

Как защититься от мошенников 2.0

Альфа Банк

Сегодня вы узнаете:



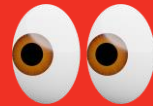
1

Актуальная
статистика
и основные виды
мошенничества



2

Современные
методы
телефонного
мошенничества



3

Новые схемы
интернет-
мошенничества



4

Мошенничество,
направленное
на детей: риски
и защита



Сталкивались ли вы с мошенниками?

Альфа Банк

Статистика за 2025 год



13,1

млрд ₽

мошенники похитили
у россиян за период 1-2
квартал 2025 года, что
на 32,6% больше, чем в
период 2024 года

по данным ЦБ РФ

43,8

млн.

попыток мошенников
похитить деньги
предотвратили банки,
что в 2 раза больше,
чем в 2024 году

269,1

тыс.

мошеннических
операций пришлось
на физических лиц

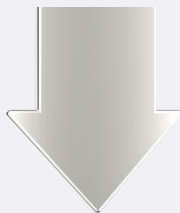
7,6%

украденных средств
банки вернули
клиентам

Мошеннические схемы

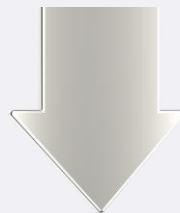


По телефону и SMS



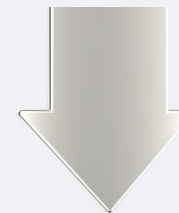
- 1 Фишинг
- 2 Мошенничество с выигрышами
- 3 Служба поддержки
- 4 Мошенничество с кредитами
- 5 Лжеблаготворительность

В интернете



- 1 Фишинг- сайты
- 2 Мошенничество в соц. сетях
- 3 Инвестиционные схемы
- 4 Ложные интернет-магазины
- 5 Дропперство

С помощью нейросетей



- 1 Генерация поддельных видео и аудио
- 2 Автоматизированный фишинг
- 3 Манипуляции с текстом
- 4 Имитация общения
- 5 Создание поддельных документов

Новые угрозы

Телефонное мошенничество

Альфа Банк

Телефонные SMS и звонки от мошенников



Признаки

- 1** На вас выходят сами
Операции по карте, выигрыши, выплаты
- 2** С вами говорят о деньгах
Операции по карте, выигрыши, выплаты
- 3** Вас просят сообщить данные
Персональные данные, данные банковской карты, коды
- 4** Вас выводят из равновесия
Пугают, торопят, не оставляют выбора
- 5** На вас «давят»
Предлагают вложения с большой доходностью прямо сейчас



Способы защиты

- 1** Регулярно проверяйте кредитную историю через НБКИ и Госуслуги
- 2** Установите определитель номера
- 3** Никому не сообщайте ваши данные

Примеры

- Звонки с незнакомых номеров
- Взлом аккаунта и ведение диалога от другого лица
- На почту приходят письма о зачислении средств
- Обвинение в нарушении закона

Мошенничество под видом доставки



Мошенники звонят от лица маркетплейсов, курьерских служб или цветочных магазинов, сообщая о доставке и предлагая подтвердить личность по СМС-коду, чтобы получить доступ к личным данным и банковским счетам жертвы

Схема

1

Сообщение о доставке:

Злоумышленники утверждают, что заказ посылки или цветов уже оплачен и предлагают согласовать время получения

2

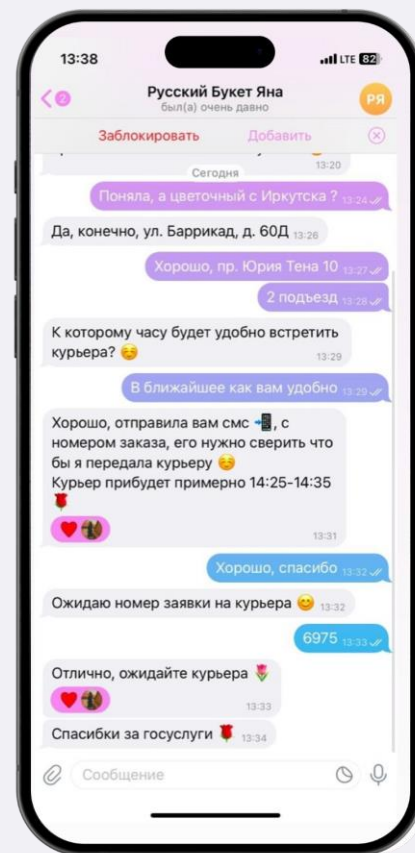
Запрос кода из СМС:

Жертве предлагают подтвердить личность, попросив назвать код из СМС, якобы для службы доставки или безопасности платформы

3

Ссылка на поддельный сайт:

В некоторых случаях мошенники направляют ссылку на фальшивый сайт курьерской компании, где запрашивают ввод личных данных



Опасность таких звонков:

- Подобные действия направлены на получение доступа к вашим личным данным или финансовой информации, что может привести к серьёзным последствиям

Рекомендация:

- При малейшем подозрении на мошенничество немедленно прекратите общение и обратитесь в правоохранительные органы для предотвращения возможных рисков



Мошенничество под видом социальных служб



Мошенники звонят, представляясь работниками Социального фонда России или сотрудниками страховой компании и предлагают различные услуги, такие как перерасчет пенсии или продление полиса медицинского страхования

Социальный фонд

- 1 Звонок от «Социального фонда»:**
Преступники представляются сотрудниками Социального фонда и предлагают провести перерасчёт пенсии с целью её увеличения
- 2 Запрос личных данных:**
Под предлогом оформления заявления они просят предоставить личные данные, код из СМС или установить приложение на телефон
- 3 Доступ к устройству:**
Получив доступ к устройству, мошенники входят в личный кабинет пенсионера на портале «Госуслуги»
- 4 Финансовые риски:**
Используя доступ к личным данным, злоумышленники оформляют кредиты на имя жертвы или выводят средства через онлайн-банк

Страховая компания

- 1 Звонок от «страховой компании»:**
Злоумышленники представляются сотрудниками страховой компании и настойчиво предлагают продлить полис обязательного медицинского страхования (ОМС)
- 2 Запрос установки приложения:**
Под предлогом оформления продления полиса они убеждают установить на телефон якобы приложение Минздрава. На самом деле это вредоносное ПО, которое предоставляет преступникам доступ к устройству
- 3 Запрос СМС-кода:**
Мошенники могут также попросить СМС-код для входа в личный кабинет на портале «Госуслуги», что позволяет им получить доступ к личным данным и финансовым ресурсам жертвы

Мошенничество с «аккаунтом безопасности»:

- 1 **Злоумышленники** представляются сотрудниками сервиса и убеждают активировать «аккаунт безопасности»
- 2 Под предлогом защиты данных они запрашивают **код из СМС** от портала «Госуслуги»
- 3 Объясняют запрос якобы **интеграцией** мессенджера с государственными сервисами
- 4 На самом деле такая интеграция не существует, а **цель мошенников** — получить доступ к личным данным



Сегодня 16:00

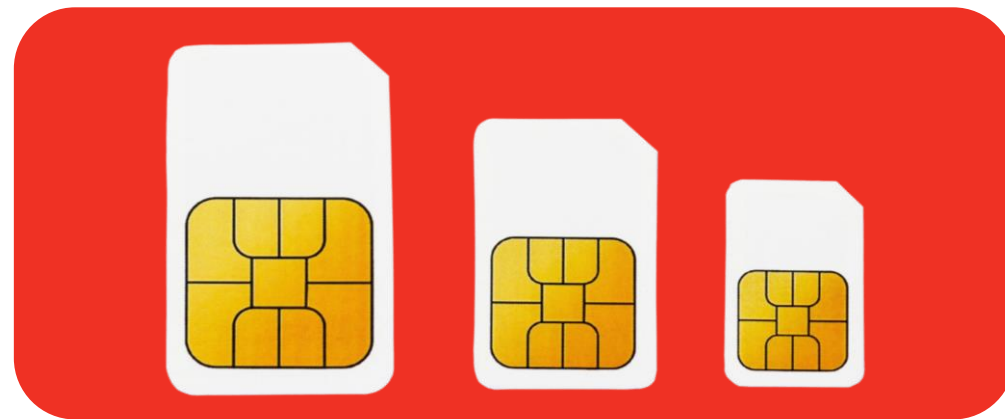
Подтверждение смены пароля на Госуслугах Никому не сообщайте код. Его спрашивают ТОЛЬКО мошенники. Код

«Серые» SIM-карты



- 1** Мошенники звонят и сообщают, что номер телефона находится в реестре **«серых» SIM-карт** и может быть заблокирован
- 2** Чтобы **«вынести»** номер из этого списка, они просят назвать личные данные (ФИО, адрес электронной почты, ИНН или тип документа) и код из SMS
- 3** **Получив код**, мошенники получают доступ к личному кабинету жертвы и её персональным данным

! Благодаря коду и прочим данным, злоумышленник получает доступ к аккаунтам жертвы на важных ресурсах вроде «Госуслуг»



Мошенник или нет?



Вы получили телефонный звонок от службы доставки. Вам сообщают, что курьер уже находится рядом, но для окончательного подтверждения доставки необходимо назвать полученный в SMS код.

Как Вы поступите?

- 1 Назову код, чтобы курьер смог завершить доставку
- 2 Попрошу курьера назвать мои данные (адрес, номер заказа), чтобы убедиться, что это действительно мой заказ, и только потом назову код
- 3 Завершу разговор, не называя никаких кодов, и самостоятельно свяжусь со службой доставки по официальным контактам, чтобы уточнить информацию

Новые угрозы в интернете

Альфа Банк

*вид интернет-мошенничества, когда мошенники притворяются кем-то надёжным (например, банком или знакомым), чтобы обманом выманить у вас пароли, данные банковской карты или другую личную информацию



Способы защиты

- 1 Не переходите по ссылкам от незнакомых отправителей
- 2 Не вводите персональные данные
- 3 Не доверяйте случайным выигрышам

Признаки

- 1 Вам предлагают перейти по ссылке
Из смс-сообщения или из письма на почте
- 2 Вас просят сообщить данные
Персональные данные, данные банковской карты, коды

Примеры

- Сайты-двойники популярных сервисов
- Предложение перейти по ссылке, чтобы получить подарок
- Маскировка под письмо от существующей компании или сервиса

Фишинговые письма о штрафах ГИБДД



Мошенники рассылают фальшивые уведомления о штрафах ГИБДД, чтобы обмануть автовладельцев и украсть их деньги

Схема

- 1 Рассылка сообщений якобы от ГИБДД с утверждением о нарушении ПДД
- 2 В тексте сообщения содержится призыв оплатить штраф до указанной даты
- 3 К письму прикрепляется поддельный PDF-документ и кнопка «Оплатить»
- 4 При нажатии на кнопку открывается фальшивый сайт, где запрашиваются данные банковской карты и СМС

Помните

- Настоящие штрафы приходят только через официальные каналы
- Официальные органы и банки не требуют оплат по ссылкам и не запрашивают пароли и коды из смс
- Никогда не переходите по подозрительным ссылкам и не открывайте вложения от неизвестных отправителей



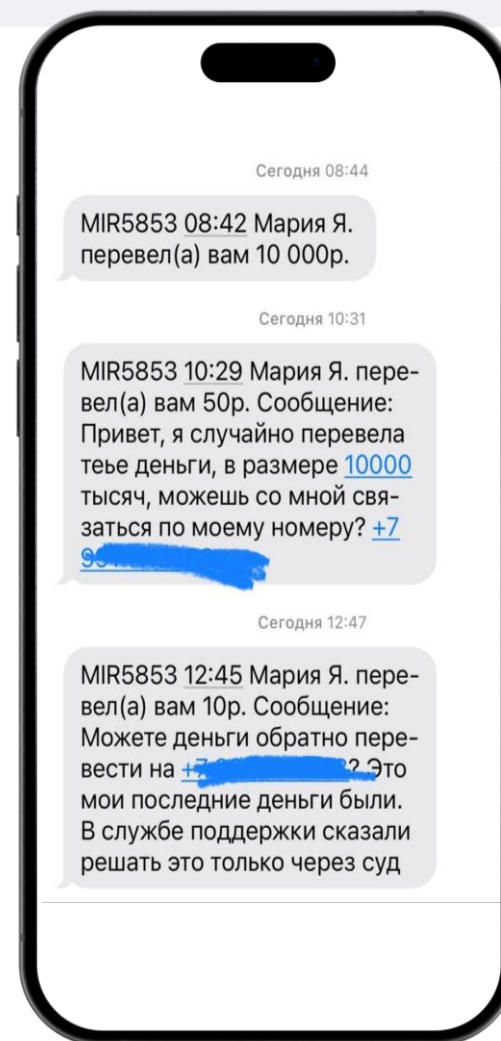
Ложные переводы



Вид мошенничества, при котором создаётся иллюзия ошибочного зачисления денег на ваш счёт. Мошенники под различными предлогами требуют вернуть средства, утверждая, что перевод был случайным

Развитие событий

- 1 Неожиданный перевод средств:**
На ваш банковский счёт или электронный кошелек поступает перевод. Сумма может быть как небольшой, так и значительной
- 2 Контакт с «отправителем»:**
Вскоре с вами связывается человек, представляющийся отправителем или его представителем, и утверждает, что перевод был ошибочным
- 3 Убедительные объяснения:**
Мошенники предлагают причины «ошибки», чтобы вызвать доверие:
 - Неправильный ввод номера карты при оплате
 - Ошибочный перевод родственнику
 - Ошибка бухгалтера при перечислении зарплаты
- 4 «Давление» на жертву:**
«Отправитель» требует срочного возврата средств, используя «давление», агрессию или демонстрируя беспомощность
- 5 Манипуляция способом возврата:**
Мошенник предлагает удобный для себя способ возврата: перевод на другой счёт, номер телефона, электронный кошелек или наличными при личной встрече



Ложные переводы: Как распознать и защититься



Схема 1

Перевод с украденной карты:

- Деньги переводятся с украденной карты
- После возврата средств отправителю банк списывает их, и получатель теряет как переведённые, так и свои деньги

Схема 2

Без фактического перевода:

- Мошенники используют поддельные чеки или скриншоты, создавая иллюзию перевода
- Средства отправляются из личных денег получателя



Схема 3

С заблокированного счёта:

- Перевод осуществляется с счёта, который вскоре блокируется
- Банк отменяет транзакцию, но деньги уже возвращены мошенникам

Как защититься?

✓ Сохраняйте бдительность:

Не спешите возвращать деньги при получении неожиданного перевода, пока не убедитесь в его законности

✓ Проверяйте информацию:

Свяжитесь с банком или платежной системой для подтверждения подлинности и легитимности транзакции

✓ Не поддавайтесь давлению:

Избегайте принятия поспешных решений, даже если на вас оказывают эмоциональное или психологическое воздействие

✓ Действуйте при подозрении:

Сообщайте о подозрительных действиях в банк и правоохранительные органы для предотвращения дальнейшего мошенничества

✓ Игнорируйте подозрительные сообщения:

Не реагируйте на сомнительные запросы, чтобы минимизировать риск стать жертвой мошенников

Мошенник или нет?



Вы получили письмо на почту о том, что кто-то пытается получить доступ к вашему аккаунту на Госуслугах. В сообщении предлагается подтвердить безопасность аккаунта, пройдя по ссылке и введя логин и пароль, в противном случае аккаунт будет заблокирован.

Как Вы поступите?

- 1 перейду по ссылке в SMS и введу логин и пароль, чтобы «защитить» аккаунт
- 2 Позвоню в службу поддержки по номеру из письма, чтобы разобраться
- 3 Не переходя по ссылке, сразу зайду на официальный сайт Госуслуг самостоятельно, проверю уведомления и при необходимости сменю пароль

Новые угрозы с детьми

Альфа Банк

Мошенничество с детьми



25%

рост количества несовершеннолетних, ставших жертвами киберпреступников по сравнению с прошлым годом

Мошенники связываются с детьми в онлайн-играх, завоевывают доверие и убеждают их совершить действия, направленные на хищение средств со счетов взрослых, такие как отправка фото карты или перевод денег в приложении онлайн-банка



Советы

- 1 Настройте семейный доступ и лимиты покупок в смартфоне ребёнка
- 2 Разрешите установки приложений только из официальных магазинов; включите запрет неизвестных источников
- 3 Введите кодовое слово семьи для экстренных ситуаций

Мошенничество в игровых сообществах



1

Вирусы через игры

Мошенники предлагают скачать моды или бонусные версии Minecraft, Roblox. Вместо этого устанавливается вредоносное ПО, получающее доступ к устройству и финансам

2

Фишинговые сайты

Создаются поддельные сайты-магазины с дешевыми скинами и игровыми предметами. Ребёнок вводит логин/пароль, данные карты, мошенники крадут аккаунт и средства

3

Переводы через детей

Мошенники убеждают ребёнка ввести данные карты родителей или перевести деньги за «промокод», бонус или победу в конкурсе

4

Розыгрыши бонусов

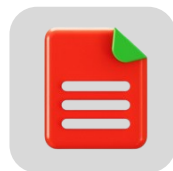
Предлагают выиграть внутриигровую валюту, просят данные аккаунта или карты, после чего захватывают учётную запись



Мошенничество в родительских чатах

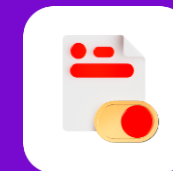


1 Школьные чаты



- Мошенники взламывают мессенджер классного руководителя и создают группу с родителями
- При переходе в такие чаты вы столкнётесь с просьбами перевести деньги на школьные нужды, учебные материалы, экскурсии и прочее
- При переводе денежных средств на счета мошенников они удаляют группу

2 Опросы для родителей и детей



- Мошенники рассылают сообщения в мессенджеры и соцсети о готовности к школе, питании в школьных столовых, школьных кружках и прочее
- Сообщения могут прийти от имени классного руководителя или родительского комитета
- В сообщении содержится ссылка на сайт мошенников, где вас попросят авторизоваться через личный аккаунт, указав логин и пароль
- После авторизации ваш личный аккаунт перейдёт мошенникам, которые будут использовать его для обмана ваших родственников, друзей и знакомых

Мошенник или нет?



В родительском чате вашего класса приходит сообщение с ссылкой на сайт от классного руководителя о том, что в связи с обновлением школьного портала, для доступа к новому онлайн-дневнику всем необходимо пройти повторную регистрацию через Госуслуги.

Как Вы поступите?

- 1 Перейду по ссылке и введу свой логин и пароль от Госуслуг, чтобы получить доступ к дневнику
- 2 Не буду переходить по ссылке из чата, а самостоятельно зайду на официальный школьный портал или в приложение онлайн-дневника, чтобы проверить информацию
- 3 Напишу в личные сообщения классному руководителю, чтобы уточнить, действительно ли требуется повторная регистрация через Госуслуги

Подведем итоги



SMS и звонки от мошенников

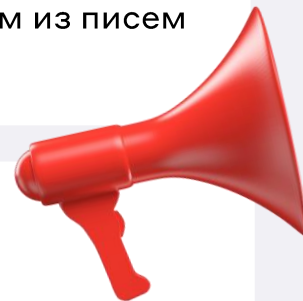
- 1 Всегда будьте насторожены при неожиданных звонках и сообщениях, вызывающих страх или срочность
- 2 Никогда не передавайте личные данные, банковские реквизиты, коды из SMS и пароли
- 3 Лучшее решение — прекратить разговор и самостоятельно связаться с организацией по официальному номеру

Фишинг

- 1 Мошенники создают поддельные сайты и рассылают письма, похожие на настоящие, для кражи данных
- 2 Проверяйте адрес отправителя и ссылки перед переходом
- 3 Не вводите конфиденциальную информацию на сомнительных сайтах
- 4 Лучше заходить на сайты напрямую через браузер, а не по ссылкам из писем

Мошенничество с детьми

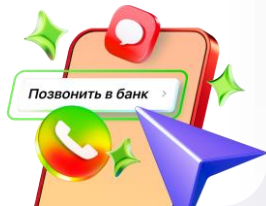
- 1 Дети — одна из самых уязвимых групп для мошенников, особенно в онлайн-играх и чатах
- 2 Обучайте детей правилам цифровой безопасности и используйте родительский контроль
- 3 Поддерживайте доверительные отношения, чтобы ребенок мог рассказать о подозрительных контактах и ситуациях в интернете
- 4 Введите кодовое слово семьи для экстренных ситуаций



Что делать, если вы стали жертвой мошенников



Заблокируйте карту
и немедленно
обратитесь
в банк



Подайте заявление
в банк о несогласии
с проведенной
операцией
не позднее 1 дня,
следующего
за днём получения
подозрительной
операции



Подайте заявление
в полицию

*В отделении,
по телефону 102 или 112, на
официальном сайте МВД
России*



Сообщите
о мошенниках
в Альфа-Мобайл



**Спасибо
за внимание!**

Альфа Банк