может быть использована для дела. Она способна причинить боль, но способна также стать движущей силой той деятельности или проекта, на который вы решите ее направить. Теперь живо представьте себе, что вы осуществляете этот проект или деятельность. Представьте это в мельчайших деталях и подробностях. Представьте происходящие изменения, но представьте их проникнутыми и усиленными той жизненной энергией, которую вы решили в них вложить.

Метод диафрагмального дыхания не более 5 минут. Вдох животом через нос, затем задержка дыхания на 2-3 сек., и выдох через рот, губы трубочкой до 8-10 сек. На выдохе про себя говорим: Здесь и сейчас я вижу и называю 5 объектов, которые находятся перед вами; затем: Здесь и сейчас я слышу и тоже сосредоточиться

на звуках. Здесь и сейчас я чувствую, сосредоточиться на телесных ощущениях. Затем, после этого, на выдохе проговаривать: здесь и сейчас я совершенно спокоен, здесь и сейчас меня ничто не тревожит. Затем переключаемся на свободное дыхание и представляем себя на природе, образ вашего самого уютного уголка в природе (речка, море, горы, водопады) и несколько минут побыли там.

Белый экран. Этот способ позволяет не только «разгрузить мозги», но и улучшить процесс засыпания и сам сон. Вечером перед сном надо лечь на кровати и закрыть глаза, представив «белый экран» перед глазами. Как только на «экране» начнут появляться картинки, образы, спровоцированные мыслями, надо тут же «очищать экран», заполняя его белым цветом.

Выписывание на бумагу. Писать много и без анализа, не подбирая слова. Писать все, что приходит в голову и без разбора. Выплескивая на бумагу эмоции, пережитое и навязчивое, чтобы освободиться от гнета мыслей. И не обязательно это потом перечитывать, можно просто выбросить. Этот способ даже позволит, как «ниточке к душе», добраться до самого сокровенного, до тех проблем, которые мучают. И решить их.

Удалить от себя токсичных людей. Тех, кто постоянно чем-то недоволен, жалуется на всё и всех, неудачников, сидящих на месте и не стремящихся двигаться куда-либо. Такие люди наносят очень большой вред вашему энергетическому балансу. Они распространяют негатив, который проникает в вас. Если вы не можете перевоспитать или перенастроить такого человека, лучше свести общение к минимуму.

Прогулки на свежем воздухе. Гулять в парке или за городом. Достаточно 20-минутной прогулки на природе, чтобы избавиться от потока мыслей, чтобы получить новый толчок к вдохновению.

Пишите списки. Это может быть список дел на день, которые вы держите в голове, список покупок, или список обид, которые регулярно «проживаются» в голове. Любой из списков автоматически освобождает голову от «мусора».

Подготовка ко сну. Уделите перед сном 20 минут себе. Лягте, расслабьтесь и мысленно прокрутите в голове прошедший день. Сделайте такой себе виртуальный тур по всем событиям, в которых вы принимали участие. Представьте, что ваш мозг - это компьютер, в котором открыто множество окошек - это и есть ваши события за день. Необходимо нажать крестик в крайнем правом углу каждого окошка, ибо не закрытые программы за день накапливаются, зависают, мешают и не дают продуктивно работать даже самому сверхмощному компьютеру, каким и является наш мозг. Анализируем событие, свои чувства, эмоции, мысли и поведение, сделали выводы и принимаем решение на будущее. Сон будет спокойным и глубоким, а завтра все начнем с чистого листа.

Научитесь останавливаться. Социальные сети, телевидение и другие источники информации не только помогают нам жить активно, но и «засоряют» мозг, держат его в постоянном напряжении. И об этом стоит помнить. Давайте

учиться просеивать информацию, оставляя для себя лишь важную и необходимую. Отключайте время от времени гаджеты, освоите медитацию, методики релаксации, или просто посмотрите в окно так, будто картину за ним вы видите впервые. Путешествуя по городу, на природе представляйте, что вы в новом незнакомом для себя месте. Посмотрите на привычную картину как-бы новым взглядом. Рассматривайте, любуйтесь и живите как самый счастливый человек в мире. Ведь мозг после «генеральной уборки» будет на вашей стороне.

Четко отредактировать свой план целей и список дел. Почти каждый из нас забивает голову огромным списком дел, которые необходимо выполнить сегодня или в течение месяца. Не успеваете, расстраиваетесь и переносите на следующий день. И так длится бесконечно. Что-то делается, но совсем не в том темпе, как хотелось бы. Крутитесь как белка в колесе, а жизнь проходит мимо. Не стоит хвататься за всё и сразу. Проанализируйте и расставьте приоритеты по 10-бальной шкале (10- самое важное, 1 - самое неважное), по возможности делегируйте ряд задач на близких, выполняйте по очереди.

Мгновенное снятие напряжения.

Сядьте, вдохните. сильно, насколько можете, напрягите все мышцы тела, включая мышцы лица, пресса, рук, ног, сожмите кулаки. Выдержите паузу в несколько секунд. Выдохните и максимально расслабьтесь. Получите мгновенный результат. Если не удалось полностью расслабиться, повторите несколько раз. И осваивайте методику до тех пор, пока не научитесь стряхивать напряжение с первого раза. Правило: не забывайте расслабляться.

Повышение работоспособности и продуктивности. Каждый день лучше до 3-х раз садитесь, закрывайте глаза и в течение пяти минут упрямо улыбайтесь. Сознание при этом концентрируется на улыбке, не на мыслях. Важно, что бы вы просидели не меньше пяти минут, а потом можете снова возвращаться к работе. Правило: цените отдых.

Избавление от состояния тревоги. Восстанавливаем связь с телом, просто включите ощущения, начните практиковать осознанность и победите не только тревогу, но и множество других психологических дисфункций. Упражнение «Здесь и сейчас». (здесь и сейчас я чувствую правую руку, левую руку, живот, правую ногу, левую ногу и т. д.) Правило: помните о телесных ощущениях.

Как быстро перестать думать о плохом. Закройте глаза, обратись к источнику негатива – то есть к тому воспоминанию, из которого исходят плохие мысли. Скажите мысленно: «Благодарю за опыт. Я принимаю свои ошибки и прощаю себя. Прости и ты меня». Сказав так, обязательно улыбнитесь. Сделайте все это от души и вам тут же станет значительно легче. Правило: принимайте, прощайте, благодарите.

Освобождение ума от ментального мусора. Для этого необходимо дважды в день – после пробуждения и перед сном – заниматься 5-10 минутной медитацией. Медитируйте дважды в сутки, и душа скажет: спасибо. Цель медитации – снизить

активность коры головного мозга. Все остальное мозг сделает сам. Как это делается. Сядьте удобно. Закройте глаза. Расслабьтесь. Дышите ровно. Останавливайте поток мыслей. Не думайте абсолютно ни о чем в течение 5-10 минут. Правило: избавляйтесь от ненужных мыслей.

Заключение

Значительные меры по борьбе с преступной деятельностью и по профилактике правонарушений принимаются со стороны правоохранительных органов и в других государственных структур на всех уровнях. Эта работа уже составляет неотъемлемую часть повседневной деятельности. Поскольку все мы так или иначе погружены во взаимоотношения с незнакомыми нам лицами, особенно удаленное общение при помощи технических средств, 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. Самообразование в сфере компьютерной и финансовой грамотности должно происходить постоянно.

Позвонив по Единому социальному телефону Свердловской области **8-800-300-81-00**, можно достоверно узнать о социальных услугах и выплатах, порядке их предоставления. Для оперативного реагирования на происки злоумышленников 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**, и банков, где открыты счета и вклады. Периодически напоминать об этом 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

1. Портал Госуслуги [Электронный ресурс] URL: <https://www.gosuslugi.ru/cybersecurity> (дата обращения: 07.11.2024).
2. Официальный телеграм-канал УБК МВД России. [Электронный ресурс] URL: https://t.me/cyberpolice_rus/2972 (дата обращения: 28.01.2025).
3. Киберпреступники (Социальные инженеры) погружают жертву в тайну — Немов Филипп, генерал-майор полиции [Электронный ресурс] URL: https://vk.com/video-165808579_456241167 (дата обращения: 07.11.2024).
4. Официальный сайт ГУ МВД России по Свердловской области [Электронный ресурс] URL: <https://66.мвд.рф/news/item/53323545> (дата обращения: 07.11.2024).
5. Подробное интервью потерпевшей от действий мошенников. Разбор многоходовой операции по схеме «звонок от оператора связи о продлении договора» [Электронный ресурс] URL: <https://yandex.ru/video/preview/5106133420035387881> (дата обращения: 07.11.2024).
6. Я и моя «тень». Как мошенники собирают на нас информационное досье? [Электронный ресурс] URL: <https://ural.aif.ru/society/ya-i-moya-ten-kak-moshenniki-sobirayut-na-nas-informacionnoe-dose> (дата обращения: 07.11.2024).
7. Фильм "Цифровой след: что ты лайкнул?", открывающий мир, где каждый шаг фиксируется и тщательно исследуется [Электронный ресурс] URL: <https://yandex.ru/video/preview/16312116773078272954> (дата обращения: 07.11.2024).
8. Свердловский врач составил психологический портрет жертвы и рассказал, как мошенники манипулируют нами и как от них защититься [Электронный ресурс] URL: <https://www.mzso.info/articles/novosti-minzdrava/sverdlovskiy-vrach-sostavil-psikhologicheskiy-portret-zhertvy-i-rasskazal-kak-moshenniki-manipuliruyut/> (дата обращения: 07.11.2024).
9. Российская газета. Телефонные мошенники развернули охоту за финансовыми картами несовершеннолетних [Электронный ресурс] URL: <https://rg.ru/2024/08/05/bankiry-i-malchishki-a-takzhe-ih-roditeli.html?ysclid=m3sp6i94wy15365259> (дата обращения: 07.11.2024).
10. Безсонов Д.В. «Методы информационно-психологического влияния, применяемые украинскими подразделениями информационно-психологических операций против участников СВО, их родственников и других граждан». [Электронный ресурс] URL:

https://vk.com/doc205712135_673321980?hash=09DyAxNUlaEzD0L4fZUXihS2sNofmCRFCHQrlEgwSTT (дата обращения: 07.11.2024).

11. Официальный телеграм-канал УБК МВД России. [Электронный ресурс] URL: https://t.me/cyberpolice_rus/1803 (дата обращения: 07.11.2024).

12. Читайте на WWW.KP.RU [Электронный ресурс] URL: <https://www.kp.ru/daily/27560/4828951/> (дата обращения: 07.11.2024).

Список рекомендуемой литературы

1. Дементьев М. Кинетический интеллект / М. Дементьев. – М.: АСТ, 2024. – 240 с.
2. Дилтс Р. Фокусы языка. Изменение убеждений с помощью НЛП / Р. Дилтс. – М: Прогресс книга, 2024. – 384 с.
3. Литвак М. Психологическое айкидо / М. Литвак. – М.: АСТ, 2024. – 224 с.
4. Экман П. Психология лжи. Обмани меня, если сможешь / П. Экман. – М.: Питер, 2022. - 480 с.
5. Экман П. Психология эмоций. Я знаю, что ты чувствуешь / П. Экман. – М.: Питер, 2023. - 336 с.
6. Манипуляции во взаимодействии и способы их нейтрализации / Сост. М. Д. Иванова. – Тирасполь: Изд-во Приднестровского университета, 2024. – 136 с. [электронный ресурс] URL: http://pedagog.spsu.ru/images/files/bibl/bibl_2024_%2002-02_man.pdf (дата обращения: 07.11.2024).

Приложение 1

Что важно знать пожилым людям, чтобы защититься от МОШЕННИКОВ



	Распространенные виды обмана		Будьте бдительны!
!	Позвонил якобы родственник, который попал в ДТП и просит денег. Пришло сообщение в Ватсап или Телеграм от знакомого с просьбой одолжить денег.	*	Не торопитесь соглашаться, позвоните сами на его телефон или другим родственникам.
!	Проникновение в жилище под видом работников разных госслужб, проверки окон, установки счетчиков.	*	Не принимайте незнакомых людей, когда вы одни. Позвоните в учреждение, от которого пришли незнакомцы, старшему по дому, в ТСЖ или Управляющую компанию.
!	Позвонили по телефону и представились сотрудниками банка, сотовой компании, МВД, ФСБ, прокуратуры.	*	Немедленно кладите трубку, не разглашайте личную информацию: ФИО, сведения о паспорте, пароль, код из СМС, данные банковской карты (номер, срок действия и трехзначный код).
!	Посещение квартир с сообщениями о надбавке к пенсии, перерасчете квартплаты, обмене денег "для ветеранов и пенсионеров".	*	Не давайте никаких устных и письменных подтверждений. Позвоните в полицию.
!	Продажа дорогостоящих товаров с навязанной рекламой или с большими скидками «только один день», предложение медицинского обследования.	*	Позвоните родственникам, соседям, обратитесь в комитет по защите прав потребителей. Скорее всего, это мошенники. Не совершайте такие покупки без обсуждения с близкими.

Куда звонить

Полиция: **02, 102, 112**, дежурная часть отдела полиции _____

Адрес отдела полиции: _____

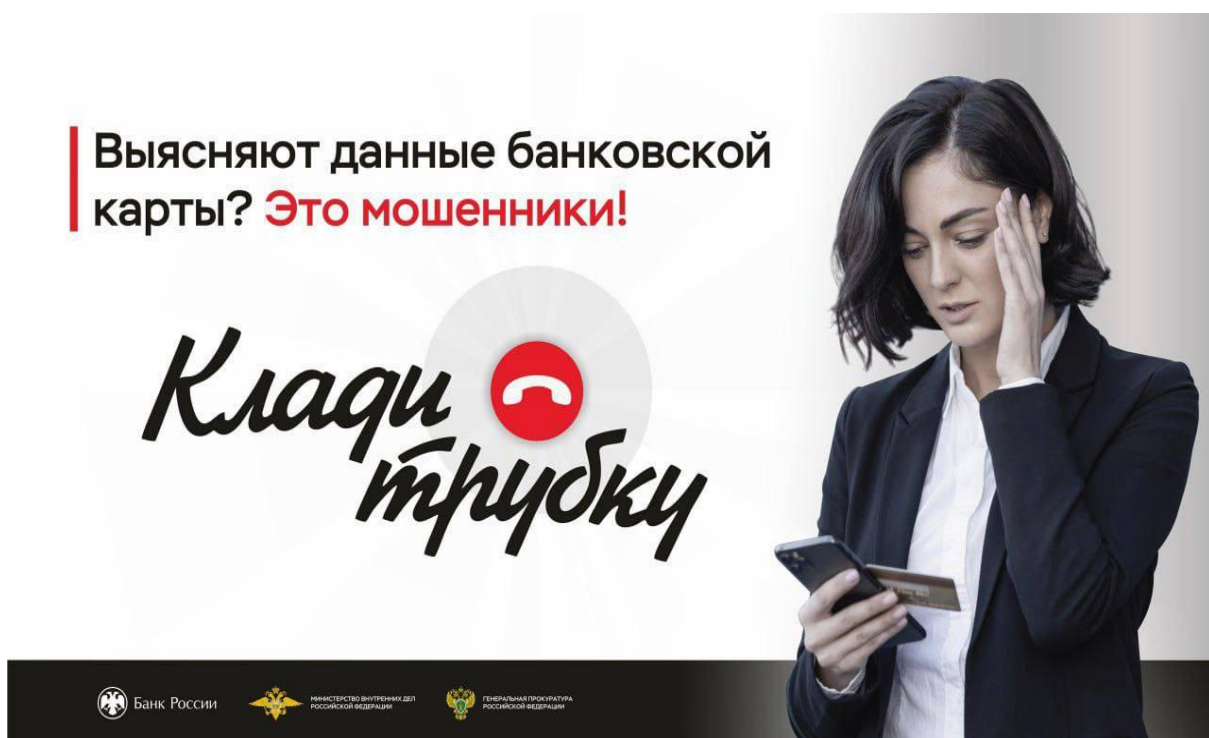
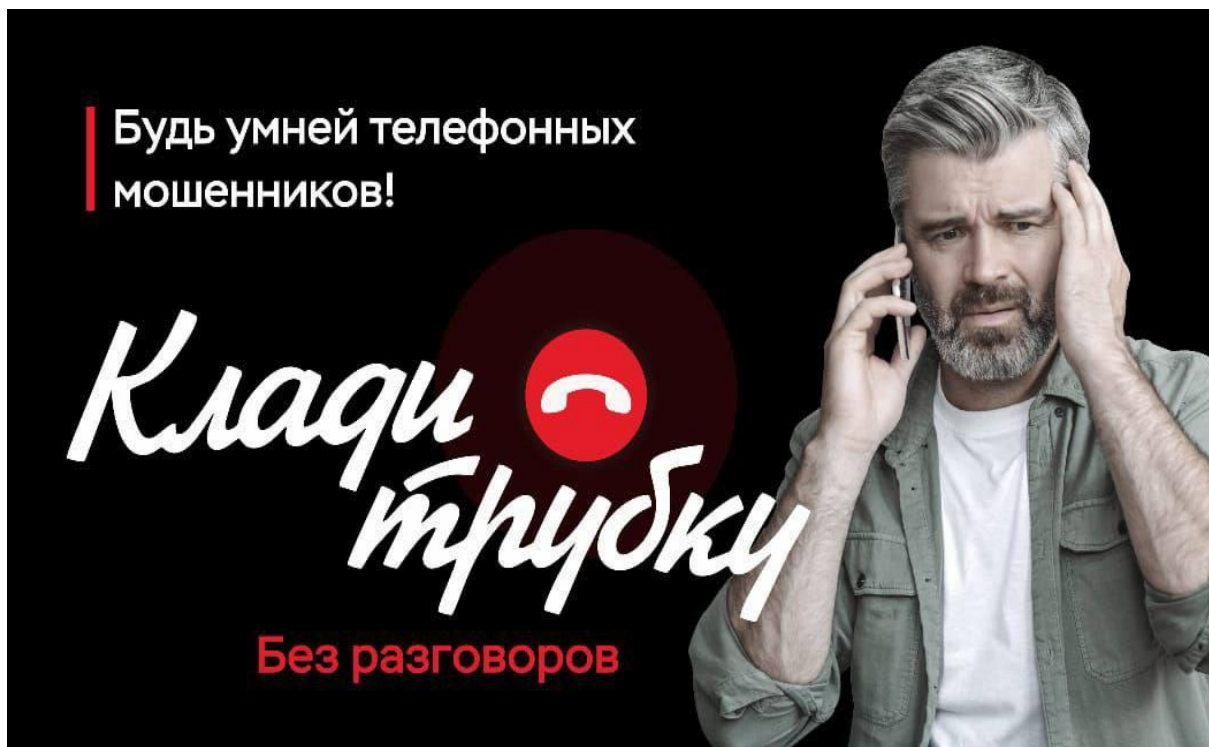
Участковый уполномоченный полиции: _____

Телефон доверия ГУ МВД России по Свердловской области: **(343) 358-71-61, (343) 358-70-71**

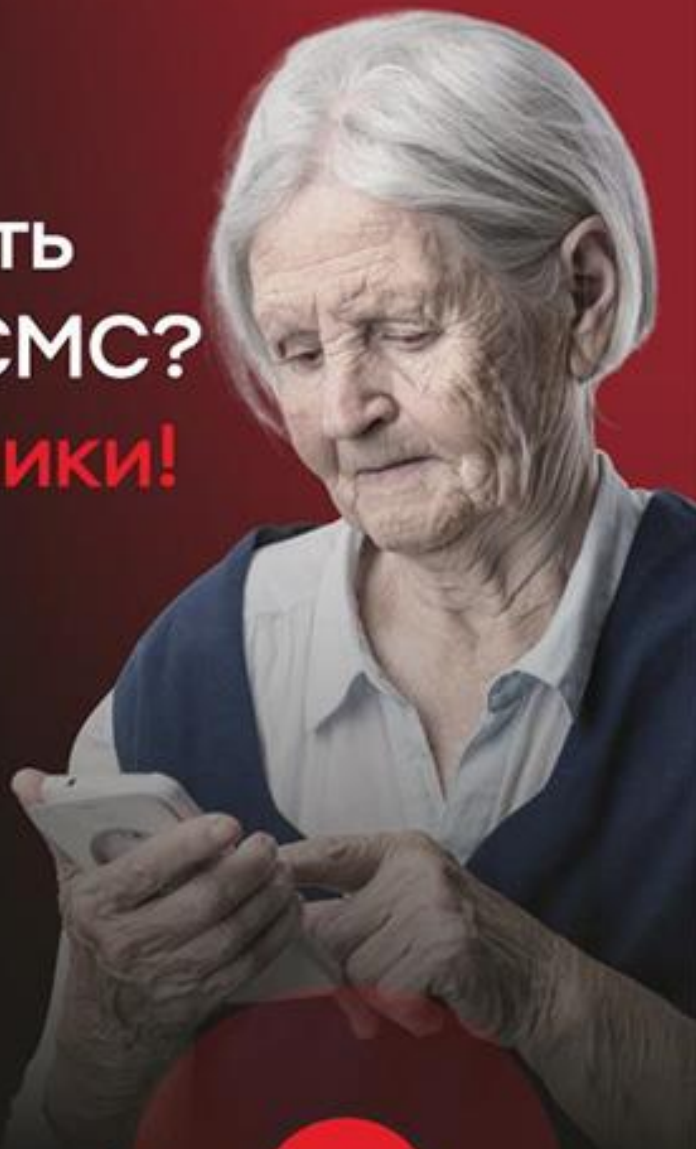
Управляющая компания, ТСЖ, администрация _____

Родственники, соседи: _____

Приложение 2: Образцы листовок



Просят
сообщить
код из СМС?
Мошенники!



Клади
трубку



Без разговоров

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!

