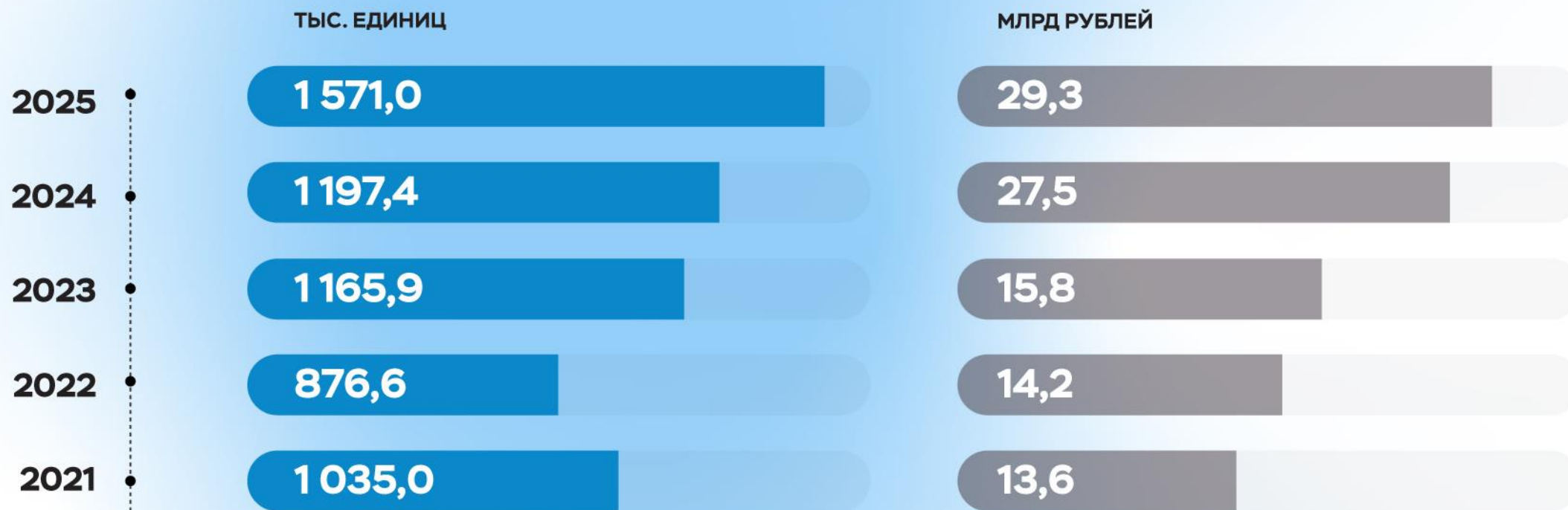




Банк России

КИБЕРМОШЕННИЧЕСТВО: ПРОТИВОДЕЙСТВИЕ НОВЫМ УГРОЗАМ

КИБЕРМОШЕННИЧЕСТВО: КОЛИЧЕСТВО ОПЕРАЦИЙ И УЩЕРБ*



В 2025 году банки предотвратили 134,2 млн мошеннических операций на 13,9 трлн рублей

* Физические и юридические лица

МОШЕННИКИ ПОДСТРАИВАЮТСЯ ПОД АКТУАЛЬНУЮ ПОВЕСТКУ

СОБЫТИЕ

СХЕМА ОБМАНА

1

Пандемия COVID-19

Предложение о выгодной покупке специальных лекарств или выплате социальных пособий

2

Ежегодная индексация пенсий

Предложение пересчитать пенсию из-за неучтенного стажа работы

3

Период подачи декларации о доходах за прошлый год

Рассылка электронных писем с требованием заплатить налоги

4

Летний сезон отпусков

Предложение о фиктивных горящих турах с огромными скидками

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«Сотрудник Пенсионного фонда
(социальной службы)»

Вам положена социальная выплата
по приказу Президента РФ



«Работник банка»

По карте зафиксирована
подозрительная операция



«Сотрудник Центробанка
(Банка России)»

Для сохранности денег вам нужно
перевести их на «безопасный»
(«специальный») счет в Центробанке



«Оператор мобильной связи»

Нужно переоформить договор
об оказании услуг связи



«Друг, родственник»

Ваш сын только что в результате
ДТП сбил человека. Я готов
помочь избежать наказания



«Представитель правоохранительных
органов (МВД, ФСБ, СК РФ)»

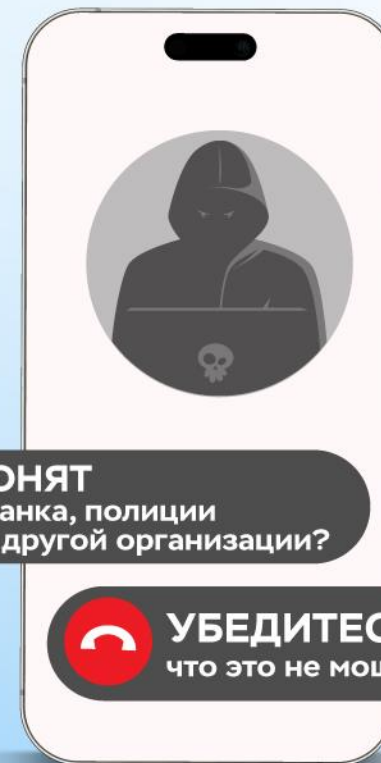
Беспокоит следователь МВД.
Вы являетесь свидетелем
по уголовному делу

ТЕЛЕФОН – ОСНОВНОЙ ИНСТРУМЕНТ МОШЕННИКОВ

Обман или злоупотребление
доверием

Психологическое
давление

Манипулирование



ЗВОНЯТ
из банка, полиции
или другой организации?



УБЕДИТЕСЬ,
что это не мошенники!



Под влиянием мошенников человек добровольно расстается
с деньгами или раскрывает личные и финансовые данные,
которые нужны злоумышленникам для хищения денег

ФОРМУЛА УСПЕХА ТЕЛЕФОННЫХ МОШЕННИКОВ



**ЭФФЕКТ
неожиданности**

+



**ЯРКИЕ
эмоции**

+



**ПСИХОЛОГИЧЕСКОЕ
давление**

+



**АКТУАЛЬНАЯ
тема**

**ЧЕЛОВЕК ГОТОВ СДЕЛАТЬ МНОГОЕ,
О ЧЕМ ЕГО ПРОСЯТ МОШЕННИКИ**

МОШЕННИКИ ИГРАЮТ НА ВАШИХ ЭМОЦИЯХ И ЧУВСТВАХ



ПОЛОЖИТЕЛЬНЫЕ

- Радость
- Надежда
- Доверие

«Вы выиграли крупную сумму денег»

«Вам положены социальные выплаты»

«Пенсионный фонд рад сообщить о перерасчете вашей пенсии, вам положена выплата в размере...»



ОТРИЦАТЕЛЬНЫЕ

- Страх
- Паника
- Стыд

«С вашего счета списали все деньги»

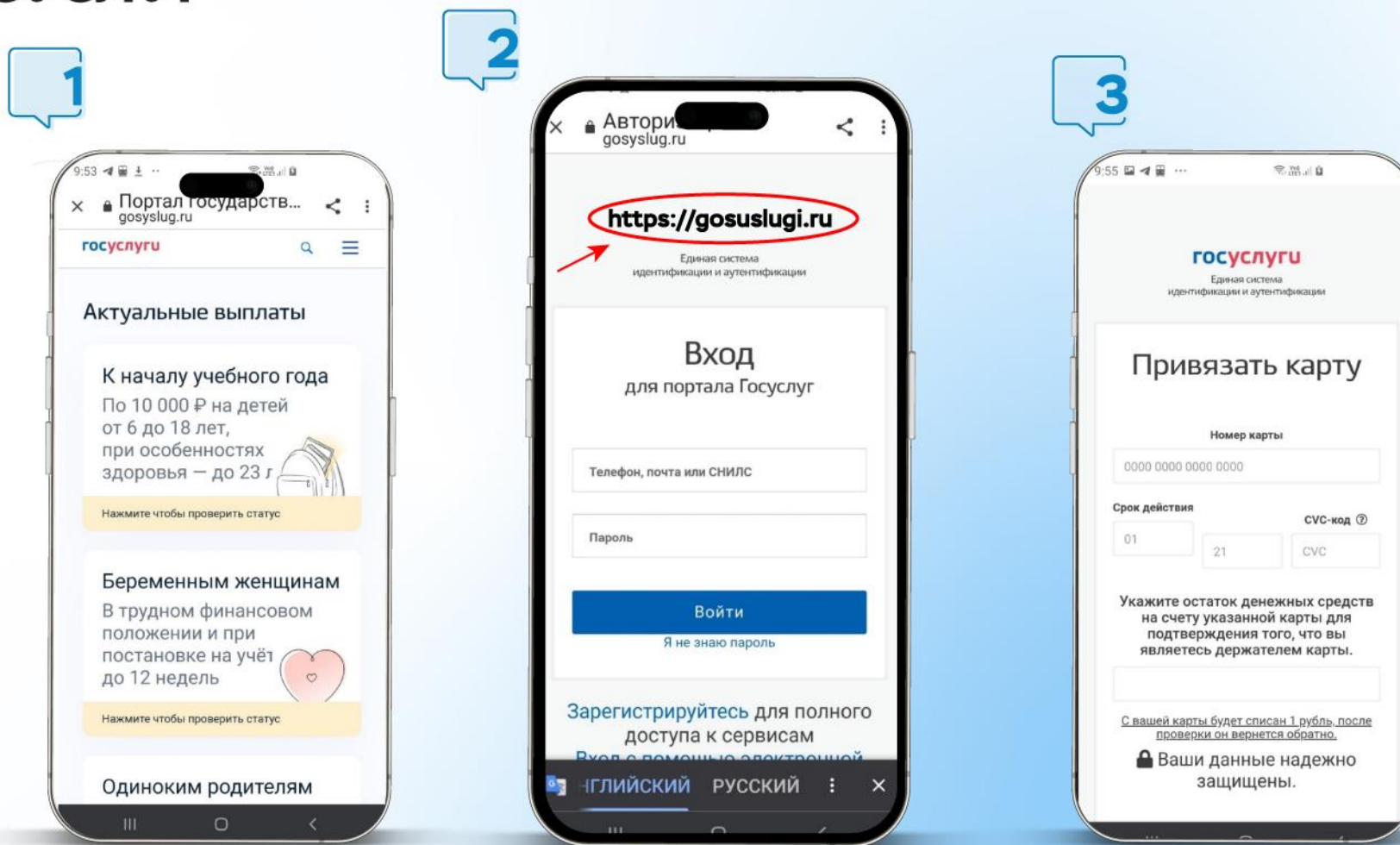
«Ваш родственник попал в аварию и сбил человека»

«Беспокоит следователь МВД. Вы являетесь свидетелем по уголовному делу»

ЛЖЕСОТРУДНИКИ ЦЕНТРОБАНКА: ФАЛЬШИВЫЕ ДОКУМЕНТЫ



МОШЕННИКИ ПОДДЕЛЫВАЮТ САЙТ ГОСУСЛУГ



Официальный сайт Госуслуг <https://gosuslugi.ru>

ПРИЗНАКИ ФИШИНГОВЫХ САЙТОВ

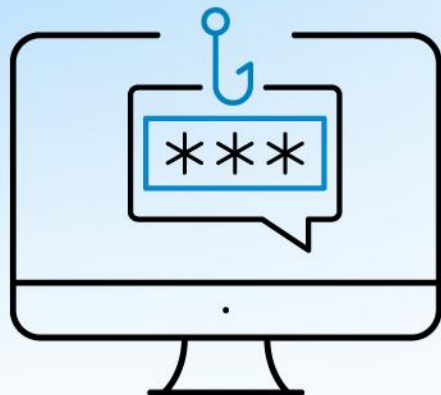


- ❶ Ошибки в адресе сайта
- ❷ Сайт состоит из 1 страницы (только для ввода данных)
- ❸ В адресной строке отсутствует значок замка
- ❹ В названии сайта нет **https://**
- ❺ Ошибки в тексте и недочеты в дизайне
- ❻ Побуждение ввести свои личные/финансовые данные
- ❼ Предложение скачать файл, установить программу



Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания!

ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ В ИНТЕРНЕТЕ



- Интернет-магазины и аукционы
- Онлайн-опросы и конкурсы
- Восстановление кредитной истории
- Сообщение о крупном выигрыше или выплате от государства
- Заманчивое предложение о работе
- Льготные кредиты
- Туристические путевки со скидкой
- Сбор «пожертвований» для детей, больных, животных и т. д.
- Предложение вложиться в высокодоходные инвестиции



Не верьте слепо предложениям в Интернете – проверяйте информацию на достоверность!

СРЕДНЕСТАТИСТИЧЕСКИЙ ПОРТРЕТ ПОСТРАДАВШЕГО

- Стать жертвой кибермошенников может любой человек, независимо от уровня образования и социального статуса
- В 2025 году с разными видами кибермошенничества сталкивались 29,1% граждан, принявших участие в опросе* Банка России
- Лишились денег 2,6% респондентов



**Работающая женщина
со средним уровнем
дохода**

Возраст: от 25 до 44 лет

Среднее образование

Проживает в городе

* В опросе, проведенном в ноябре 2025 года, приняли участие почти 460 тыс. человек

КАКИЕ СПОСОБЫ ВЗАИМОДЕЙСТВИЯ ПРЕДПОЧИТАЮТ МОШЕННИКИ*

55%

телефонный звонок
или СМС-сообщение

16%

мессенджеры

12%

сообщения в социальных
сетях и по e-mail

17%

иные
способы**

СКОЛЬКО ДЕНЕГ ТЕРЯЮТ ПОСТРАДАВШИЕ*

54,0%

до 20 тыс. рублей

20,2%

от 20 тыс.
до 100 тыс. рублей

14,6%

от 100 тыс.
до 500 тыс. рублей

4,9%

от 500 тыс.
до 1 млн рублей

6,3%

более
1 млн рублей

* Результаты опроса Банка России в 2025 году

** Вредоносные ссылки или компьютерные вирусы, поддельные интернет-ресурсы или QR-коды, получение доступа к аккаунту на Госуслугах, дипфейки и др.

КУДА ОБРАЩАЮТСЯ ПОСТРАДАВШИЕ



В свой банк



В полицию



Никуда



В иные организации
(в Роспотребнадзор,
Банк России,
к финансовому
уполномоченному)

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ ОТ КИБЕРМОШЕННИКОВ

- 1 **Не сообщайте** никому личную и финансовую информацию (данные карты)
- 2 **Не читайте** сообщения и письма от неизвестных отправителей и не перезванивайте по неизвестным номерам
- 3 **Не переходите** по сомнительным ссылкам и не скачивайте неизвестные файлы или программы
- 4 **Установите** на все свои гаджеты антивирусные программы и регулярно обновляйте их
- 5 **Заведите** отдельную банковскую карту для покупок в Интернете



**Будьте бдительны: не действуйте впопых и проверяйте информацию!
Расскажите об этих правилах поведения своим друзьям и знакомым**

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ ОТ КИБЕРМОШЕННИКОВ



Самостоятельно звоните в свой банк по номеру телефона, указанному на оборотной стороне карты или на официальном сайте банка



Установите двухфакторный способ аутентификации — например, логин и пароль + подтверждающий код из СМС



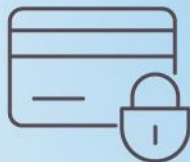
Пользуйтесь только официальными сайтами финансовых организаций, в поисковых системах (Яндекс, Mail.ru) они помечены цветным кружком с галочкой



Будьте бдительны: не действуйте впопых и проверяйте информацию! Расскажите об этих правилах поведения своим друзьям и знакомым

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ

1.



**ЗАБЛОКИРУЙТЕ
КАРТУ**



- ✓ в мобильном приложении банка
- ✓ по телефону горячей линии банка
- ✓ в отделении банка

СРАЗУ ЖЕ

2.



**СООБЩИТЕ
В БАНК**



- ✓ при личном обращении в отделение банка
- ✓ в мобильном приложении крупных банков

В ТЕЧЕНИЕ СУТОК

3.



**НАПИШИТЕ
ЗАЯВЛЕНИЕ
В ПОЛИЦИЮ**



- ✓ при личном обращении в ближайший отдел полиции

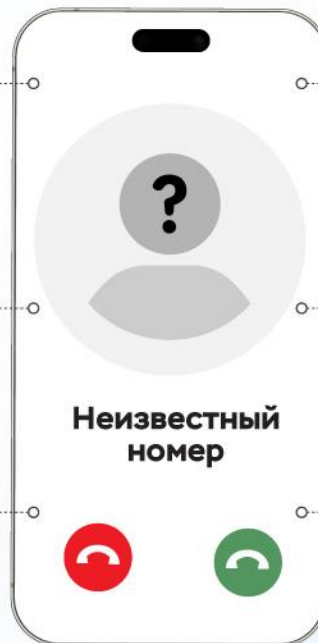
КАК МОЖНО СКОРЕЕ

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

Не отвечайте на звонки с незнакомых номеров

Прервите разговор, если он касается финансовых вопросов

Не торопитесь принимать решение



Самостоятельно позвоните близкому человеку / в банк / в организацию

Проверьте информацию в Интернете или обратитесь за помощью к близким

Не перезванивайте по незнакомым номерам



Возьмите паузу и спросите совета у родных и друзей!

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСКИМ ТЕЛЕФОННЫМ ЗВОНКАМ И ИНТЕРНЕТ-РЕСУРСАМ



Банк России инициирует блокировку телефонных номеров и интернет-ресурсов, которые используют злоумышленники для обмана людей*



* Сайты, страницы в соцсетях, приложения, телефонные номера

БАЗА ДАННЫХ О МОШЕННИЧЕСКИХ ОПЕРАЦИЯХ



Банк России ведет базу данных «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента»



База содержит большое количество параметров — уникальных идентификаторов, в том числе данных о плательщиках и получателях похищенных денег



Обновляется ежедневно после получения от банков информации о новых мошеннических переводах



Банки обязаны учитывать сведения из базы в своих системах безопасности и не допускать новых переводов на счета мошенников



База постоянно пополняется за счет сведений банков, которые обязаны передавать регулятору информацию обо всех случаях и попытках мошенничества

ДВЕНАДЦАТЬ ПРИЗНАКОВ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ

- 1 Реквизиты получателя денег есть в базе данных Банка России о мошеннических операциях
- 2 Нетипичная для клиента операция — например, по сумме перевода, периодичности, времени и месту совершения
- 3 Операция с устройства, которое ранее использовалось злоумышленниками и сведения о котором есть в базе данных регулятора
- 4 Сведения о получателе денег содержатся в собственной базе данных банка о подозрительных переводах
- 5 Есть информация о возбуждении уголовного дела по факту мошенничества в отношении получателя денег
- 6 Наличие информации от сторонних организаций (например, операторов связи), свидетельствующей о риске мошенничества (нехарактерная телефонная активность, рост числа входящих СМС-сообщений). Банки учитывают сведения о таких фактах, выявленных сторонними организациями как минимум за 6 часов до перевода



Приказ Банка России от 05.11.2025 № ОД-2506

ДВЕНАДЦАТЬ ПРИЗНАКОВ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ

- 7 Подозрительные события на устройстве клиента, которое используется для переводов (например, наличие ВПО*). Смена номера телефона в онлайн-банке или на Госуслугах за 48 часов до перевода
- 8 Внесение наличных в банкомате с помощью токенизированной (цифровой) карты на счет человека, который за последние 24 часа до этого совершил трансграничный перевод физическому лицу на сумму больше 100 тыс. рублей
- 9 Перевод денег человеку, с которым за последние полгода не было денежных взаимоотношений, при условии, что такой операции менее чем за 24 часа предшествовал перевод самому себе из другого банка через СБП на сумму более 200 тыс. рублей
- 10 Превышено время обмена данными, установленное НСПК, между картой, в том числе токенизированной, и банкоматом при бесконтактной операции в банкомате
- 11 Банк получил от НСПК информацию о риске мошенничества при совершении переводов
- 12 Сведения о получателе денег есть в ГИС «Антифрод»

* Вредоносное программное обеспечение

ЧТО ИЗМЕНИЛОСЬ С 25 ИЮЛЯ 2024 ГОДА*



**Двухдневный период
охлаждения
для переводов
по мошенническим
и подозрительным
реквизитам из базы
данных Банка России**



**Блокировка карты
и онлайн-банка
клиентов, которые
занимаются выводом
и обналичиванием
похищенных денег**



**Возмещение
похищенных денег
в течение 30 календарных
дней: если банк
не приостановил
мошеннический перевод
или не уведомил об этом
клиента, то он несет
за это финансовую
ответственность**

* Внесены изменения в Федеральный закон от 27.06.2011 № 161-ФЗ
«О национальной платежной системе»

БЛОКИРОВКА БАНКОВСКИХ КАРТ: ЧТО ВАЖНО ЗНАТЬ



При включении реквизитов в базу данных Банка России «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента» банк вправе заблокировать карту или онлайн-банкинг. Банк обязан заблокировать их при получении от правоохранительных органов информации о расследовании фактов мошенничества в отношении клиента



Блокировка действует до тех пор, пока сведения о клиенте находятся в базе данных регулятора. Человек или юридическое лицо могут обжаловать включение сведений двумя способами:

- 1 Обратиться с заявлением в любой из банков, клиентами которых они являются
- 2 Направить заявление в Банк России через интернет-приемную, выбрав в качестве темы обращения «Информационную безопасность» и указав соответствующий тип проблемы



Банк России рассмотрит заявление в течение 15 рабочих дней

АТАКИ НА ЛЮДЕЙ СТАНОВЯТСЯ ЦЕЛЕНАПРАВЛЕННЫМИ

1.



**Предварительное
изучение информации
о человеке, в том числе
в социальных сетях**

2.



**Использование
современных технологий,
в том числе дипфейков —
подделка голоса
и видеоизображения**

3.

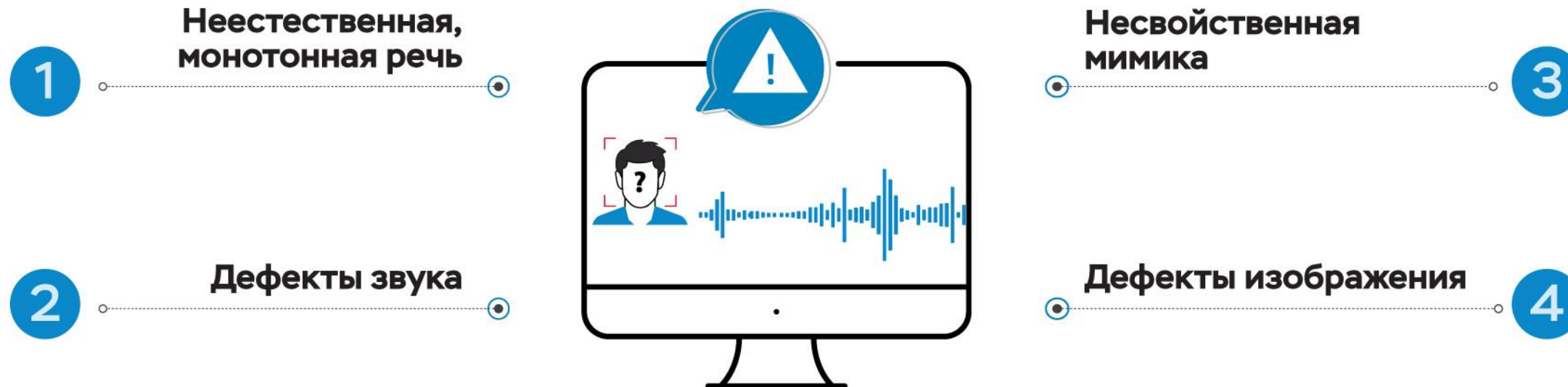


**Применение
персонифицированных
многоходовых схем
обмана**



- 1** Чтобы создать цифровую копию конкретного человека, злоумышленники **используют фото и видео, а также запись голоса**, полученные в основном в результате взлома его аккаунта в социальных сетях или мессенджерах
- 2** С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети
- 3** В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет

ПРИЗНАКИ ДИПФЕЙКА



Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи



Дроппер (дроп) — это помощник злоумышленников, который с использованием своих карт или онлайн-банка помогает мошенникам выводить и обналичивать похищенные у людей деньги



Студенты



Люди с большим количеством кредитов



Уязвимые слои населения



Иногородные рабочие



Чем занимаются дропперы:

- **Получают** на свои счета деньги и передают их другим лицам — наличными или переводом
- **Принимают** наличные деньги, вносят их на свои счета для последующего перевода
- **Предоставляют** злоумышленникам банковские карты или доступ к онлайн-банку

ГДЕ И КАК ИЩУТ ДРОППЕРОВ

Основной канал – Интернет (социальные сети, мессенджеры, электронная почта)

- Обещают высокий доход и удаленный режим работы
- Не требуют опыта работы и специальных навыков
- Единственное требование – наличие банковских карт или доступа к онлайн-банку

ЧТО ГРОЗИТ ДРОППЕРАМ

- Дропперы попадают в базу данных Банка России
- Банки ограничивают им доступ к онлайн-банку и картам
- Для дропперов такая работа заканчивается уголовным наказанием (ст. 187 УК РФ, до 6 лет лишения свободы)

ДРОППЕРЫ: МЕРЫ ПРОТИВОДЕЙСТВИЯ

1

Сейчас банки вправе блокировать дропперам карты и отключать доступ к онлайн-банку. А при получении сведений о них от правоохранительных органов это делается обязательно

2

Для клиентов, сведения о которых есть в базе данных Банка России, установлен лимит: 100 тыс. рублей в месяц на переводы (в том числе на собственные счета) с помощью карт или онлайн-банка и снятие наличных через банкоматы

3

Банки не выдают новые карты дропперам, информация о которых есть в базе данных Банка России

РЕЗУЛЬТАТЫ:

100%

блокировка карт и онлайн-банкинга при наличии сведений о мошенничестве от МВД России

в 40 раз

снижение транзакционной активности при попадании сведений в базу данных Банка России о мошеннических операциях

от 70 тыс. рублей

СТОИМОСТЬ «дроп-комплекта». **Рост издержек мошенников**

СЕРВИС ОПЕРАТИВНОГО УВЕДОМЛЕНИЯ О МОШЕННИЧЕСТВЕ



Функционал в мобильных приложениях крупных банков* для пострадавших

Он позволяет клиентам банков:

- ✓ подать заявление в банк о мошеннической операции
- ✓ сформировать справку о мошеннической операции для обращения в полицию
- ✓ ответить на вопрос банка, была ли операция, по которой поступил запрос Банка России, мошеннической

Доля пострадавших, которые обращались по факту хищения сразу и в банк, и в полицию, в 2025 году выросла почти до 40% (по результатам опроса Банка России)

* Системно значимые кредитные организации и кредитные организации, значимые на рынке платежных услуг

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ ПРИ СНЯТИИ НАЛИЧНЫХ ЧЕРЕЗ БАНКОМАТЫ



**Банки, выпустившие
платежную карту, обязаны
перед выдачей наличных
через банкоматы
проводить проверку
на признаки совершения
мошеннической
операции**



**Если банк выявляет хотя бы
один признак, вводится
на 48 часов лимит
на выдачу наличных
через банкоматы:
не более 50 тыс. рублей
в сутки с момента
направления запроса
на выдачу***



**К концу 2025 года хищения при снятии наличных через банкоматы сократились
на 40% по сравнению с пиковыми значениями в июне – июле 2025 года**

ПРИЗНАКИ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ ПРИ СНЯТИИ НАЛИЧНЫХ В БАНКОМАТАХ

1

Нехарактерное поведение клиента при снятии наличных через банкомат

Например, непривычные время суток или местонахождение банкомата, нетипичные сумма или количество операций

2

Превышение времени направления ответа карты на запрос банкомата

3

Нехарактерный способ снятия наличных

Например, вместо пластиковой карты используется QR-код

4

Направление запроса на выдачу наличных в течение 24 часов с момента:

- предоставления кредита/займа, увеличения лимита на выдачу наличных или лимита по кредитной карте
- досрочного расторжения договора банковского вклада на сумму более 200 тыс. рублей
- перевода на свой счет по СБП со своего счета в другом банке более 200 тыс. рублей

5

Информация об уровне риска осуществления мошеннической операции, полученная от НСПК

ПРИЗНАКИ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ ПРИ СНЯТИИ НАЛИЧНЫХ В БАНКОМАТАХ

6

Нетипичная телефонная активность за 6 часов до направления запроса на снятие наличных (в том числе в мессенджерах)

7

Информация о 5 отказах и более в выдаче наличных в течение календарного дня
Например, в связи с ошибками при вводе ПИН-кода, превышением лимита кредитования и т. д.

8

Информация о нетипичных параметрах и характеристиках устройства клиента
Например, наличие ВПО, нетипичный провайдер связи, активный VPN-сервис, смена номера в личном кабинете, нетипичная операционная система и т. д.

9

Наличие сведений о клиенте или его электронных средствах платежа в ГИС «Антифрод»

САМОЗАПРЕТ НА КРЕДИТЫ И ЗАЙМЫ



Гражданин может бесплатно и неограниченное количество раз устанавливать и снимать в своей кредитной истории запрет на заключение договоров кредита или займа



Установить можно через



Запрет не распространяется:

- 1 На ипотеку**
(обеспечена залогом недвижимого имущества)
- 2 На автокредиты**
(обеспечены залогом транспортного средства)
- 3 На основные образовательные кредиты**
(на оплату обучения, которая сразу перечисляется в образовательную организацию)

Узнать больше
о самозапрете



ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ*

- 1** Банки и МФО обязаны проводить антифрод-мероприятия перед выдачей потребительских кредитов и займов
- 2** Если банк или МФО нарушат антимошеннические нормы и будет возбуждено уголовное дело по факту хищения заемных денег, то заемщик освобождается от исполнения обязательств до вступления в силу приговора суда по уголовному делу
- 3** Период охлаждения для потребительских кредитов и займов:



4 часа

для сумм от **50** тыс. до **200** тыс. рублей



48 часов

для сумм свыше **200** тыс. рублей

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ*

Период охлаждения не применяется в случаях оформления:

- 1 кредитов и займов до 50 тыс. рублей
- 2 ипотечных и образовательных кредитов, автокредитов (при зачислении денег продавцу автомобиля – юридическому лицу)
- 3 кредитов, по которым заемщик не позднее чем за 2 дня до заключения договора назначил уполномоченное (доверенное) лицо для подтверждения заключения договора
- 4 покупки товаров (услуг) в кредит при личном присутствии потребителя в магазине (организации)
- 5 кредитов на рефинансирование ранее взятых обязательств, если это не приведет к увеличению их размера
- 6 кредитов, обязательства по которым принимают несколько созаемщиков или по которым у заемщика есть поручители

* Федеральный закон от 13.02.2025 № 9-ФЗ

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ*



МФО при дистанционном оформлении займа зачисляют деньги на счет, только если сведения о заемщике и получателе денег совпадают



Банки не перечисляют заемные деньги на счет человека, сведения о котором содержатся в базе данных Банка России о мошеннических операциях, если заемщик указал его реквизиты в качестве третьего лица для получения денег



МФО отказывают в выдаче займа, если сведения о заемщике содержатся в базе данных Банка России о мошеннических операциях



Будет ускорен обмен информацией между БКИ и кредиторами: БКИ будут обязаны принимать информацию, направляемую банками и МФО, и передавать ее им в онлайн-режиме (с 01.07.2026)

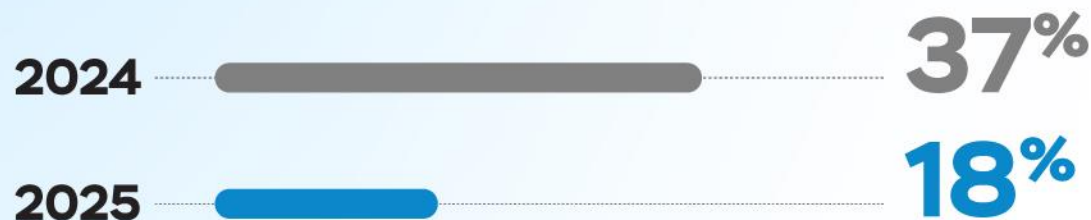


Банки и МФО будут обязаны получать информацию из БКИ, фиксировать факт ее получения, хранить и учитывать ее в своих антифрод-процедурах (с 31.12.2026)

ПРОТИВОДЕЙСТВИЕ КРЕДИТНОМУ МОШЕННИЧЕСТВУ: РЕЗУЛЬТАТЫ



Объем кредитных средств, похищенных у граждан, в сравнении с общим объемом мошеннических операций



на **39,2%** снизилась общая сумма потребительских кредитов и займов, оформленных гражданами в крупных банках под воздействием мошенников

Общая сумма потребительских кредитов и займов, оформленных под воздействием мошенников

2,7
млрд
рублей

1,8
млрд
рублей

1,8
млрд
рублей

1,5
млрд
рублей

2025

I квартал

II квартал

III квартал

IV квартал