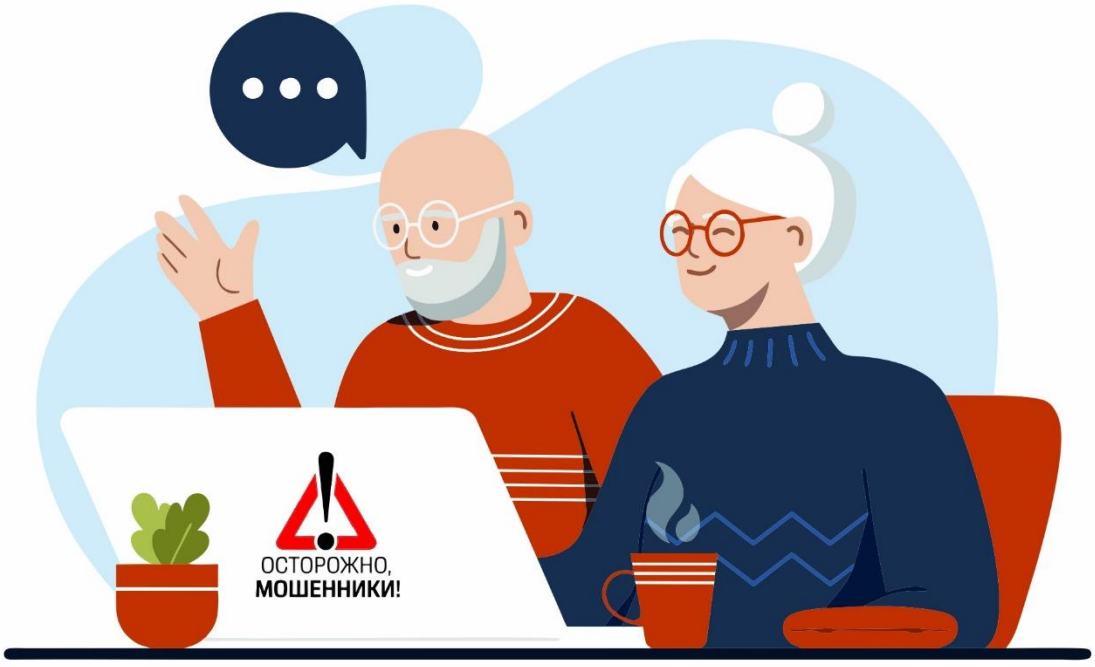
ОСНОВЫ БЕЗОПАСНОЙ ЖИЗНИ ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

ЭЛЕКТРОННОЕ МЕТОДИЧЕСКОЕ ПОСОБИЕ
(Выпуск 2)



Сургут, 2025

Департамент социального развития
Ханты-Мансийского автономного округа – Югры

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

ОСНОВЫ БЕЗОПАСНОЙ ЖИЗНИ ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

ЭЛЕКТРОННОЕ МЕТОДИЧЕСКОЕ ПОСОБИЕ
(Выпуск 2)

Бюджетное учреждение
Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»
Сургут, 2025

Дорогие граждане!

Представляем Вашему вниманию актуализированное, дополненное и переработанные с учетом новых видов мошенничества электронное методическое пособие, выпуск 2.

Мошеннические схемы с каждым разом становятся вся более изощренными. Злоумышленники действуют без капли сострадания и выбирают наиболее уязвимых граждан, таких как пенсионеры или людей, попавших в сложную жизненную ситуацию. Мошенники регулярно придумывают новые схемы обмана и модернизируют старые, чтобы ввести в заблуждение граждан и заполучить их финансовые средства. На фоне стремительного развития нейросетей мошенники все чаще используют их в преступных целях.

Как показывает практика, наказать виновных, добиться справедливости и вернуть утраченные средства практически невозможно. Поэтому наша главная цель остается прежней – предупредить угрозу: предупрежден – значит вооружен.

СЛОВАРЬ ТЕРМИНОВ

SIM-свопинг (подмена SIM-карты) – это метод кибератаки, при котором злоумышленники «угоняют» чужой мобильный номер и переносят его на устройство, принадлежащее атакующему.

Антивирус (антивирусное программное обеспечение, средство антивирусной защиты) – специальное программное обеспечение для обнаружения вредоносных программ и восстановления поврежденных ими файлов.

Вредоносное программное обеспечение (Malware) – это приложения или коды, получающие несанкционированный доступ к компьютерным системам и размещенным в них данным.

Дипфейк (от англ. deepfake – глубокий обман, достоверная подделка) – фальшивое видео, аудио или изображение, созданное с помощью алгоритмов искусственного интеллекта, чаще всего нейросетей.

Дропперы (дропы) – это люди, которые выступают в роли посредников в нелегальных схемах, связанных с финансовыми операциями. Они соглашаются получить на свой счет деньги, добытые незаконным путем, и затем перевести их другим лицам. Чаще всего – за определенное вознаграждение.

ЕГИСЗ – единая государственная информационная система в сфере здравоохранения.

Искусственный интеллект (от англ. artificial intelligence) – это интеллект, демонстрируемый машинами, в частности, компьютерными системами.

Нейросеть (искусственная нейронная сеть) – это компьютерная программа, вдохновленная работой человеческого мозга.

Спуфинг (от англ. spoof – обман, подделка) – это кибератака, при которой мошенники маскируются под других людей или компании.

Фейк – что-либо ложное, недостоверное, сфальсифицированное, выдаваемое за действительное, реальное, достоверное с целью ввести в заблуждение.

Фишинг (от англ. fishing – рыбачить, выуживать) – вид интернет-мошенничества, главная цель которого – получить данные пользователей.

КОРОТКО О МОШЕННИЧЕСТВЕ

«Старики всему верят,
люди зрелого возраста во всем сомневаются,
молодые все знают»

По данным банковских аналитиков, которые постоянно отслеживают объемы мошеннических операций, к основным категориям риска относятся:

граждане в возрасте 70+;

вдовцы старше 65 лет;

одинокие женщины в возрасте от 50 лет.

Все эти граждане гораздо чаще выступают в роли мишени, чем остальные категории россиян. Службы безопасности банков выявили, что мужчины всех возрастов в три раза реже страдают от мошенничества, чем женщины. Меньше всего злоумышленники пытаются завладеть данными и деньгами клиентов банка в возрасте от 25 до 45 лет.

Уязвимость пожилых людей достаточно просто объяснить. В их молодости не было такого обилия информации, которую требовалось зашифровывать, запоминать и использовать. Кроме того, пенсионерам постоянно приходится сталкиваться с развитием и изменением в технологиях. Иногда они просто не успевают за этим следить.

Вдовцы, старше 65 лет отличаются в два раза большей уязвимостью по сравнению с вдовами того же возраста. Считается, что мужчины, побывавшие в браке, оказываются менее приспособленными к жизни в одиночестве, чем женщины. Но если мужчина всю жизнь был одинок и не состоял в браке никогда, он показывает в три раза большую осмотрительность, чем те женщины, которые вообще не были замужем.

Наиболее распространенные зацепки, которые используют мошенники для выманивания денег у жертвы – психологические триггеры или болевые точки:

тревожность из-за неумения приспособиться к современным условиям жизни;

желание вернуть молодость, здоровье, красоту;

одинокое проживание;

жадность или получение легкой наживы;

страх сказать «нет» и выглядеть грубым, невоспитанным, бесчувственным;

сложное финансовое положение;

стремление быть нужным и полезным;

привычка подражать или не выделяться из социума;

трудная жизненная ситуация и вера в чудеса и сверхъестественное;

неловкость при обращении за помощью к близким людям, которая толкает на необдуманные действия;

жалость, сопереживание;

стремление помочь обездоленному, больному или нуждающемуся.

Злоумышленники в настоящее время активно применяют искусственный интеллект (далее – ИИ): модулируют голоса родственников и знакомых, подделывают изображения. Скорость работы нейросетей такая высокая, что позволяет мошенникам создавать фейки один за другим.

Сейчас чаще всего злоумышленники пытаются получить доступ не к онлайн-банкингу, а к Госуслугам потенциальной жертвы. Ведь через эту систему можно узнать, в каких банках есть счета у человека, провернуть некоторые махинации с его недвижимостью (если не установлен запрет на это) и даже подать заявку на кредит через некоторые сервисы, привязав к ним авторизацию на Госуслугах.

Рассмотрим новые виды мошенничества более подробно.

ВИДЫ МОШЕННИЧЕСТВА

Голосовой фишинг с использованием искусственного интеллекта

Мошенники используют нейросети для клонирования голосов. Вам может позвонить «родственник» или «друг» с просьбой о помощи, но на самом деле это будет ИИ, имитирующий голос близкого вам человека.

Совет

Распознать обман сложно, поэтому будьте бдительны, если слышите в трубке знакомый голос, но собеседник просит о чем-то необычном, задавайте вопросы, ответы на которые знает только настоящий человек, или перезвоните ему сами, чтобы убедиться, что это действительно он.

Имитация голоса

Популярностью у мошенников пользуется имитация голоса. Для подделки нужен только образец речи человека (например, аудиозапись). Нейросеть анализирует его и затем озвучивает текст, имитируя носителя. Заметить неладное можно лишь на длинных записях, где ощущается неестественность речи. Голос на коротких аудиофрагментах практически не отличить от оригинала. Злоумышленники взламывают аккаунты людей, рассылают контактам просьбу помочь деньгами и для убедительности прикрепляют небольшое голосовое сообщение.

Развитие технологий открывает поистине удивительные возможности для мошенников. Сейчас появляется все больше приложений, доступных любому желающему, которые позволяют создать ваш виртуальный клон – дипфейк. Бесплатно или за небольшую плату уже можно сделать аудиозапись с голосом другого человека и даже видеозапись с его образом.

Для обмана мошенники обычно используют платные версии дорогих программ и приложений, работающих с возможностями

виртуальной реальности и ИИ, а иногда и вовсе создают свои. Высылают сообщение-подделку злоумышленники часто пожилым людям или детям, их легче обмануть. В аудио или видео, имитирующем хорошо знакомого человека, вас могут попросить срочно дать в долг, прислать данные вашей карты для перевода или прийти в назначенное место. Образцы голоса и видео мошенники берут из открытых социальных сетей или незаметно взломав ваш мессенджер.

Совет

Если в аудио- или видеосообщении вас что-то смутило, особенно если собеседник просит у вас деньги – самостоятельно, не предупреждая его, позвоните ему по телефону или видеосвязи. На текущий момент технологии позволяют злоумышленникам оперативно сгенерировать и отправить дипфейк, но в моменте сразу предстать в образе вашего знакомого большинство из них не умеет.

QR-код-ловушка

Вам приходит СМС с сообщением о выигрыше, посылке или необходимости оплатить штраф. В сообщении есть QR-код, который якобы нужно отсканировать для получения приза или оплаты. Но при сканировании этого кода на ваш телефон может быть установлено вредоносное программное обеспечение (далее – ПО), которое украдет ваши данные или деньги.

Еще одна инновационная схема – **применение поддельных QR-кодов.** С началом сезона аренды велосипедов и самокатов мошенники активизировались. Они наклеивают поддельные QR-коды поверх оригинальных на руле арендных транспортных средств. Ничего не подозревающий пользователь сканирует такой код и попадает на фальшивый сайт, имитирующий интерфейс легального сервиса аренды, и вводит данные своей банковской карты для оплаты. В результате деньги уходят мошенникам, а арендовать транспорт пользователю не удается. Как сообщает МВД России, такие случаи уже зафиксированы в различных регионах страны.

Совет

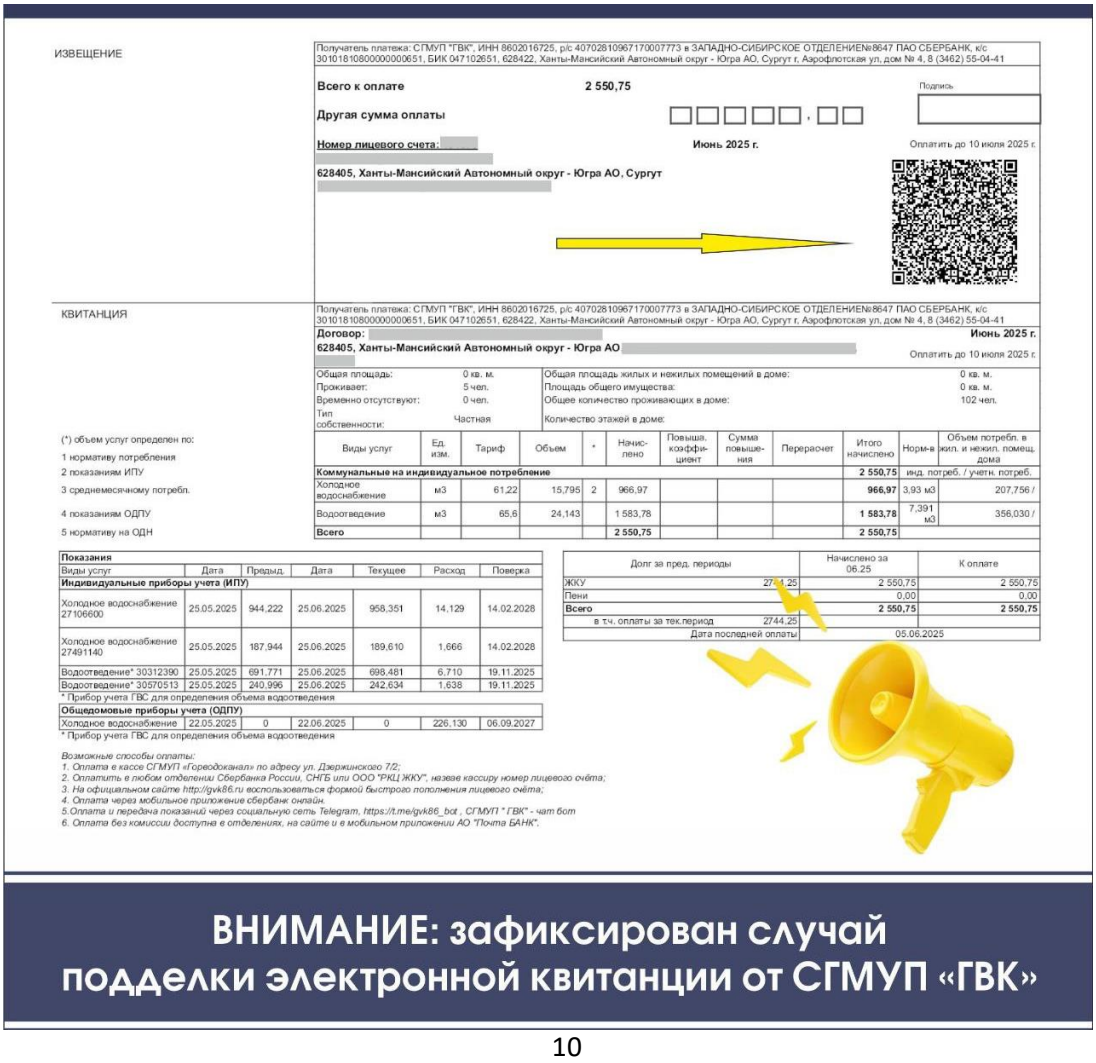
Собираясь арендовать транспорт, убедитесь, что QR-код не наклеен поверх другого и не выглядит подозрительно.

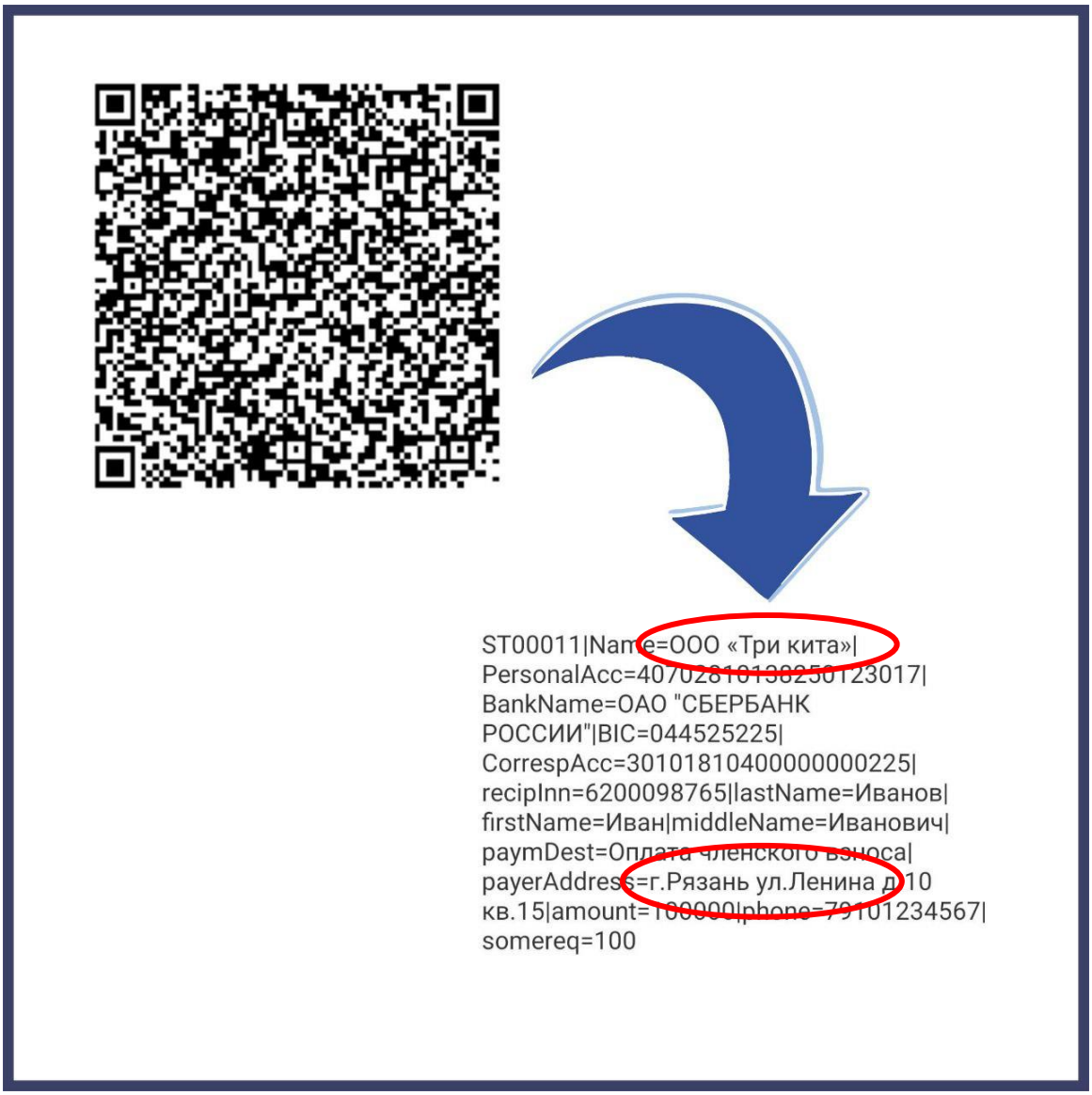
Сканируйте QR-коды только через официальное приложение сервиса аренды, а не через камеру смартфона.

Если после сканирования QR-кода вы попали на сайт, который вызывает сомнения, не вводите свои персональные данные и реквизиты банковской карты.

Если вы заметили поддельный QR-код, сообщите об этом в службу поддержки сервиса и правоохранительные органы.

Точно так же работают и **QR-коды на оплату коммунальных услуг**, о чем предупреждают управляющие компании. В Югре (г. Сургут) уже зафиксированы случаи подделки электронных квитанций от СГМУП «Горводоканал». Квитанции полностью идентична оригиналу, заменен только QR-код. Он ведет на оплату некого «членского взноса» в организацию ООО «Три кита», расположенную в г. Рязани.





«Вступай в новый чат дома!»

В подъездах домов стали появляться объявления с предложением вступить в новый чат, на которых размещены поддельные QR-коды. Если человек перейдет по такому коду, его данные могут стать доступны мошенникам. В QR-коде может содержаться любая информация: ссылка на сайт злоумышленников или на скачивание вредоносной программы.

Совет

Никогда не сканируйте QR-коды из ненадежных источников.

Не указывайте личные данные на подозрительных сайтах, не скачивайте приложения из ненадежных источников.

Используйте антивирусные программы и проверенное ПО для защиты информации.

Мошенники используют новые уловки **с помощью «Системы быстрых платежей»**. Потенциальная жертва, заинтересовавшись дорогостоящим товаром в интернет-магазине, оставляет на сайте заявку на его приобретение. После чего покупателю поступает звонок или сообщение в мессенджере от человека, который представляется сотрудником этого магазина. Лжесотрудник подтверждает, что интересующий товар есть в наличии, и его даже можно приобрести со скидкой, но только при условии оплаты через «Систему быстрых платежей» по QR-коду.

В случае согласия злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Как только доверчивый покупатель подтверждает платеж, деньги отправляются на счет мошенника.

Реализация подобной мошеннической схемы возможна, когда учетные данные модераторов и администраторов таких сайтов скомпроментированы.

Совет

Общайтесь со службами поддержки онлайн-магазинов только на официальных сайтах или в официальных приложениях.

Не переходите по ссылкам, которые заманивают акциями, подарками и розыгрышами, если они размещены не на сайте интернет-магазина.

Не сохраняйте для оплаты в личных кабинетах кредитные карты и карты с овердрафтом.

Заведите отдельную карту для оплаты товаров на маркетплейсах и вносите на нее сумму, которой хватает только для оплаты конкретной покупки.

Если вы сомневаетесь, что вам звонят представители компании, положите трубку и сами позвоните в поддержку магазина по номеру, который указан на сайте.

Поддельные звонки от службы поддержки платежных систем

Вам звонят якобы из службы поддержки Visa, Mastercard или другой платежной системы и сообщают о подозрительной активности по вашей карте. Чтобы «защитить» ваши деньги, они просят предоставить данные карты или коды из СМС.

Совет

Никогда не сообщайте эту информацию по телефону.

Сотрудники платежных систем никогда не запрашивают такие данные.

SIM-свопинг с социальной инженерией

Мошенники используют социальную инженерию, чтобы убедить сотрудника мобильного оператора перенести ваш номер на новую SIM-карту, которая находится у них. После этого они получают доступ ко всем вашим аккаунтам, привязанным к номеру телефона, и могут украсть ваши деньги.

Совет

Чтобы защитить себя, используйте сильный пароль для своего аккаунта у мобильного оператора и включите двухфакторную аутентификацию.

«Срок действия вашей SIM-карты истек. Вам нужно продлить договор с мобильным оператором». Эта схема появилась не в 2025 году, а намного раньше, однако в последнее время мошенники особенно активно ее используют.

Жертве звонит человек, представляющийся сотрудником мобильного оператора, например, «МТС» или «Билайн» и сообщает, что срок действия SIM-карты истек, скоро закончится договор с мобильным оператором и нужно его продлить, в противном случае SIM-карта перестанет функционировать и/или будет заблокирована.

Якобы для того, чтобы не потерять номер телефона, злоумышленник предлагает продлить договор во время беседы, без посещения офиса. Для этого необходимо назвать код из СМС-сообщения. Естественно, никакого заключения договора не

происходит. Если назвать код, злоумышленники получат доступ к аккаунту жертвы, к онлайн-банку, электронной почте, социальным сетям, мессенджерам и даже порталу государственных услуг и смогут оформить микрозаймы или кредиты.

Совет

Никогда и никому не называйте коды из СМС по телефону.

Прерывайте подозрительный разговор, самостоятельно перезванивайте в организацию и уточняйте информацию. Номер телефона лучше посмотреть на официальном сайте компании.

Абонентские договоры по использованию или обслуживанию SIM-карт **являются бессрочными, их не нужно продлевать**. Если вам позвонил оператор для уточнения какой-либо информации, лучше обратиться в офис лично и при необходимости обновить свои данные, например, если вы поменяли паспорт.

«Крик о помощи»

Старый способ, один из самых отвратительных способов хищения денежных средств, но он до сих пор используется мошенниками. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идет на часы. Срочно необходимы дорогие лекарства, операция за границей и т. д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Совет

Мы не призываем отказывать в помощи всем, кто просит! Но!

Прежде чем переводить свои деньги, проверьте – имеются ли контактные данные для связи с родителями (опекунами, родственниками) ребенка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

Не слишком умный дом

Чем более «умными» становятся наши дома, тем больше возможностей у мошенников взломать систему, но не технологически, а психологически.

В крупных городах сейчас все чаще устанавливаются новые домофоны в многоквартирных домах. Они позволяют попасть в подъезд не только с помощью магнитного ключа, но также через приложение, а некоторые даже оснащены системой видеонаблюдения. Чтобы получить полноценный доступ к новому домофону, собственнику квартиры необходимо установить приложение и зарегистрироваться в нем, а также получить новый комплект магнитных ключей. Именно этим и пользуются злоумышленники.

Под видом представителей управляющей компании или установщиков домофонов они связываются с собственниками квартир и просят назвать код из СМС-сообщения, который якобы нужен для подключения квартиры к домофону. Для правдоподобия звонящие уточняют сколько нужно изготовить электронных ключей, как удобнее будет их получить, предлагают за отдельную плату сделать запасные. Успокоив таким образом бдительность гражданина, мошенники сообщают, что теперь у каждой квартиры будет свой код от домофона, так как общий код противоречит политике безопасности. «Персональный код домофона» отправляют жертве и просят его продиктовать. На самом деле код обычно приходит от системы Госуслуг, в которой злоумышленники пытаются сменить пароль на свой. Дальнейшее развитие схемы может варьироваться.

Совет

Любые вопросы с управляющей компанией решайте только с ней, позвонив на номер телефона, указанный на официальном сайте.

Если вам звонит сантехник, электрик или любой другой мастер, которого, по его словам, прислала управляющая компания, смело перезванивайте в ее главный офис и уточняйте этот момент.

Покажи свой экран

Это не новый способ обмана, однако в последнее время он получил вторую жизнь.

Обычно его используют при покупке какой-то вещи с рук. Злоумышленник находит объявление в сети о том, что человек продает новую или бывшую в использовании вещь, и обращается к продавцу по этому вопросу. Чтобы посмотреть вещь, злоумышленник просит созвониться по видеосвязи, но во время нее у него якобы случаются какие-то технические неполадки. Чтобы обойти их, он просит собеседника включить демонстрацию экрана. В это время мошенник может, например, пытаться зайти в ваш интернет-банк или аккаунт на Госуслугах, поэтому вам на телефон придет СМС с кодом для входа или смены пароля, который злоумышленник хочет увидеть и использовать.

Совет

Никогда не включайте демонстрацию экрана для незнакомого человека и не отсылайте ему запись экрана. Такой функционал на самом деле редко требуется использовать в реальной жизни.

«Это ты на видео?»

Сегодня есть риск через мессенджер Telegram получить сообщение следующего содержания: «Это ты на видео?» и прикрепленный файл с **расширением.apk.** Также слово «видео» может быть использовано в названии файла.

При открытии такого файла на телефон устанавливается приложение, зараженное трояном Mamont (тип вредоносного ПО). Вирус может считывать push-уведомления, СМС и фотографии из галереи. Более того, троян автоматически рассылает вредоносный файл всем контактам пользователя в мессенджере. В первую очередь, злоумышленники пытаются получить доступ к платежным средствам. Однако персональные данные пользователя и другая информация тоже могут быть использованы в противоправных целях.

Совет

Ни в коем случае не открывайте неизвестный файл, от кого бы не пришло данное сообщение.

Устанавливайте приложения только из официальных магазинов, а также регулярно обновляйте операционную систему и антивирусное ПО.

Также рекомендуем включить двухфакторную аутентификацию в банковских приложениях и отключить показ уведомлений на заблокированном экране, чтобы злоумышленники не могли перехватить коды доступа.

Также мошенники продолжают использовать троян Mamont, который замаскирован **под списки пропавших в зоне специальной военной операции**.

Злоумышленники создают каналы, визуально похожие на официальные группы, посвященные помощи семьям военнослужащих, в которых регулярно публикуют сведения о пропавших военнослужащих, их фотографии, а также PDF- и Excel-файлы с персональными данными. В тех же сообществах позднее начинают выкладывать вредоносные APK-файлы (архив, внутри которого находятся все компоненты приложения), которые содержат банковский троян Mamont для операционной системы Android.

С помощью данного вредоноса злоумышленники получают полный контроль над устройством жертвы, смогут собирать информацию о нем, перехватывать и отправлять СМС, получить доступ к пользовательским файлам, истории звонков, контактам и т.д., а также банковским приложениям и мессенджерам.

Совет

В целях безопасности отключите автозагрузку файлов в Telegram, проверяйте формат документов.

Спуфинг

Спуфинг является видом кибератаки, при которой мошенники маскируются под других людей или компании, чтобы войти в доверие потенциальной жертвы. У этой схемы есть несколько функций, которыми пользуются злоумышленники. Так, например, мошенники звонят якобы с номера 900 или от имени вашего друга.

Целью кибератаки является завоевать доверие жертвы, чтобы получить доступ к устройствам, контактам; распространение вируса на устройство, кража денег и личных данных.

Совет

Соблюдайте бдительность при открытии почтовых вложений, обращайте внимание на адрес отправителя, проверяйте адресную строку в браузере, а также не разглашайте личные данные в сети и осмотрительно относитесь к телефонным звонкам.

Курьеры-соучастники

Появилась новая изощренная схема телефонного мошенничества, жертвами которой становятся пожилые люди. Преступники не просто обманывают пенсионеров, но и заставляют их участвовать в своих преступлениях, превращая жертв в соучастников. Пенсионеры невольно становятся соучастниками мошенников, становясь курьерами.

Мошенники звонят пенсионерам, представляясь сотрудниками правоохранительных органов, силовых ведомств или других государственных структур. Они сообщают о якобы проводимой проверке, утверждая, что пенсионер причастен к финансированию враждебной армии. Под предлогом помощи следствию или проверки подлинности банкнот, мошенники просят передать деньги через курьеров для «специальной экспертизы». Далее они используют обманутых пенсионеров в роли курьеров. Преступники внушают своим жертвам, что, участвуя в этой мнимой «операции», они якобы помогают разоблачить мошенников, спасают других пенсионеров и способствуют проверке подлинности денег. Таким образом,

доверчивых стариков заставляют ездить к другим пожилым людям, которые уже подверглись обману и готовят деньги для псевдопроверки.

Уже зафиксированы случаи, когда пенсионеров задерживали при получении денег от обманутых граждан или после перевода средств на счета мошенников.

Совет

Полиция настоятельно просит пожилых людей, быть бдительными и не поддаваться на провокации мошенников.

График отключения горячей воды

«Почему нет горячей воды, и когда она появится?» – один из самых популярных запросов в сезон отключения воды – с мая по август. Как аферисты ловят жертву на живца?

Мошенники рассылают фейковые письма с предложением проверить график отключения горячей воды. Цель остается той же – похитить персональные данные. Ссылки в таких письмах ведут на фишинговые сайты, с помощью которых злоумышленники получают доступ к персональной информации.

Совет

Проверяйте график отключений только на официальных ресурсах:

- на сайтах и в соцсетях управляющих компаний и местных администраций;
- на информационных стендах внутри подъездов и на входных группах;
- на Госуслугах.

«Фонд «Защитники Отечества»

Злоумышленники начали использовать новый метод мошенничества: создают сайты, точь-в-точь копирующие бренд госфонда «Защитники Отечества». На сайтах «двойниках» мошенники под видом социального проекта предлагают людям

инвестировать в российские компании и обещают заработать до 30 млн рублей.

Мошенники просят указать ФИО и номер телефона. Затем жертве звонят, убеждают перевести деньги или установить вредоносное приложение. Также могут запрашивать скан паспорта – такие данные потом используются в новых атаках.

Совет

Не передавайте личную информацию незнакомым лицам.

В случае согласия эта личная информация окажется у злоумышленников и может быть использована для других мошеннических атак.

«Владельцы домашних животных под угрозой»

Мошенники добрались и до владельцев домашних животных. Злоумышленники под видом продавцов импортных лекарств для питомцев выманивают деньги и платежную информацию у россиян.

На фоне новостей о сокращении поставок ветеринарных препаратов в Россию мошенники активизировались: они создали несколько каналов в мессенджере Telegram, где предлагают людям «приобрести необходимые лекарства у перекупщиков». Речь идет, в частности, о средствах для защиты от блох и клещей, для профилактики бабезиоза и боррелиоза, препаратах, которые используются в качестве лекарства от воспалительных процессов, зуда и против аллергических реакций.

В описаниях каналов значится информация о том, что поставки лекарств «осуществляются из-за рубежа», а перекупщики занимаются не только розничной, но и оптовой продажей. При этом мошенники в свойственной им манере уверяют, что весь товар оригинальный. О покупке конкретного лекарства с потенциальной жертвой договариваются в личных сообщениях. После того как пользователь переводит средства за выбранный товар ему сообщают, что препарат закончился, и предлагают вернуть деньги. Для этого нужно перейти по присланной ссылке и ввести на странице реквизиты банковской карты, а также сообщить код из

СМС. Однако страница на деле оказывается фишинговой. Таким образом, возврат не происходит, а злоумышленникам уходит финансовая информация человека. К тому же мошенники могут списать еще большую сумму с карты жертвы, если жертва сообщит код из СМС.

Совет

Совершайте покупки только у проверенных продавцов и в магазинах с положительными отзывами.

Если для оплаты необходимо ввести на странице данные банковской карты, проверьте доменное имя на опечатки или необычные символы.

Никому не сообщайте код из СМС или push-уведомлений.

«Выдуманный налог» на СВО

Сразу после завершения налогового периода, когда миллионы людей оплачивали квитанции от ФНС, злоумышленники стали рассылать по электронной почте предупреждения от имени банков **о несуществующем новом налоге на специальную военную операцию** и предлагают отказаться от его уплаты. Далее следует переход по ссылке, после чего жертва непроизвольно оставляет свои данные злоумышленникам.

В письмах, оформленных в стиле крупных финансовых организаций, мошенники предупреждают, что если не отказаться от уплаты налога, то у человека будут постоянно списывать «десятки тысяч рублей». Чтобы не платить нужно перейти по ссылке на поддельный сайт банка и там войти в личный кабинет. Получив эти данные, мошенники могут вывести деньги со счета жертвы или оформить кредит на ее имя.

Совет

Проверяйте информацию в официальных источниках.

Сведения о налогах можно проверить в личном кабинете на сайте https://www.nalog.gov.ru/.

«Письма от Госавтоинспекции»

Гражданин по электронной почте или в мессенджере получает сообщение с формулировкой «Вы нарушили ПДД. Ознакомьтесь с постановлением и оплатите штраф до 10.09». К письму прикреплен файл в формате PDF, оформленный под официальное постановление. В документе может быть указано реальное имя человека, номер автомобиля или иные персональные данные – это создает ощущение подлинности.

В самом письме размещена кнопка «оплатить сейчас», ведущая на стороннюю интернет-страницу. Переход по ссылке приводит к различным вариантам развития событий. В некоторых случаях пользователь попадает на фальшивый сайт, визуально копирующий интерфейс государственных или банковских онлайн-сервисов. Здесь у него запрашивают данные банковской карты: номер, срок действия, CVV-код, а иногда и коды подтверждения из СМС. В других случаях ссылка ведет на зараженный ресурс, который автоматически загружает вредоносное ПО на устройство пользователя, которое может перехватывать пароли, получать доступ к банковским приложениям, мессенджерам и даже использовать камеру и микрофон.

Совет

Настоящие уведомления о штрафах приходят только через официальные каналы, в частности через Госуслуги.

«Бесплатная» медицинская услуга

Мошенники начали обманывать россиян с помощью новой схемы – они предлагают своим жертвам пройти флюорографию в поликлинике за счет средств обязательного медицинского страхования. Звонящий предлагает выбрать поликлинику и записаться на прием, а для этого просит назвать код из СМС. На практике с помощью этого кода злоумышленники осуществляют транзакцию по списанию средств с банковской карты жертвы.

Код из СМС также может понадобиться мошенникам, чтобы авторизоваться на Госуслугах, где могут, к примеру, отправить заявку на получение микрозайма или кредита.

Совет

Помните, что записаться на прохождение флюорографии вы можете самостоятельно, бесплатно, в поликлинике по месту жительства, на ее сайте или на Госуслугах.

«Перерасчет» пенсии

Не редко мошенники используют схему обмана людей старшего возраста: обещают им **перерасчет пенсии в обмен на код идентификации**.

Мошенники представляются сотрудниками Социального фонда России и пытаются внушить гражданам, что у них обнаружен «неучтенный стаж», после чего предлагают оформить заявление на перерасчет пенсии для ее повышения. Далее процедура самая обычная и стандартная, мошенники направляют код и просят его назвать.

Совет

Настоящие сотрудники государственных служб, в том числе Социального фонда России, не звонят с подобными вопросами.

По любым социальным вопросам нужно самостоятельно позвонить в единый контактный центр фонда по телефону 8 800 10-000-01 либо обратиться в ближайшее отделение фонда.

«Сайты МВД России»

Мошенники взяли на вооружение давно забытую схему по выманиванию денег у россиян с помощью всплывающих окон в браузере. Новые сайты-вымогатели препятствуют работе в браузере и выманивают деньги у пользователей под предлогом оплаты штрафов.

Достаточно перейти по еле заметной подозрительной ссылке из электронного письма, например, с рекламой, – экран компьютера тут же блокируется сообщением с фейкового сайта МВД. Оно гласит,

что нужно срочно заплатить штраф за посещение запрещенных ресурсов. Пытаясь закрыть уведомление, пользователь оказывается на фейковом портале МВД, полностью копирующем интерфейс официального (https://мвд.рф/). Там говорится, что устройство пользователя было заблокировано в соответствии с приведенным на сайте постановлением. Для разблокировки человека просят оплатить штраф (перевести деньги на указанные реквизиты). А невыполнение требований, по заявлению мошенников, «ведет к юридической ответственности».

Каждый новый клик или попытка закрыть окно увеличивает сумму штрафа. При этом весь интерфейс как будто заблокирован. На самом же деле ссылка от мошенников открывает сайт и автоматически переводит браузер в полноэкранный режим, что создает впечатление как будто и правда ничего сделать нельзя, кроме как заплатить.

Совет

Выход прост – надо нажать **ESC**, **F11** или любую другую комбинацию горячих клавиш, которые сворачивают окна либо выключают полноэкранный режим. Схема хотя и выглядит примитивной, но вполне способна сбить с толку.

Если же горячие клавиши не помогают (или если у вас просто возникли сомнения по поводу безопасности сайта), можно просто перезагрузить компьютер. А затем сообщить об инциденте на портале Госуслуг или на сайте МВД России.

«Приложение Минздрава»

Злоумышленники предлагают установить новое приложение «от Минздрава» и получить положенный кешбэк, а затем выводят деньги.

Чаще всего звонки от них поступают тем россиянам, которые недавно обследовались в медучреждениях. Мошенники представляются жертве сотрудниками больницы и просят установить приложение, которое поможет перейти с системы ЕГИСЗ

на Минздрав. Важно отметить, что подобные звонки чаще всего поступают в популярных мессенджерах.

После того как жертва установит приложение на телефон, мошенники сообщают, что ей положен кэшбек, а затем дают ей логин и пароль от формы для его получения, она вводит туда данные своей банковской карты и лишается всех своих сбережений, которые сразу же попадают в руки аферистов.

Совет

Устанавливайте приложения только с проверенных источников, иначе можно лишиться не только денег с банковской карты, но и всех своих данных, что чревато серьезными последствиями.

«Бесплатная замена» счетчиков воды и электроэнергии

Звонок поступает от имени энергосбытовой компании или Горводоканала. Злоумышленники обращаются по имени и называют домашний адрес. Замена счетчиков, по их словам, бесплатна, но для оформления заказа нужно прислать копию паспорта и назвать код из СМС.

С помощью этого злоумышленники получают доступ к странице на Госуслугах и похищают оттуда личные данные.

Обмануть могут даже тех, кто не назвал свои данные: жертве начинают посылать сообщения о входе на портал Госуслуг и оформлении там некой доверенности. Для отмены этого документа предлагается позвонить на подставной номер. Многие недоверчивые люди после этого пытаются «защититься» от взлома и уже охотнее идут на контакт.

Существует третий этап мошенничества для тех, кто не стал жертвой двух первых. Звонок в мессенджере от имени сотрудников правоохранительных органов. Он поступает через несколько дней после предыдущей попытки. В диалоге «сотрудник» сообщает, что получил от сотового оператора информацию о разговоре, в котором абонент назвал мошенникам данные своего аккаунта и тем самым

дал доступ к своей странице. Далее запускается сценарий получения доступа к личной странице.

Совет

Чем больше времени человек говорит с мошенниками, тем выше его шанс стать жертвой. Для безопасности лучше либо вообще не отвечать на звонки с неизвестных номеров, либо не вступать в переговоры.

Надежнее всего будет выключить телефон на несколько часов и обратиться в полицию.

Оформление кредитов на граждан

Сбербанк выявил десять кредитных финансовых пирамид, от которых уже пострадали более 2 тысяч человек. Эксперты отмечают, что вновь стали появляться финансовые пирамиды, и если раньше мошенники стремились привлечь средства неосведомленных граждан, обещая им необоснованно высокие доходы, то сейчас они предлагают жертве оформить на себя кредит.

Суть обмана заключается в том, что жертва берет **кредит на свое имя за вознаграждение.**

Основная часть полученных средств передается мошенникам. Заемщику оставляют небольшую долю и обещают ежемесячно направлять деньги на погашение кредита. Так происходит несколько месяцев, чтобы у жертвы не возникло подозрений, и она не забила тревогу слишком рано. Многократно повторив обман, мошенники исчезают с деньгами.

При этом в Сбербанке отметили, что им уже удалось спасти от таких аферистов-пирамидчиков 1,6 миллиарда рублей клиентов банка.

Совет

Будьте бдительны! Не поддавайтесь на уловки мошенников, не сообщайте посторонним людям личные данные, информируйте о мошеннических схемах своих родных.

Маскировка писем под рассылки известных магазинов

Мошенники могут маскировать свои письма под рассылки магазинов, чтобы получить доступ к персональной информации россиян.

Сообщения приходят как от ранее неизвестных, так и от уже знакомых отправителей. Злоумышленники маскируются под стандартные рассылки. К примеру, вам регулярно приходят рассылки от маркетплейсов или интернет-магазинов. Тут риски открыть вредоносную ссылку возрастают. Ведь когда в таких рассылках появляется «вброс» интересующей нас информации, например, розыгрыш квартиры, бесплатный приз, то, это может заинтересовать большое количество пользователей.

Злоумышленники могут точно скопировать рассылку и отличить реальное письмо от потенциально опасного порой не просто.

Совет

Внимательно смотрите на письмо: даже минимальные отличия могут свидетельствовать о том, что тут работают мошенники.

Двойное мошенничество

МВД России сообщает, что мошенники придумали новую схему обмана россиян, нацеленную на тех, кто уже пострадал от действий других злоумышленников. Специалисты ведомства обнаружили фишинговый ресурс, на котором злоумышленники якобы от имени Организации Договора коллективной безопасности (далее – ОДКБ) обещают тем, кто пострадал от действий мошенников, вернуть потерянные деньги.

Согласно скриншоту сайта, опубликованному ведомством, злоумышленники утверждают, что Совет ОДКБ принял указ о борьбе с инвестиционным мошенничеством. Пользователей сети просят ввести свои данные в форму для начала процедуры возврата денег, однако в действительности эта информация оказывается в руках злоумышленников.

Совет

Будьте предельно внимательны и осторожны!

Не открывайте «слепо» письма и сообщения, которые приходят в качестве рассылки, не переходите по ссылкам.

Обязательно перепроверяйте информацию на официальных ресурсах и сайтах компаний.

Если вы стали жертвой мошенников – обратитесь в полицию.

Недобросовестная косметология

Злоумышленники распространяют в Telegram фишинговые сообщения с приглашением женщин на омолаживающие процедуры лица в качестве моделей. Услуги обещают предоставить бесплатно.

Заявляется, что для записи на данное обследование клиника косметологии открыла запись на сайте, куда необходимо перейти по ссылке. Как правило, мошенники используют завлекающие фразы, такие как «бесплатная процедура», «всего 20 мест», «успейте записаться», в том числе охватывается широкая возрастная категория от 27 до 75 лет, ну и «только для граждан РФ». В конце сообщения прикрепляется ссылка. После прохождения «регистрации» злоумышленники получают доступ к личным данным и банковским картам жертв.

Совет

Не переходите по сомнительным ссылкам.

Будьте максимально критичными при поиске медицинских услуг. Эта та сфера, где недобросовестное предпринимательство может навредить в первую очередь вашему здоровью.

Обязательно проверяйте лицензии и отзывы на всех возможных платформах.

Обман в домовых чатах

Мошенники начали регистрироваться в домовых чатах под видом жильцов. Такие «соседи» предлагают бесплатно забрать ненужную технику или мебель, затем для оформления доставки присылают фишинговые ссылки.

Злоумышленники размещают в домовых или районных чатах сообщения с предложениями бесплатно забрать ненужную бытовую технику или мебель. Заинтересованные граждане получают подтверждающие фото/видео для правдоподобности. Накануне встречи фальшивый «сосед» извиняется и утверждает, что технику может отправить только с курьером. Для оформления доставки он предлагает перейти по ссылке. Перейдя по ссылке, человек «заражает» свой телефон вредоносным ПО, а его персональные данные похищаются.

Совет

Перепроверяйте все входящие сообщения по официальным каналам.

Применяйте принцип «нулевого доверия» к любой информации, побуждающей к активным действиям, связанным с личными данными и деньгами.

Сообщения от имени Почты России

Аферисты начали воздействовать на подростков, поскольку они являются активными пользователями услуг маркетплейсов и доставок Почтой России.

На телефон ребенка приходит сообщение с СМС-кодом о том, что пришла посылка. После мошенники звонят, представляются сотрудниками «Почты России» и просят сообщить код для регистрации заявки. В большинстве случаев подросток называет код злоумышленникам. Далее поступает звонок от якобы сотрудника Госуслуг, который предупреждает, что аккаунт ребенка взломан и мошенники оформили на него микрозаймы. Затем поступает звонок уже из «Банка России» с запугиванием, что эти деньги перечислены в пользу запрещенных организаций и теперь ребенку грозит уголовная ответственность.

После этого подросток в панике соглашается провести дистанционный обыск квартиры и показывает, где в доме лежат ценности. В конце мошенники просят передать их курьеру «для расследования».

Совет

Будьте предельно внимательны и осторожны!

Предупредите своих родственников, детей и внуков, напомните, что сотрудники Госуслуг никогда не звонят, а «дистанционные обыски» – это уловки мошенников.

Ложная диспансеризация

Новая мошенническая схема во всю набирает популярность. На этот раз злоумышленники предлагают пройти диспансеризацию. Неизвестные звонят и представляются работниками поликлиник. В процессе разговора жертве сообщают, что для записи нужно назвать код от портала Госуслуг.

Вторым этапом может стать звонок с предупреждением, что аккаунт взломан и для восстановления требуется позвонить в техподдержку. Далее человек звонит по подложному номеру телефона, где его перенаправляют за консультацией в Росфинмониторинг. В конце схемы якобы сотрудники Росфинмониторинга просят гражданина заполнить заявление и приложить к нему фото банковских карт, откуда потом начнутся списания денежных средств.

По данным МВД, подобные мошеннические атаки направлены в адрес наиболее доверчивых категорий граждан – пожилых и несовершеннолетних.

Совет

Чтобы защитить себя и своих близких, используйте сложные пароли и двойную систему защиты.

Никому не сообщайте коды из СМС. При малейших сомнениях обращайтесь в полицию!

Звонок от «помощника судьи»

Мошенники представляются сотрудниками суда и звонят гражданам, называя якобы реальное дело (например, «по иску такого-то к такому-то»). Затем сообщают о назначении судебного заседания и просят подтвердить явку или согласие на рассмотрение

дела без участия гражданина. Чтобы подтвердить решение, мошенники требуют назвать код из поступившего СМС.

На самом деле этот код – подтверждение смены пароля от личного кабинета Госуслуг. После его ввода злоумышленники получают доступ к аккаунту жертвы, включая ее персональные данные, и могут взять кредиты на ее имя.

Совет

Проверяйте информацию о назначенных заседаниях на официальных сайтах судов или через Госуслуги.

Если вам поступил такой звонок, не предоставляйте никакой личной информации.

«Скачайте приложение»

«Кто-то пытается похитить ваши деньги, скачайте приложение!». Мошенники все также звонят или пишут в мессенджерах жертве, утверждая, что у нее пытаются похитить деньги. Чтобы спасти сбережения, киберпреступники предлагают установить «приложение Центрального банка», которое на самом деле является вредоносной программой.

После этого жертву просят поднести банковскую карту к телефону и ввести СМС-код «для защиты». На самом деле так мошенники создают виртуальную копию карты, после чего могут снимать деньги через банкоматы с бесконтактной оплатой.

Совет

Не скачивайте приложения по просьбе неизвестных.

Не сообщайте данные карты и пароли от своих приложений.

Если вы подозреваете, что у вас могут похитить деньги, лучше позвонить в банк по официальному номеру.

«Подарки и выплаты» ко Дню Победы

Мошенники активизируются перед важными датами, используя праздник как повод для обмана пожилых людей. Представляясь сотрудниками Госуслуг, соцзащиты или муниципальных администраций, злоумышленники сообщают пенсионерам о

положенных им к празднику «особых выплатах» или подарках. Для получения этих «привилегий» жертву просят предоставить персональную информацию: номер СНИЛС, паспортные данные и коды из СМС – якобы для подтверждения заявки или оформления документов.

На самом деле СМС приходит от портала Госуслуг, где злоумышленники пытаются войти в личный кабинет жертвы. Получив доступ, мошенники могут оформить кредиты в микрофинансовых организациях или выманить у жертвы деньги.

Совет

Будьте бдительны: сотрудники государственных органов не запрашивают персональные данные или коды из СМС по телефону.

Не переходите по подозрительным ссылкам и не вводите личные данные на незнакомых сайтах.

Проконсультируйтесь с родственниками или обратитесь в организацию по официальным каналам связи перед тем, как предоставлять какую-либо информацию.

«Бесконтактный» обман (через NFC)

Мошенники все чаще используют технологии бесконтактной оплаты для кражи средств с банковских карт. Они звонят жертве, представляясь сотрудниками банка или правоохранительных органов, и сообщают, что якобы взломаны Госуслуги, зафиксированы незаконные транзакции или жертва финансирует Вооруженные силы Украины. Для «защиты» средств предлагают установить специальное приложение на смартфон.

После этого жертву просят приложить свою банковскую карту к телефону и ввести PIN-код. При этом мошенники успокаивают жертву: карта остается у нее на руках, поэтому PIN-код вводить не опасно. На самом деле приложение считывает данные карты через NFC и передает их мошенникам, которые в этот момент находятся у банкомата. Злоумышленники прикладывают свое устройство с таким же приложением к терминалу банкомата. Терминал считывает устройство мошенника как карту жертвы, поэтому после ввода PIN-кода

преступник получает доступ к ее личному кабинету и может снять все деньги со счетов.

Совет

Не устанавливайте приложения из непроверенных источников или по ссылкам из сообщений.

Держите PIN-код в секрете, не вводите в приложениях, которые не являются официальными банковскими программами.

Ограничьте использование NFC, включайте его только при необходимости и отключайте после использования.

Установите антивирусное ПО на свой смартфон и регулярно обновляйте его.

Будьте бдительны и не доверяйте незнакомым звонкам, особенно если вас просят установить приложения или предоставить конфиденциальную информацию.

«Отпуск» под угрозой

В летний период (в период отпусков и каникул) мошенники обманывают жертв, предлагая арендовать или забронировать жилье на популярных курортах. Злоумышленники размещают видео в социальных сетях с заманчивыми предложениями: «Апартаменты за 2 тыс. рублей в сутки» или «Квартира у моря всего за 1 рубль». Для бронирования предлагают перейти по ссылке на сайт, похожий на известные сервисы бронирования, и внести символическую сумму для подтверждения брони.

На самом деле эти сайты фишинговые, они созданы для кражи персональной и банковской информации. После ввода данных карты и кода из СМС мошенники получают полный доступ к счету жертвы. В некоторых случаях пользователям Android предлагается установить приложение, якобы необходимое для завершения бронирования. На самом деле оно является вредоносным ПО, способным перехватывать данные и управлять устройством.

Совет

Не переходите по подозрительным ссылкам, особенно если они пришли от незнакомых отправителей или размещены в непроверенных источниках.

Не вводите данные карты на незнакомых сайтах, особенно если вас просят внести символическую сумму для подтверждения бронирования.

Скачивайте приложения только из проверенных источников, таких как App Store, Google Play или RuStore.

Будьте осторожны с предложениями, которые выглядят слишком хорошо, чтобы быть правдой: низкая цена может быть приманкой для жертвы.

Самозапрет на кредиты

С 1 марта 2025 г. россияне получили возможность установить через портал Госуслуг самозапрет на получение кредитов. Эта мера призвана защитить граждан от мошеннических займов и импульсивных покупок в долг. Однако злоумышленники начали использовать эту возможность в своих схемах обмана.

Мошенники звонят, представляясь сотрудниками Госуслуг и предлагают установить самозапрет на получение кредита. Для подтверждения нужно сообщить код из СМС. Жертва в данном случае ничего не подозревает, ведь самозапрет действительно устанавливается через Госулуги. Получив код, злоумышленники получают доступ к аккаунту Госуслуг жертвы. После этого они используют личные данные для совершения неправомерных действий.

Совет

Сотрудники портала Госуслуг не обзванивают пользователей с предложениями что-либо оформить. О новом функционале они могут информировать с помощью сообщений внутри приложения.

Помните, что самозапрет на кредиты **не является** обязательной процедурой и его можно подключить **добровольно и самостоятельно** в приложении, без чьей-либо помощи.

Согласно данным Объединенного кредитного бюро (ОКБ) за пять месяцев 2025 года уже 12,5 миллионов россиян установили самозапреты на кредиты. Подавляющее большинство граждан выбирают формат полного запрета на кредитные продукты – 90,9% от общего количества заявок были поданы на установку именно полного запрета.

4,3% заявок были поданы на ограничение онлайн-кредитов в банках и МФО;

1,6% заявок – на полный запрет займов в МФО;

1,4% заявок – на полный запрет займов в МФО и онлайн-кредитования в банках.

1,8% от общего числа заявок – прочие варианты ограничений.

За все время 472 тыс. человек успели не только установить, но уже и сняли ограничения.

«Неправильный» самозапрет на кредиты

Мошенники звонят гражданам, представляясь сотрудниками Госуслуг или бюро кредитных историй (БКИ), и сообщают о якобы некорректно установленном самозапрете на кредиты. Для «исправления ошибки» они предлагают перейти по отправленной в мессенджере ссылке, которая ведет на фальшивый сайт, имитирующий Госуслуги. После ввода данных злоумышленники получают доступ к аккаунту пользователя и от его имени могут подать заявки на оформление кредитов в микрофинансовых организациях. Часто взлом аккаунтов мошенники используют для дальнейшего обмана: человеку звонят «представители банка», «силовых ведомств» и других госструктур, запугивают и под различными предлогами убеждают отдать деньги злоумышленникам.

Совет

Не переходите по ссылкам из сообщений, даже если они выглядят официально.

Проверяйте информацию, свяжитесь с представителем организации по официальным каналам.

Не вводите данные на подозрительных сайтах, убедитесь, что вы находитесь на официальном портале.

Пользуйтесь официальным приложением Госуслуг.

Установите антивирусное ПО на свое устройство и регулярно обновляйте его.

«Опасный» международный счет

Мошенники выманивают личные данные и деньги у граждан, используя их доверие к официальным организациям. Злоумышленники рассылают электронные письма с логотипом Центробанка, в которых сообщают о якобы существующем у получателя международном счете с крупной суммой денег. В письме утверждается, что, если счет немедленно не закрыть, человеку грозит штраф, арест имущества или удержание средств с зарплаты/пенсии.

Для «закрытия» счета мошенники предлагают перейти по ссылке, которая ведет на фишинговый сайт, имитирующий официальный ресурс. На этом сайте жертву просят ввести личные данные и банковские реквизиты якобы для идентификации и закрытия счета. Иногда ссылка ведет на сайт с вредоносным ПО, которое автоматически устанавливается на устройство и предоставляет злоумышленникам удаленный доступ к смартфону пользователя.

Совет

Игнорируйте подозрительные письма, не открывайте вложения и не переходите по ссылкам от неизвестных отправителей.

Проверяйте информацию, свяжитесь с представителем организации, от имени которой пришло письмо, по официальному каналу связи.

Установите антивирусное ПО на свой компьютер и регулярно обновляйте его.

Дропперы

Дропперами (или дропами) называют людей, которые выступают в роли посредников в различных нелегальных схемах, связанных с финансовыми операциями. Говоря простыми словами, это те, кто соглашается получить на свой счет деньги, добытые незаконным путем, и затем перевести их другим лицам, чаще всего – за вознаграждение.

Представьте, что кто-то украл деньги с банковской карты и хочет «замести» следы. Для этого он переводит средства на счет другого человека (дроппера), который может даже не знать, что деньги получены незаконно. После этого дроппер отправляет их дальше, оставляя себе небольшую часть в качестве вознаграждения.

Благодаря этой схеме злоумышленникам легче скрыть свое участие в преступлении. Дропперы нередко играют значимую роль в схемах отмывания денег. Даже если они не знают, что участвуют в незаконных действиях, их могут обвинить в содействии преступной деятельности и назначить уголовное наказание.

Иногда человек становится дроппером, вовсе не подозревая об этом. Например, потеря банковской карты может привести к ее использованию в незаконных схемах. Жертва даже не догадается о том, что ее карта стала инструментом преступления.

В других случаях люди более сознательно становятся соучастниками. Это происходит, когда они активно ищут «работу» и соглашаются на условия другого участника преступной схемы. При этом для дроппера не всегда очевидно, что действия, которые он совершает, нарушают закон.

Примеры ситуаций, при которых стоит насторожиться:

Ошибочный перевод. Вам неожиданно поступает на карту определенная сумма денег. Затем звонит неизвестный человек и говорит, что случайно перевел средства не на тот счет и просит вернуть их. Вам же предлагает оставить 5 тыс. руб. себе за добрую услугу. Согласившись на это, вы можете стать соучастником преступления. Правильно будет в этой ситуации сообщить о неожиданном переводе банку.

Просьба снять деньги в банкомате. К вам у банкомата подходит человек и жалуется, что забыл банковскую карту дома. Он говорит, что ему очень нужны наличные деньги и предлагает сделать перевод вам на карту, который нужно тут же снять и отдать ему. Вроде ничего плохого в этом нет. Но если полученные деньги были украдены, вы можете стать дропом-обнальщиком. И это лишь малая часть примеров.

Совет

Будьте внимательны к неожиданным переводам. Если вы получили на карту крупную сумму без объяснений, то не соглашайтесь на просьбу вернуть деньги и оставить часть себе; сообщите банку о случившемся переводе – он проверит его законность и поможет избежать проблем.

Проявляйте бдительность, когда снимаете деньги в банкомате. Если к вам подходит человек и просит снять деньги с вашей карты, утверждая, что забыл свою, откажитесь от выполнения этой просьбы. Деньги могут быть украденными, и вы рискуете стать соучастником преступления.

Проверяйте предложения о работе. Если вам предлагают работу, связанную с финансами: тщательно исследуйте компанию и ее репутацию; не соглашайтесь на работу с переводами или обналичиванием, если что-то кажется подозрительным; убедитесь, что все операции законны, чтобы не стать жертвой мошенников.

Бережно храните свои банковские данные: не теряйте банковские карты и документы; не передавайте банковские карты или данные для доступа к онлайн-банку и мобильному приложению неизвестным людям; своевременно блокируйте карту в случае потери.

При этом, если вы поняли, что непреднамеренно стали дроппером, уже после вовлечения в преступную схему, то следует сразу прекратить все контакты с мошенниками. Даже если преступники запугивают и шантажируют тем, что вы уже стали их сообщником, нужно обратиться в полицию с заявлением и рассказать о вовлечении вас в преступную схему путем обмана.

Нелишним будет заблокировать карту и дистанционный доступ к счетам, если злоумышленники успели завладеть данными для входа или информацией о карте. Если же Банк России уже внес вас в базу дропперов, то нужно обратиться в свой банк. Оспорить внесение в базу можно и через интернет-приемную регулятора.

ПРАВИЛА
БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ
БАНКОВСКИХ КАРТ

! Заведите для онлайн-шоппинга отдельную банковскую карту. Не храните на ней значительную сумму, а переводите непосредственно перед покупкой столько, сколько вам понадобится.

! Перед тем как что-нибудь купить, почитайте отзывы об интернет-магазине. Оплачивайте покупки онлайн только на сайтах проверенных интернет-магазинов.

! Проверьте правильность интернет-адреса магазина, чтобы не попасть на фишинговую страницу.

! Используйте для покупок только свой компьютер, смартфон или планшет, чтобы ваши данные случайно не попали в руки другого человека. Если вы все-таки воспользовались чужим устройством, не сохраняйте на нем свои персональные данные и платежную информацию.

! Для совершения онлайн-покупок не требуется вводить ПИН-код. Если у вас его требуют – то вы попали на сайт, созданный мошенниками.

! При переходе на страницу оплаты обратите внимание на то, чтобы она использовала защищенное соединение – об этом свидетельствует значок «замок» в адресной строке.

! После онлайн-оплаты вам должны обязательно прислать электронный чек на адрес электронной почты. Сохраните его до получения покупки.

! Установите и регулярно обновляйте антивирусное ПО на устройствах, с помощью которых вы делаете покупки в интернете.

! Устанавливайте приложения интернет-магазинов только из надежных источников – GooglePlay, App Store, RuStore.

! Не совершайте покупки в интернете, если вы подключились к публичному Wi-Fi.

! Не сообщайте никому данные своей банковской карты и CVV/CVC/CVP код – их достаточно для совершения онлайн-покупки с помощью вашей карты.

! Никогда не отвечайте на письма с просьбой обновить данные о вашей карте через интернет-сайт – их рассылают мошенники.

! Регулярно просматривайте выписки по счету карты.

! Подключите уведомления банка об операциях по вашей карте. Имейте при себе контактный телефон банка, чтобы при необходимости оперативно связаться со службой поддержки.

! Если у вас возникли подозрения, что данные вашей карты стали известны посторонним, лучше ее перевыпустить.

НЕ СТАНЬ ЖЕРТВОЙ МОШЕННИЧЕСТВА!

СОЦРАБОТНИКИ

Незнакомец представляется социальным работником и сообщает о надбавке к пенсии, перерасчете квартплаты, премии ветеранам, срочном обмене денег на дому, якобы «только для пенсионеров». **Не верьте - это мошенничество!**

ИНЫЕ СЛУЖБЫ

Не открывайте дверь незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста.

БЛИЗКИЙ В БЕДЕ

Не доверяйте, если Вам звонят и сообщают, что **Ваш родственник или знакомый попал в аварию**, «за решетку», в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку - в общем, откупиться.
Это обман!

КУПЛЯ-ПРОДАЖА

Мошенники находят жертв через интернет-объявления о продаже или покупке товаров. Просят сказать им данные банковской карты, якобы для предоплаты. **Не называйте незнакомым лицам данные своих банковских карт** и СМС-коды, приходящие на телефон!

БАНКОВСКИЕ КАРТЫ

Если Вы получили **СМС-сообщение о блокировке карты** или списании денежных средств, не перезванивайте по указанному в СМС номеру! Чтобы узнать обо всех операциях, позвоните по номеру телефона, указанному на ВАШЕЙ банковской карте, сходите в банк лично или проверьте баланс через банкомат/ онлайн-банк.

ГАДАЛКИ

Если вас встречают на улице и **предлагают избавить от порчи**, просят для проведения ритуала передать им на время деньги или ценности - это мошенники!

В ЗАВЕРШЕНИЕ…

Телефонные звонки и сообщения в соцсетях по-прежнему остаются наиболее популярными инструментами мошенников, поэтому с осторожностью относитесь к попыткам незнакомцев выйти на связь.

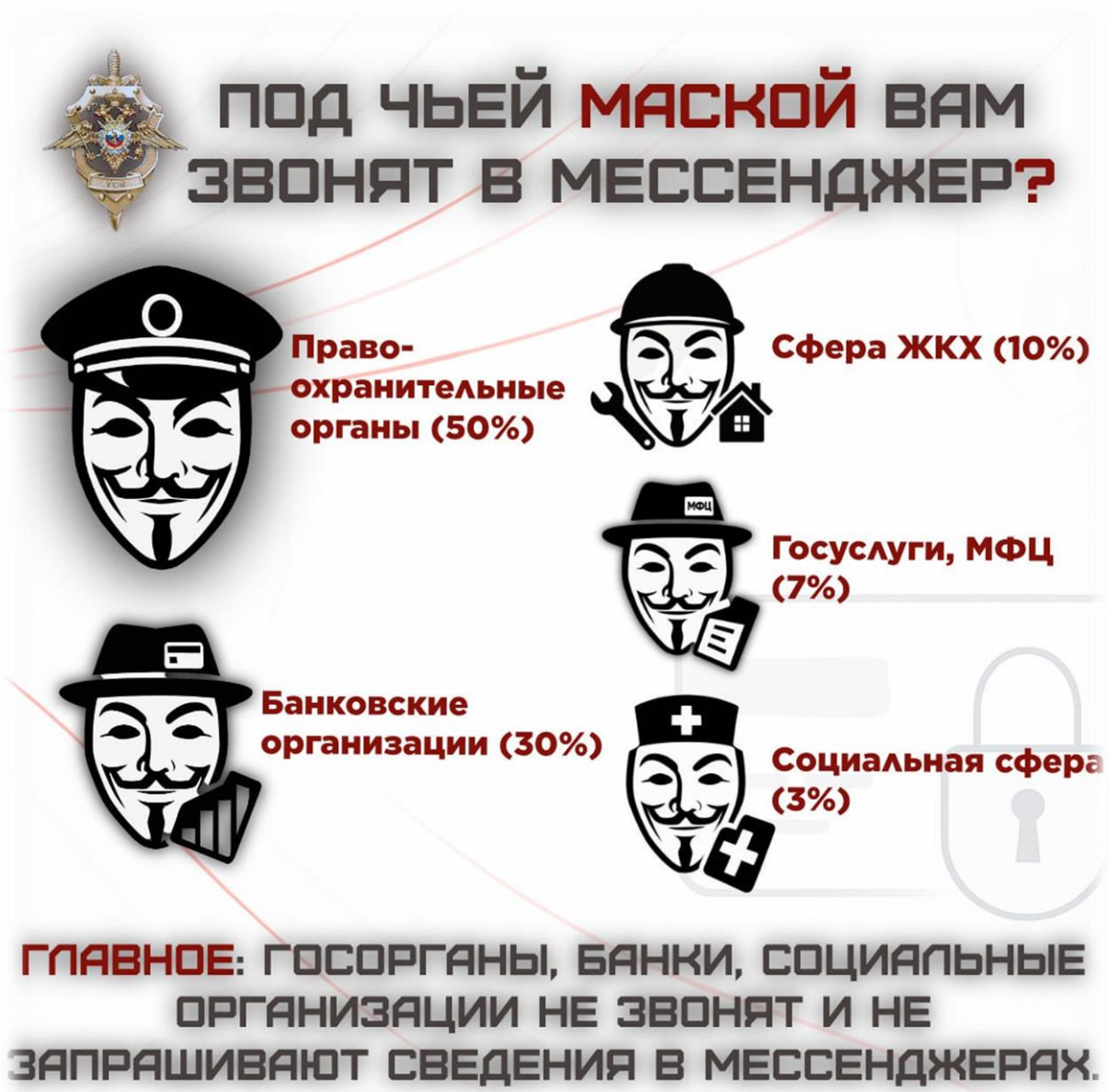
Обычно мошенники стараются психологически надавить на человека и заставить его принять поспешное и необдуманное решение. Если близкий человек звонит с незнакомого номера и просит перевести деньги, лучше перестраховаться и задать ему личный вопрос, ответ на который может знать только он.

Если родственник говорит, что попал в беду, или пишет об этом в соцсетях, сразу же свяжитесь с ним. Часто оказывается, что с человеком все в порядке, а его аккаунт взломали злоумышленники.

При телефонном разговоре сотрудники банка никогда не спрашивают пароли или коды из СМС, не просят устанавливать приложения. Если деньгам человека действительно что-то угрожает, кредитор заблокирует его счет или карту, а затем пригласит клиента в офис для решения проблемы. При любых подозрениях рекомендуется немедленно звонить в банк по официальному номеру с карты или сайта.

Остерегайтесь любых слишком выгодных предложений о вложении или инвестировании средств. Ни одна кредитная организация не предложит вклад на условиях, которые сильно отличаются от аналогичных предложений других банков.

Мир меняется, технологии развиваются, и вместе с ними появляются новые угрозы. Но именно осведомленность, внимание к деталям и готовность защитить себя делают нас сильнее перед лицом любых попыток обмана. Зная о методах злоумышленников и оставаясь внимательными, мы способны защитить не только себя, но и тех, кто нам дорог.


ПОД ЧЬЕЙ МАСКОЙ ВАМ ЗВОНЯТ В МЕССЕНДЖЕР?
Право-охранительные органы (50%)
Сфера ЖКХ (10%)
МФЦ
Госуслуги, МФЦ (7%)
Банковские организации (30%)
Социальная сфера (3%)
ГЛАВНОЕ: ГОСОРГАНЫ, БАНКИ, СОЦИАЛЬНЫЕ ОРГАНИЗАЦИИ НЕ ЗВОНЯТ И НЕ ЗАПРАШИВАЮТ СВЕДЕНИЯ В МЕССЕНДЖЕРАХ.

УВАЖАЕМЫЕ ГРАЖДАНЕ!

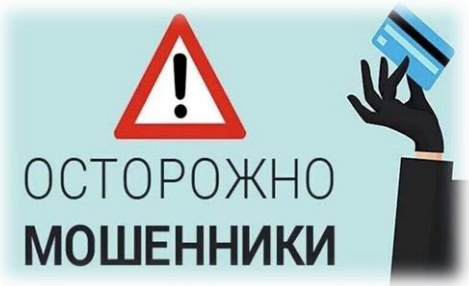
Будьте предельно внимательны и осторожны!

Если не уверены в собеседнике – немедленно прервите разговор!

Не переходите по сомнительным ссылкам!!!

Если вы все же попались на уловку мошенников, рекомендуем незамедлительно обратиться в МФЦ с паспортом и СНИЛС для замены пароля на Госуслугах. А также как можно быстрее блокируйте счета в банках по телефону горячей линии и обращайтесь в полицию!

Берегите свои данные, себя и своих близких!



Полиция всегда готова прийти на помощь пострадавшим от действий преступников, но самый лучший способ борьбы с правонарушениями –
ваша правовая грамотность и бдительность!

ЗАПОМНИТЕ!!!

НИКОГДА:

1. **НЕ** пускайте в свою квартиру посторонних людей.
2. **НЕ** сообщайте о своем материальном положении.
3. **НЕ** позволяйте пользоваться счетом в банке.
4. **НЕ** давайте в долг крупные суммы денег без должного юридического оформления и свидетелей.
5. **НЕ** позволяйте оставлять вещи в залог.
6. **НЕ** позволяете переписывать номера купюр, хранящихся у вас дома.
7. **НЕ** доверяйте лицам, позвонившим вам с незнакомого номера и сообщившим о беде с родственником или блокировке банковской карты.
8. **НЕ** переводите деньги на мобильные телефоны по требованию незнакомых людей.
9. **НЕ** передавайте деньги курьерам для последующей передачи родственникам.
10. **НЕ** сообщайте секретный код на обратной стороне вашей карты.
11. **НЕ** сообщайте посторонним лицам коды, пришедшие из банка.
12. **НЕ** доверяйте телефонным сообщениям о крупных выигрышах, победах в конкурсах, лотереях, компенсациях, за которые нужно заплатить налог или оплатить доставку приза.
13. **НЕ** верьте людям, сообщающим о порче или сглазе. ЭТО – МОШЕННИКИ!

ВСЕГДА:

1. **Спрашивайте** удостоверяющие личность документы у пришедших к вам людей.
2. **Перезванивайте** родственникам ТОЛЬКО по знакомым номерам.
3. **Проверяйте** отзывы об интернет-магазине, прежде чем совершить оплату.
4. **Советуйтесь** с родственниками перед тем, как совершить крупную передачу денег.
5. **Сообщите** в полицию, если к вам домой попытались пройти подозрительные люди.
6. **Закрывайте** двери самостоятельно, не доверяйте данную процедуру посторонним.
7. **Избегайте** чужого мнения, снимая деньги со своего банковского счета.

Если вы пострадали от действий злоумышленников, немедленно сообщите об этом в полицию по № 112.

ПОЛЕЗНЫЕ ССЫЛКИ

1. Интернет-ресурс Департамента региональной безопасности ХМАО – Югры

https://deprb.admhmao.ru/profilaktika-moshennichestva/

2. Интернет-ресурсы МВД России, Банка России, осуществляющих деятельность в сфере информационной безопасности, содержащих информационно-разъяснительные материалы по профилактике дистанционных преступлений:

https://мвд.рф/ (официальный сайт МВД)

https://мвд.рф/mvd/structure1/Upravlenija/убк (официальный сайт УБК МВД)

https://t.me/cyberpolice_rus (Вестник Киберполиции России)

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

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

https://www.sberbank.ru/ru/person/kibrary/articles/pyatnadcat-pravil-bezopasnogo-ispolzovaniya-bankovskikh-kart-onlajn (Кибрарий от Сбербанка)

https://zakon.gov.spb.ru/vnimanie-moshenniki/novye-vidy-moshennichestva-v-2023-godu/ (Комитет по вопросам законности, правопорядка и безопасности, Правительство Санкт-Петербурга)

https://fincult.info/rake/ (Финансовая культура – сайт о финансовой грамотности, созданный Банком России)

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

5. Сюжет телеканала "Санкт-Петербург" о новых мошеннических схемах (https://zakon.gov.spb.ru/news/89786/)

6. Фильм «Днепр на проводе» (https://clck.ru/3NXSoX)

7. Дистанционный курс Банка России Практичные финансы: от знаний к действиям. Материалы по каждому модулю можно скачать по ссылке https://clck.ru/3NXSoX.