

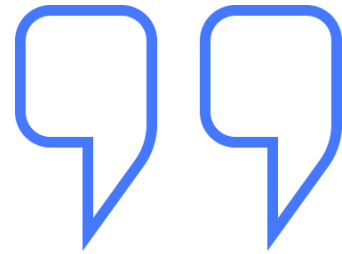
Социальная инженерия





Социальная инженерия

Атака на человека



... **индивидуально подобранные** психологические, социологические приемы, методы, техники и **инструменты** влияния, **позволяющие** применяющему их **получить желаемое** от оппонента / достичь заранее продуманного результата...

Чтобы получить доступ к Вашему личному кабинету в **Госуслугах** мошенники используют различные схемы:

Сотрудник **Социального фонда** сообщает, что трудовой стаж учтен неверно

Мошенник приглашает якобы на консультацию в МФЦ или отделение Социального фонда России для решения вопроса. Для подтверждения записи просит назвать код из СМС

Сотрудник **поликлиники** предлагает записаться к врачу/на флюорографию/на диспансеризацию

Мошенник предлагает выбрать ближайшую поликлинику из числа реальных медицинских учреждений, выбрать дату и время приема, а для подтверждения записи просто назвать код из СМС

Сотрудник **Почты России или иной службы доставки** сообщает о неполученных важных письмах, которые якобы были утеряны с адресом и именем отправителя

Чтобы забрать письма нужно записаться онлайн на приём в учреждения и подтвердить запись с помощью кода из СМС

Представляются сотрудниками компании «Мосэнергосбыт», предлагают назначить время для проверки и замены электросчетчиков или осуществить возврат денег после перерасчёта платежей

Мошенники общаются деликатно, в ходе диалога демонстрируют свои знания в электрике, чтобы любым способом выманить код из СМС для получения доступа к аккаунту Госуслуг

Лже-оператор сотовой связи сообщает, что срок действия вашей сим-карты истекает, необходимо его продлить

Мошенник присылает человеку СМС с кодом, который просит сообщить для продления договора

Главная цель мошенников: получение доступа к аккаунту Госуслуг!
Никому не сообщайте код из смс от Госуслуг, его спрашивают ТОЛЬКО мошенники!

Легенда «звонок от имени руководителя»

1

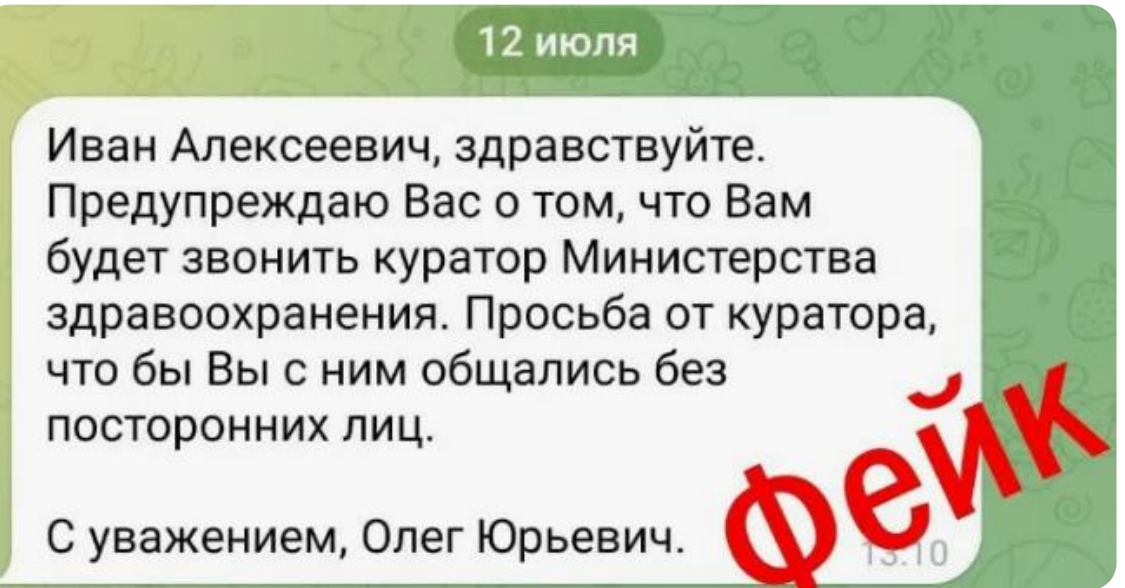
Руководитель / иное лицо, в подлинности которого нет сомнений предупреждает о звонке из правоохранительных органов и просит ответить на этот звонок, а также оказывать всяческое содействие представителю ведомства.

2

Звонок поступает с фотоизображением и ФИО руководителя организации, в том числе мошенники могут использоваться возможности нейросети по искажению голоса, после чего он становится схожим с голосом руководителя, от имени которого осуществляется звонок.

Желаемая реакция

Идеальная жертва в такой ситуации бы испугалась. Все внимание сфокусировано не на фейковом аккаунте или желании разобраться в ситуации, а на страхе вызвать гнев руководителя и нежелании быть несправедливо уволенным.



Как необходимо действовать на самом деле

Необходимо сразу проверить номер, с которого поступает звонок, критически отнестись к поступающей информации и незамедлительно прекратить разговор, при возможности установить личный контакт с руководителем.

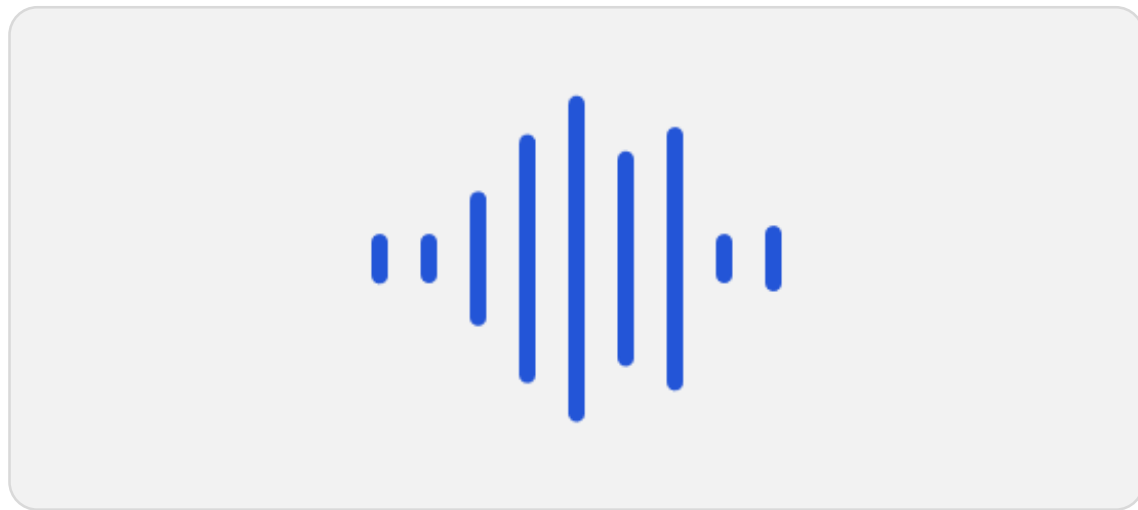
Данной атаке наиболее часто подвергаются граждане, работающие в сфере образования, медицины, науки, реже сотрудники иных государственных организаций.

Примеры использования нейросетей мошенниками

Подделка голоса

Будьте внимательны с предложением о платной озвучке рекламы и фильмов, которую распространяют злоумышленники в сети.

Собранные экземпляры голосов злоумышленники используют для обучения нейросетей и генерируют на их основе аудиосообщения, с помощью которых потом вымогают деньги у друзей и родственников жертвы.



Deepfake – подделка видео

- **Нечёткое изображение** лица на видео
- **Отсутствие мимики** при разговоре (инструменты создания дипфейков зачастую некорректно отображают мимику говорящего человека)
- **Неестественная мимика** лица (моргание глаз, движение бровей и губ)
- **Границы** наложенного изображения (различие в тенях, освещённости и оттенке кожи)



Как защититься

договоритесь внутри семьи о «кодовом слове»

в любой подозрительной ситуации спросите собеседника о тех вещах/ситуациях из жизни, детали которых знаете только вы с ним

Схема «фейковый родственник»

При помощи искусственного интеллекта **мошенники создают фейковые голосовые/видео сообщения**, которые сложно отличить от реального голоса/изображения вашего родственника

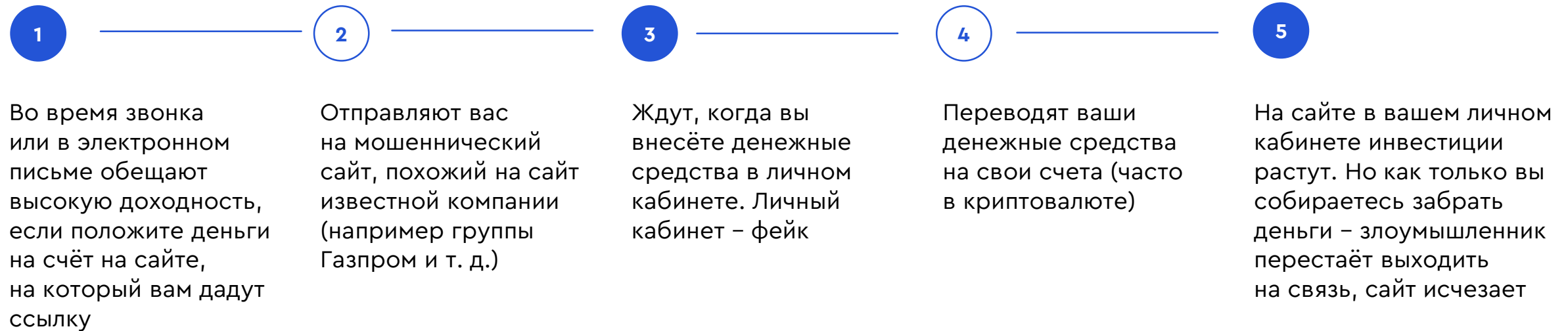
Таким образом, потерпевший полагает, что говорит со своим родственником, верит ему, и переводит деньги по указанному номеру или передаёт их стороннему человеку в условленном месте



Как поступить:

позвонить по известному вам номеру тому человеку, который, как вам показалось, вам звонил. И уточнить у него, правда ли он попал в затруднительную ситуацию и ему нужны деньги. **Важно задать какой-нибудь вопрос, ответ на который знаете только вы и ваш родственник!**

Схема мошенничества под видом инвестиций



Посты в соцсетях и рекламные баннеры в интернете часто обещают быстрый и очень высокий доход

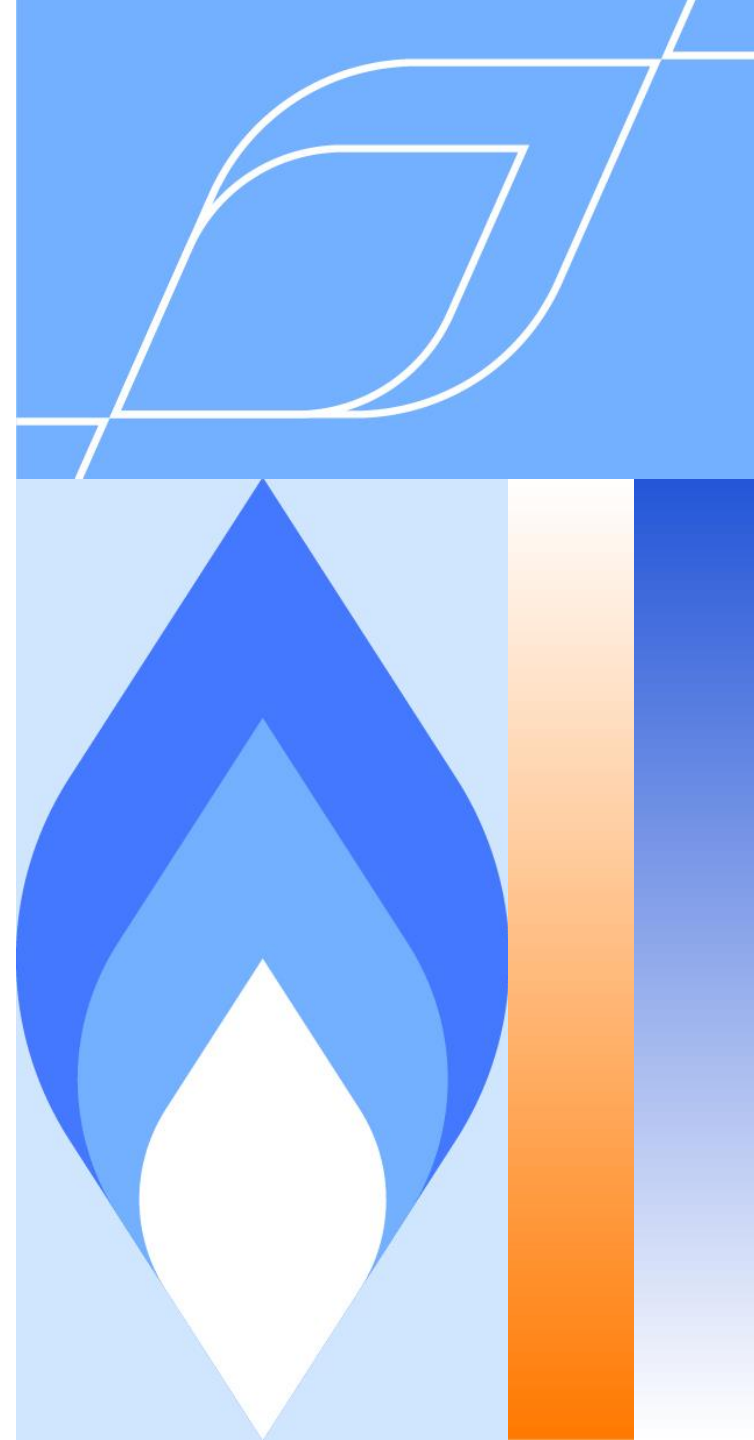
Цель злоумышленника – завлечь людей на мошеннические сайты, где якобы можно инвестировать в ценные бумаги и получить больше прибыли, чем на других площадках

После регистрации

Мошенники прикрепляют к обманутому пользователю так называемого «финансового эксперта», который якобы должен советовать активы к покупке и помогать инвестировать.

На самом деле его задача – убедить человека вложить как можно больше денег

Схемы мошенничества с участием детей

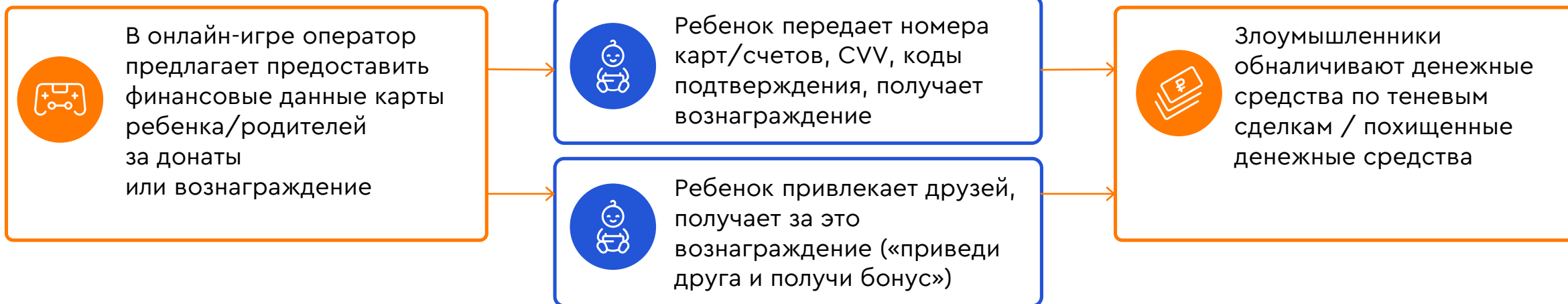


Схемы мошенничества с участием детей



Дроп (дроппер) – это человек, который задействован в **выводе похищенных денежных средств**

Противоправные действия



Звонок от имени администрации школы

Мошенники представляясь сотрудниками школьной администрации утверждают, что в системе МЭШ (Московская электронная школа) якобы произошел сбой и необходимо оперативно восстановить пароль от электронного журнала, иначе все данные будут утеряны

Когда дети называют нужный аферистам код, те получают доступ к аккаунту ученика в МЭШ и/или portalу Госуслуг Москвы

В одной из реализованных схем по легенде «МЭШ» 15-летний школьник отдал мошенникам около 5 млн. рублей. Подростка запугали угрозами, убедили вынести и передать курьеру деньги, которые родители копили на покупку квартиры. Далее ребенка отправили в квартиру к бабушке и заставили разговаривать с ними по видеосвязи для определения ценностей вещей

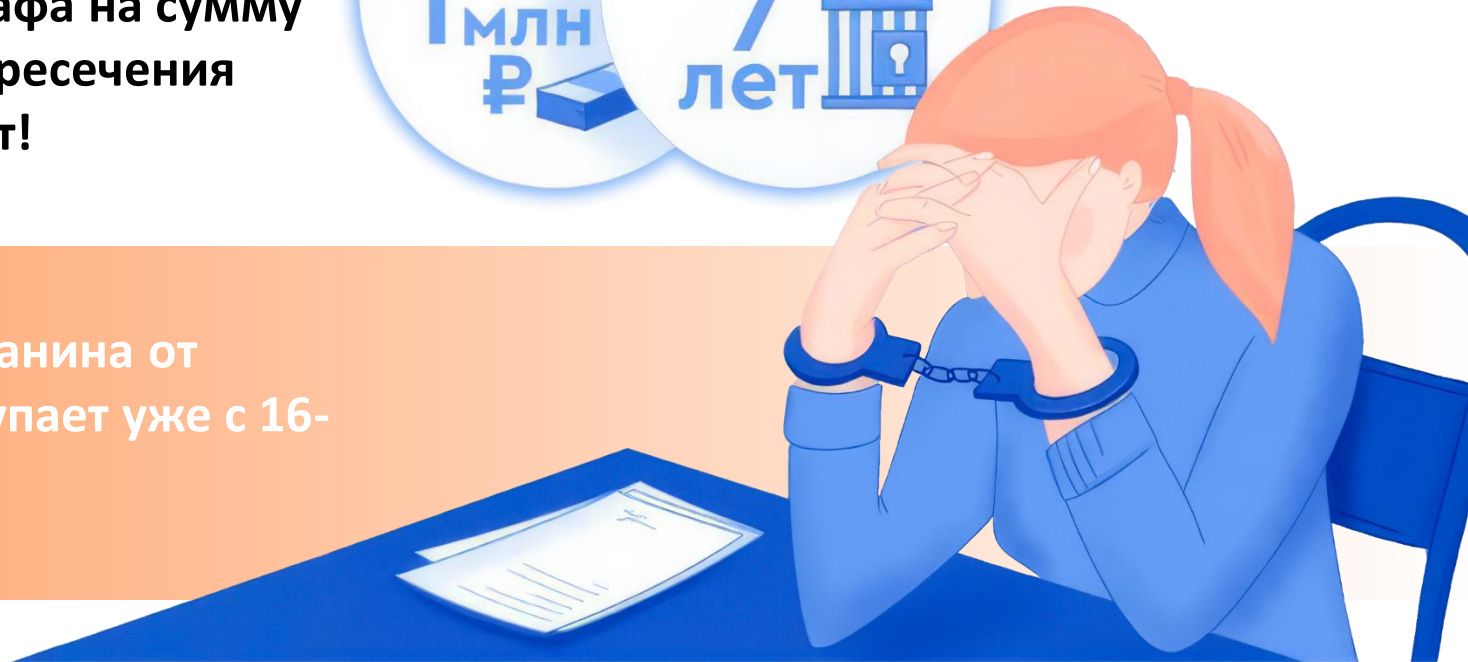
Ответственность за дропперство

В настоящее время **дропперство** может быть квалифицировано по нескольким статьям **Уголовного кодекса РФ**: как мошенничество (**статья 159 УК РФ**), легализация (отмывание) денежных средств (**статья 174 УК РФ**), неправомерный оборот средств платежей (**статья 187 УК РФ**), а также как организация преступного сообщества (**статья 210 УК РФ**).

Внимание родителям!

Мера пресечения устанавливается в виде лишения свободы сроком до 7 лет с выплатой штрафа на сумму до 1 млн. рублей. А самая строгая мера пресечения может быть установлена сроком до 20 лет!

Незнание законов не освобождает гражданина от уголовной ответственности, которая наступает уже с 16-летнего возраста!



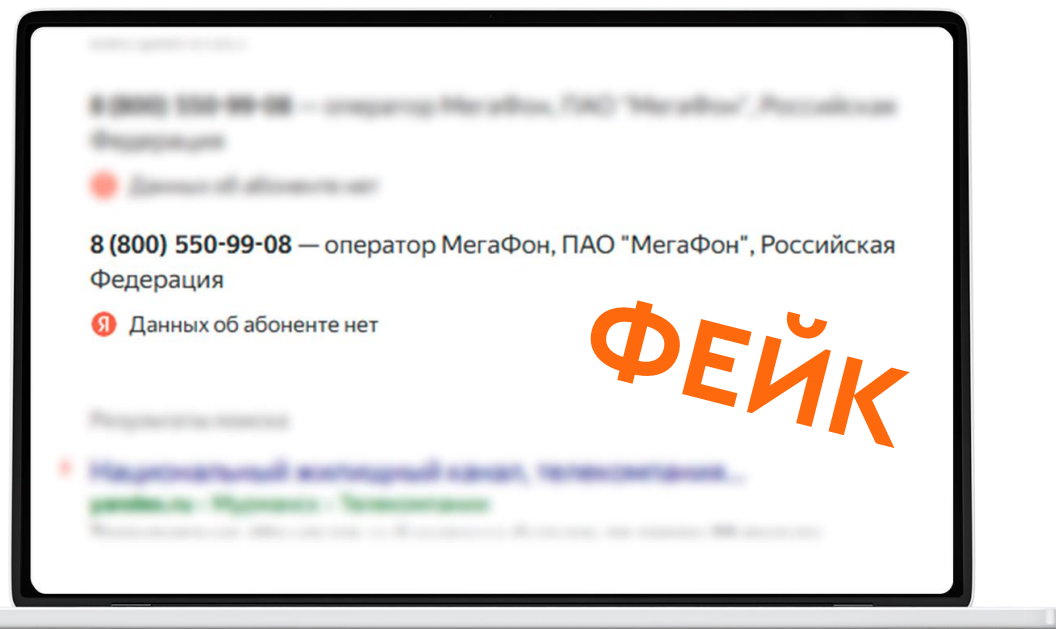
Пример из жизни

1. Ребенку **позвонил мошенник от лица Почты России** и сообщил, что на его Имя поступило заказное письмо
2. Далее **мошенник попросил озвучить код из СМС**, якобы для электронной или бумажной доставки письма (код на самом деле приходит от Госуслуг)
3. После разглашения кода из СМС, на email ребенка **поступило письмо о блокировке учетной записи на Госуслугах, с указанием фиктивного номера телефона** поддержки сервиса
4. Таким образом **мошенники хотели, чтобы жертва сама связалась с ними для «спасения» аккаунта**

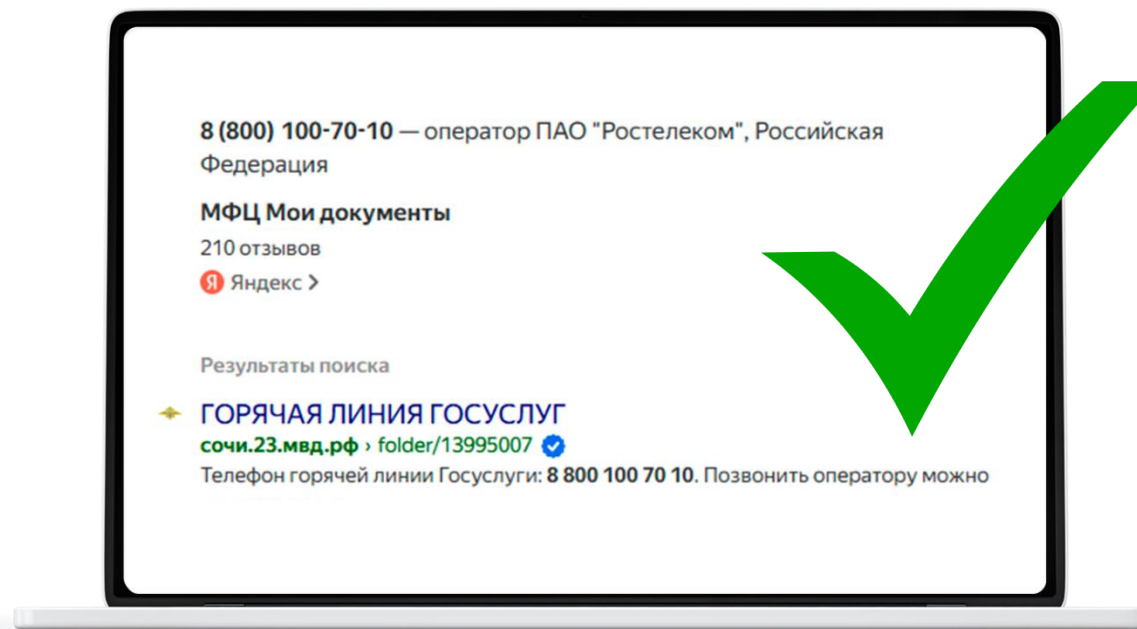


Пример из жизни

Проверка телефона указанного
в фиктивном письме в информационных
источниках



Проверка реального телефона
поддержки ГУ в информационных
источниках



Перед звонком в какие-либо структуры убедитесь в достоверности номера телефона!

Правила безопасного пользования интернетом для подростков и не только!



Правила безопасного пользования интернетом

1. **Не верьте всему, что видите или читаете в интернете.** При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.
2. **Нельзя сообщать** другим пользователям интернета **свою личную информацию** (адрес, номер телефона, номер школы, любимые места для игр и т.д.).
3. **Нельзя открывать файлы, присланные от неизвестных вам людей.** Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием. Если есть необходимость открыть файл, всегда можно проверить его через антивирус.
4. **Используйте веб-камеру только при общении с друзьями.** Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан. Если камерой не пользуйтесь, отключайте ее от компьютера/закрывайте специальной шторкой (**Ozon**: шторка для камеры ноутбука – 99 руб).
5. **Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом родителям.**
6. Помните, что **виртуальные знакомые могут быть не теми, за кого себя выдают.**

Как защититься от мошенников в онлайн-играх

1. **Установите антивирусы** на все устройства и не забывайте их обновлять.
2. **Скачивайте игры только на официальных сайтах** и в проверенных магазинах приложений.
3. Используйте везде разные и сложные пароли.
4. **Никогда и никому не сообщайте пароли от своих аккаунтов.** Прежде чем вводить где бы то ни было персональные данные, коды или реквизиты банковской карты, удостоверьтесь, что это не мошенническая страница.
5. **Не переходите по сомнительным ссылкам** от незнакомцев, кем бы они ни представлялись — другими игроками, техподдержкой или организатором кибертурнира.

Важно! Если вы скачиваете игры и/или программы с непроверенных сайтов, не используете антивирусное ПО, активно переходите по непроверенным ссылкам, не рекомендуется хранить на данном компьютере конфиденциальную информацию (документы, личные фотографии и т.д.), заходить в банковские и государственные сервисы, использовать web-версии мессенджеров.

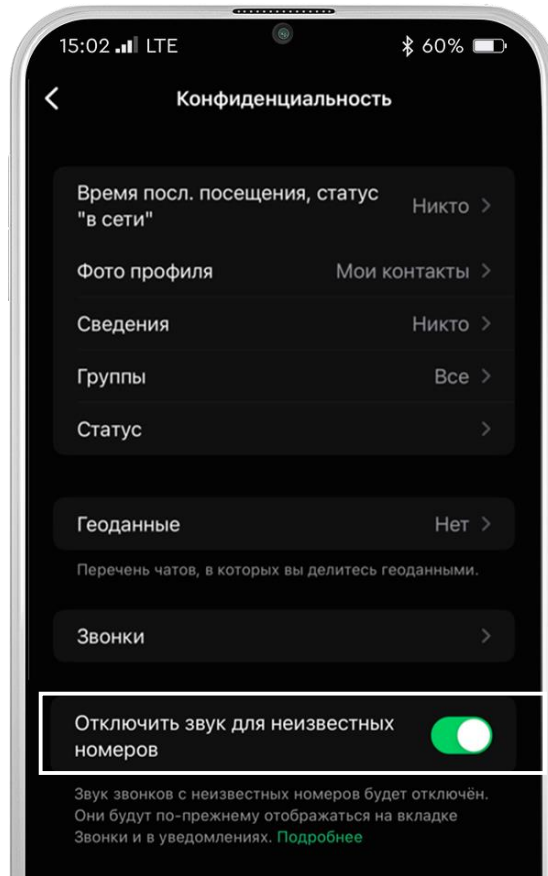
Полезные рекомендации



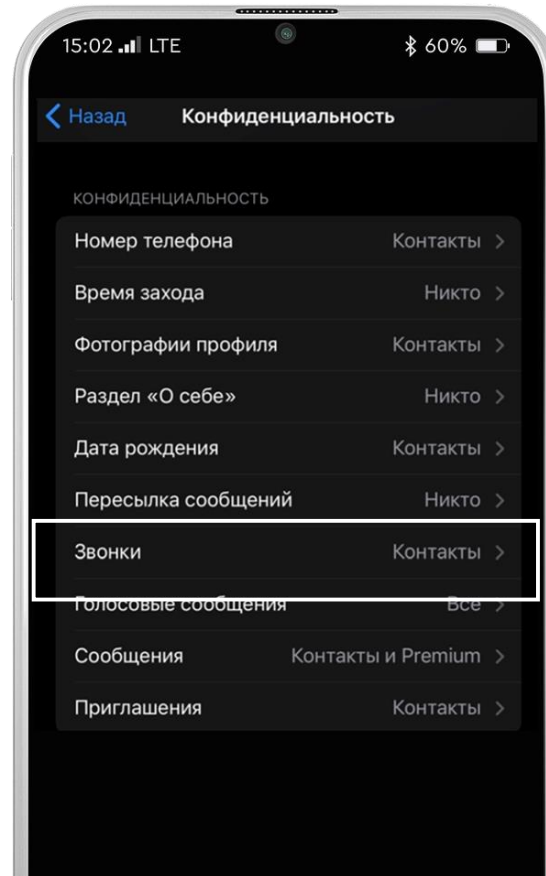
Простые настройки смартфона и мессенджеров для того, чтобы избежать нежелательных звонков

Настройки мессенджера → Конфиденциальность

WhatsApp

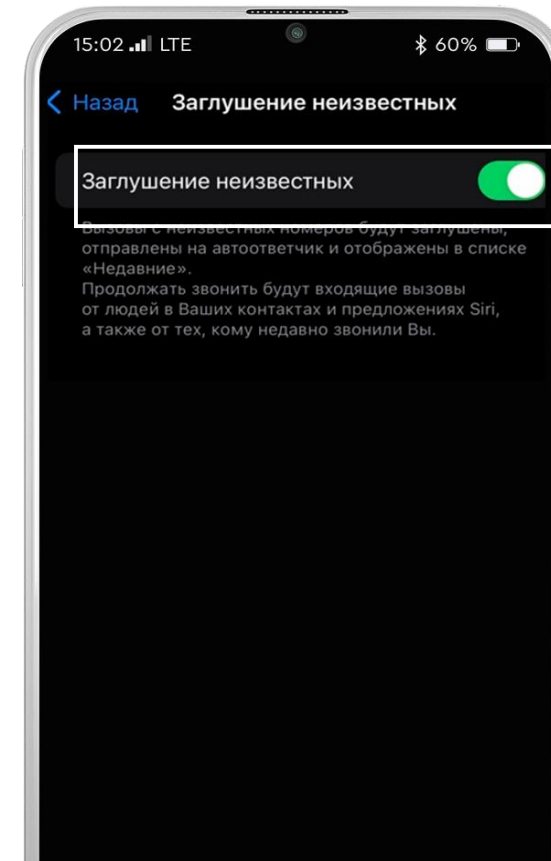


Telegram



Настройки смартфона

Сотовая связь



Установив данные настройки, мошенники просто не смогут связаться с вами, вашими родственниками и детьми!

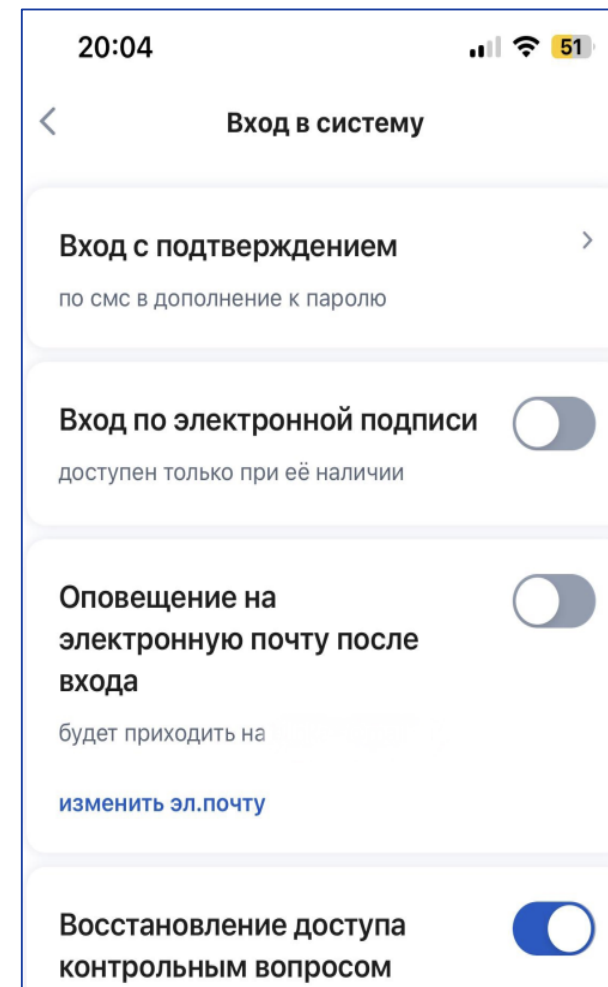
Как защитить аккаунт в Telegram

1. Не переходите по ссылкам из личных сообщений, если они ведут на неизвестные вам сайты
2. Не вводите на страницах, в подлинности которых вы не уверены, персональные данные, логины и пароли от Telegram, почты и других систем
3. Установите двухфакторную аутентификацию, обязательно укажите при этом e-mail для восстановления пароля (Настройки > Конфиденциальность > Облачный пароль > Установить пароль)
4. Проверьте раздел «Активные сессии» (Настройки > Устройства). Если там окажется незнакомая сессия, завершите ее и поменяйте пароль от аккаунта, если он был установлен
5. Своевременно устанавливайте обновления.

Выполнив простые рекомендации – вы обезопасите личную информацию от утечек и несанкционированного доступа!

Настройка восстановления доступа к Госуслугам через контрольный вопрос

Профиль → Безопасность → Вход в систему →
Восстановление доступа контрольным вопросом



Контрольный вопрос – это дополнительный уровень безопасности, который значительно усложняет жизнь мошенникам. Даже если злоумышленники смогут подобрать пароль к личному кабинету, они не смогут его заменить, не зная ответа на контрольный вопрос.

С 1 марта есть возможность установить самозапрет на выдачу кредитов через портал **Госуслуг**

Самозапрет — это добровольное ограничение, которое человек устанавливает, чтобы нельзя было оформить кредит на его имя.

Запрет вносится в базы данных бюро кредитных историй (БКИ).

И при любой проверке потенциального заёмщика банки получают уведомление, что выдача кредита запрещена.



Установление самозапрета доступно по ссылке www.gosuslugi.ru/644881/1/form или QR-коду

Обращаем внимание, что мошенники нашли новый способ обмана, теперь они звонят от имени «Госуслуг» и убеждают, что при установке самозапрета произошла ошибка, после чего:

- Присылают фишинговую ссылку для «исправления заявления»
- Крадут логин и пароль от «Госуслуг»
- Получают доступ к банковским счетам и персональным данным

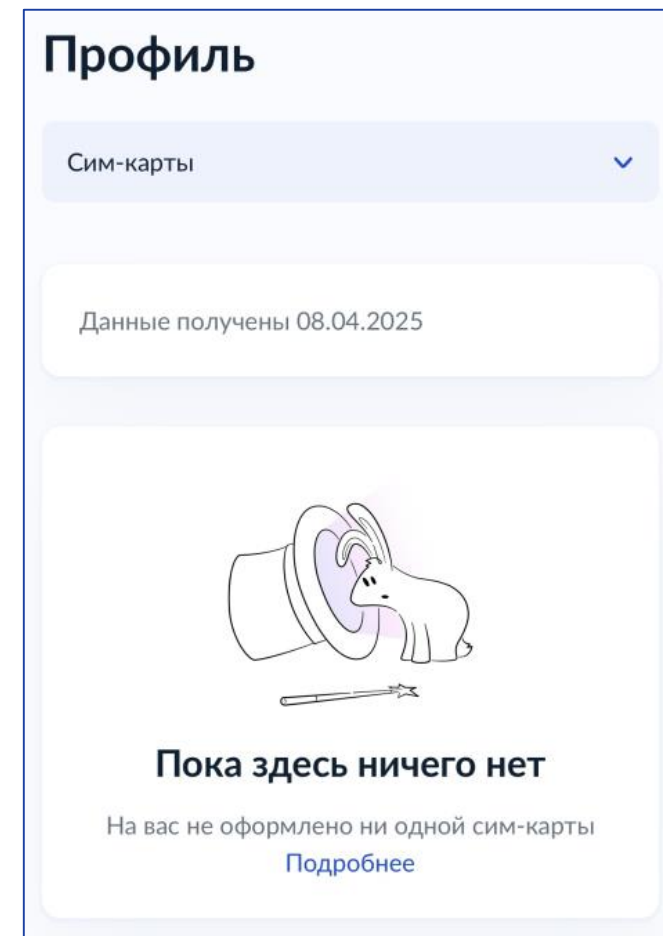


Будьте бдительны! Сотрудники **Госуслуг не звонят и не присылают никаких ссылок!**

С 1 апреля 2025 года доступен сервис «Сим-карты» на портале **Госуслуг**

Чтобы войти в него, нужно:

1. Открыть приложение или официальный сайт портала «Госуслуги».
2. Перейти в профиль в верхней части экрана.
3. В списке функций, сразу под «Учётной записью», выбрать «Сим-карты».



Проверить свои сим-карты на **Госуслуг** важно по многим причинам, например, так вы защититесь от мошенников: если на вас оформили номер телефона без вашего участия, его нужно заблокировать.

Дополнительные рекомендации к portalу Госуслуг

Для владельцев недвижимости:

В офисе МФЦ или через портал Госуслуг можно подать заявление на запрет сделки с недвижимостью без личного участия, чтобы **защитить себя и своих близких** от мошенников. Также можно воспользоваться приложением Госключ с усиленной квалифицированной электронной подписью (УКЭП).

Минимизация мошенничества со стороны сотрудника сотовой связи:

В ближайшее время на портале Госуслуг также появится возможность выставить самозапрет на оформление СИМ-карт у сотовых операторов.

Рекомендации

- **Сериал «Вас беспокоят из банка» (4 серии, доступен по qr-коду) —→**

В документальном сериале о телефонных мошенниках специалисты подробно расскажут о методах работы мошенников, приведут примеры психологических манипуляций злоумышленников и дадут несколько советов, как не попасться в их сети.



- **Выпуск «Как крадут наши деньги» на канале МИНАЕВ LIVE (доступен по qr-коду)**

← Как появилось интернет-мошенничество, для чего крадут данные, почему люди переводят деньги мошенникам, как не стать жертвой мошенников, об этом и многом другом рассказывает Сергей Минаев (блогер, писатель).

- **Сайт Банка России, раздел «Противодействие мошенническим практикам» (доступен по qr-коду) —→**

Актуальные схемы мошенничества и общие рекомендации от Банка России.



Проведите время с пользой, делитесь с родными и близкими нашими рекомендациями фильмов/каналов по теме социальной инженерии

Рекомендации

- Официальный телеграм-канал Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России «Вестник Киберполиции России» (доступен по qr-коду) →

Ежедневная публикация актуальных схем мошенничества и способах противодействия от УБК МВД России



@CYBERPOLICE_RUS



Важно посмотреть с детьми!

← Онлайн-урок директора Департамента информационной безопасности Банка России Вадима Уварова «Дропперы: как не стать помощником кибермошенников» (урок доступен по qr-коду)

Проведите время с пользой, делитесь с родными и близкими нашими рекомендациями фильмов/каналов по теме социальной инженерии

Рекомендации пострадавшему клиенту



Схемы, используемые мошенниками, в большинстве случаев, в конечном итоге приводят к получению доступа к Вашему личному кабинету в **Госуслугах или полному доступу к мобильному устройству!**

Если вам сообщают о каких-то несанкционированных действиях с вашим аккаунтом на «Госуслугах»



Позвоните на горячую линию портала

8 800 100 70 10



Используйте **чат-бот от Госуслуг**,
в котором всегда под рукой нужные
и важные чек-листы на все случаи жизни

@gosuslugi_checklist_bot

Что делать, если Вас взломали на Госуслугах?

1. Восстановите пароль

- онлайн через Банк, в котором можно онлайн восстановить доступ к госпорталу (сервис «Регистрация на «Госуслугах»);
- лично в центрах обслуживания, в т.ч. в отделениях определенных банков.

2. Защитите учетную запись (контрольный вопрос и т.п.).

3. Выйдите из учетной записи со всех устройств, кроме текущего

Профиль → Безопасность → вкл. «Действия в системе»/ «Моб. приложения» → «Выйти».

4. Посмотрите, где использовалась учетная запись

Профиль → Безопасность → вкл. «Действия в системе» (особое внимание на упоминание банков и МФО).

5. Проверьте заявления и уведомления (запросы ЭТК, 2-НДФЛ и т.п.).

6. Убедитесь, что на Вас не взяли кредит

Запросите на «Госуслугах» список БКИ, в которых есть Ваша кредитная история → Закажите отчеты в БКИ → посмотрите, какие заявки на кредиты подавались от Вашего имени. Далее обратитесь в одно из 3х БКИ для получения детального отчета (потребуется учетная запись на «Госуслугах»).

Если вы получили смс о смене пароля на «Госуслугах», нельзя переходить по ссылкам и звонить на номера, указанные в сообщении! Это может быть мошенническая схема, т.к. злоумышленники зачастую выдают себя за работников портала и заявляют, что ваш профиль якобы попал в руки мошенников.

Восстановление доступа в аккаунт Telegram:

Если доступ к аккаунту утерян, но прошло менее суток, его можно восстановить через привязанный номер телефона:

- Открыть приложение
- Ввести свой номер телефона и нажать «Войти»
- Если аккаунт не удален полностью, Telegram предложит ввести пароль или восстановить его через привязанные данные
- Завершить сеанс со всех устройств, кроме текущего, в разделе «Устройства»

Если прошло более суток, то нужно создать заявку на telegram.org/support, написать на п/я поддержки Телеграмм reports@stel.com обращение с текстом:

*Hello. My account was hacked and when I log in in to my account, it kicks me out of my session.
Can you reset all my sessions so that I can log in to my account via SMS code?
My phone number is +7****.*

Ожидайте действий технической поддержки, в течение суток вы получите ответ на электронную почту и зайдете в аккаунт.

Оперативно сообщите близким о взломе вашего аккаунта (через альтернативные источники связи, например: сотовая связь/социальные сети/мессенджеры), предупредите, что не стоит реагировать на подозрительные сообщения с вашего аккаунта!

Пришли деньги на карту от неизвестного: почему это опасно и что делать

Тратить полученные деньги ни в коем случае нельзя. Вместо этого нужно понять источник поступления и причину перевода. Обратитесь в банк, сообщите о случившемся и следуйте их рекомендациям.

Несанкционированные денежные переводы могут быть частью мошеннических схем и привести к серьезным последствиям!

Чем опасны такие переводы:

Потеря собственных средств

Если вы решите вернуть деньги по просьбе «отправителя» на указанные им реквизиты или телефон, есть риск, что перевод был фиктивным. В этом случае вы можете потерять собственные деньги, так как по закону полученные средства являются неосновательным обогащением и вам не принадлежат.

Участие в отмывании денег

Получение денег от неизвестных источников может означать, что вы непреднамеренно стали участником схемы по отмыванию денег. Это может привести к серьезным юридическим последствиям, включая обвинения в соучастии в преступной деятельности.

Эту и другие полезные статьи на тему безопасности читайте на сайте Газпромбанка: <https://www.gazprombank.ru/pro-finance/safety/>



Скачивайте памятку

«Как защитить себя и своих близких»,

отсканировав QR-код

Делитесь полезной информацией
с родными и близкими



Спасибо за внимание

