Банк России

КИБЕРМОШЕННИЧЕСТВО: ПРОТИВОДЕЙСТВИЕ НОВЫМ УГРОЗАМ

Центральный банк Российской Федерации
2025

ОГЛАВЛЕНИЕ

ТЕКУЩЕЕ СОСТОЯНИЕ

За последние несколько лет приемы и методы кибермошенников существенно изменились: «холодные звонки» якобы сотрудников банков становятся редкостью. **Атаки злоумышленников направлены на конкретного человека**, в отношении которого они используют индивидуальную схему обмана и психологические приемы. В большинстве случаев людям сложно распознать обман. **Многие пострадавшие** либо **самостоятельно отдают деньги кибермошенникам**, либо **сообщают им личные и финансовые данные**, что приводит к потере сбережений.

С каждого перевода в размере 1 миллиона рублей 6,6 рубля досталось мошенникам

Потери граждан от кибермошенников в 2024 году

Объем кредитного мошенничества вырос: в крупных банках **размер похищенных кредитных денег составил 37%** в сравнении с общим объемом хищений (25% в 2023 году).

Злоумышленники регулярно придумывают новые схемы обмана, исходя из актуальных событий.

Как мошенники подстраивались под новостную повестку

Борьба с кибермошенничеством — одна из приоритетных задач Банка России

72,17 млн
мошеннических операций

13,5 трлн руб.
объем спасенных денег

банки предотвратили

Регулятор совместно с кредитными организациями противодействует мошенническим операциям. Сейчас подавляющее большинство попыток злоумышленников похитить деньги у граждан отражается защитными системами банков.

В 2024 году эффективность антифрод-систем крупных банков составила 99,7%

БАЗА ДАННЫХ О МОШЕННИЧЕСКИХ ОПЕРАЦИЯХ

Банк России ведет список подозрительных реквизитов – базу данных «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента».

База постоянно пополняется за счет сведений банков, которые обязаны передавать регулятору информацию обо всех случаях и попытках мошенничества против клиентов. Она содержит большое количество параметров – уникальных идентификаторов, в том числе данные о плательщиках и получателях похищенных денег.

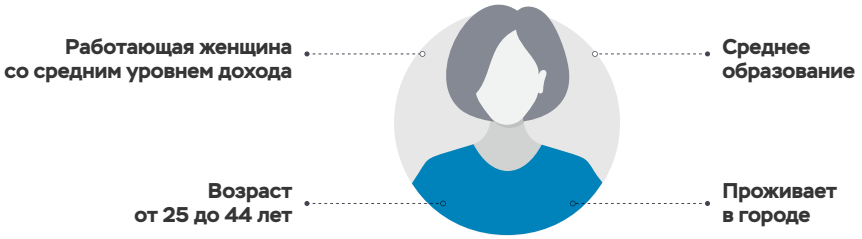
Банк России обновляет базу данных ежедневно после получения от банков информации о новых мошеннических операциях, затем направляет сведения во все кредитные организации. Они обязаны учитывать их в своих системах и блокировать новые переводы на счета злоумышленников.

ПОРТРЕТ ПОСТРАДАВШЕГО

В 2024 году с разными видами кибермошенничества сталкивались 34% граждан, принявших участие в опросе* Банка России. 9% из тех, кто контактировал со злоумышленниками, лишились денег.

Стать жертвой кибермошенников может любой человек независимо от уровня образования и социального статуса.

На основе данных опроса Банк России составил портрет среднестатистической жертвы кибермошенников.

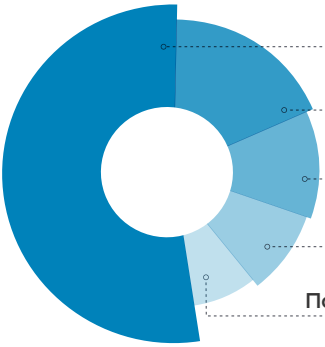


Телефонное и СМС-мошенничество до сих пор преобладает, но за 2024 год доля этого вида обмана сократилась (на 8,4 п.п.). Впервые в пятерке популярных у кибермошенников приемов – получение доступа к аккаунтам людей на Госуслугах.

---

* В опросе, проведенном в ноябре 2024 года, приняли участие 429 063 человека.

Как мошенники пытались получить доступ к деньгам



Телефонный звонок или СМС-сообщение **45,6%**

Атака через мессенджеры **15,7%**

Сообщения в социальных сетях **10,3%**

Письма на электронную почту **7,7%**

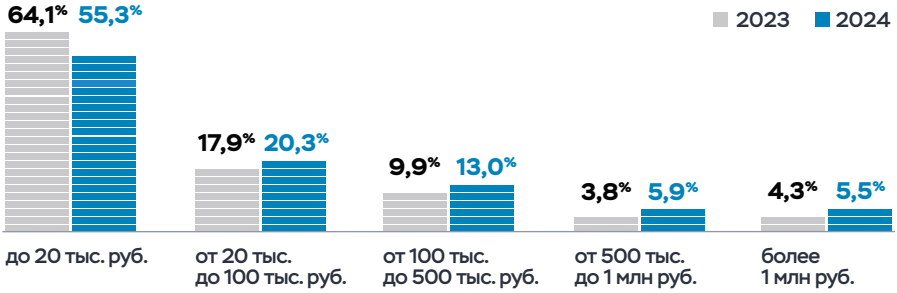
Получение доступа к аккаунту на Госуслугах **7,0%**

На остальные виды мошенничества (фишинговые ресурсы, поддельные QR-коды и прочие) пришлось 13,7%.

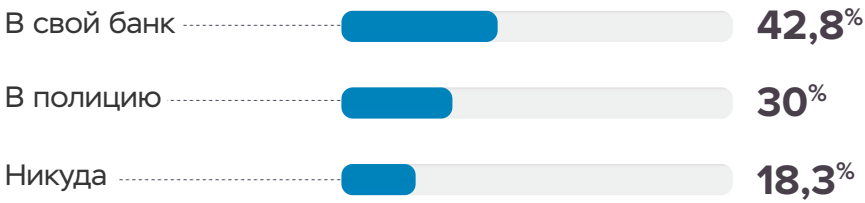
Какие действия совершали пострадавшие под влиянием мошенников

Переходили по ссылке, которую присылают злоумышленники	18,9%
Переводили деньги злоумышленникам	15,6%
Сообщали коды из СМС-сообщений от Госуслуг	11,2%
Сообщали коды из СМС-сообщений или пуш-уведомлений от банка	10,8%
Вводили данные банковской карты на сайте	7,6%
Устанавливали вредоносное приложение	6,7%
Сообщали паспортные данные	6,6%
Вводили личные данные на сайте (данные паспорта, СНИЛС и прочие)	6,2%
Сообщали данные банковской карты	5%
Набирали комбинацию цифр на телефоне	3,8%

Сколько денег потеряли люди



Куда обратились пострадавшие



Остальные пострадавшие обращались в иные организации (в Роспотребнадзор, Банк России, к финансовому уполномоченному).

ИНСТРУМЕНТЫ ЗАЩИТЫ

ЗАКОНОДАТЕЛЬНЫЕ

Период охлаждения для переводов

С 25 июля 2024 года банки обязаны приостанавливать на два дня переводы, если счет получателя есть в базе данных регулятора о мошеннических счетах, и оповещать об этом клиента. Банк обязан возместить клиенту деньги, если нарушил эти требования закона. **Крупные банки ежемесячно охлаждают около 300 тыс. мошеннических переводов**.

Онлайн-обмен данными с правоохранительными органами

В 2024 году **Банк России предоставил правоохранительным органам информацию более чем по 155 тыс. запросов в отношении мошеннических переводов**.
С октября 2023 года действует автоматизированный обмен сведениями об операциях злоумышленников между Банком России и МВД России. После обращения пострадавшего сотрудники полиции могут в течение минуты узнать информацию о получателе похищенных денег из базы данных регулятора.

Самозапрет на кредиты и займы

С 1 марта 2025 года **гражданин может добровольно** и неограниченное количество раз через Госуслуги **устанавливать и снимать** в своей кредитной истории **запрет на заключение договоров кредита или займа**. Эта услуга будет доступна и в многофункциональных центрах (МФЦ) не позднее 1 сентября 2025 года.

Признаки мошеннических операций

В июле 2024 года **Банк России вдвое расширил перечень признаков мошеннических операций**, которыми руководствуются банки для предотвращения таких переводов, — теперь их шесть:

1. Реквизиты получателя денег есть в базе данных Банка России
2. Нетипичная для клиента операция — например, по сумме перевода, периодичности, времени и месту совершения
3. Операция с устройства, ранее использовавшегося мошенниками, и сведения о нем есть в базе данных Банка России
4. Сведения о получателе денег содержатся в собственной базе данных банка о подозрительных переводах
5. Информация о возбуждении уголовного дела по факту мошенничества в отношении получателя денег
6. Данные сторонних организаций о возможном обмане — например, телефонная активность или рост числа входящих СМС-сообщений с новых номеров

Если перевод соответствует хотя бы одному из этих признаков, банк должен приостановить операцию и предупредить клиента о риске обмана.

Блокировка доступа к онлайн-банкингу и картам

В июле 2024 года Банк России также обязал кредитные организации блокировать доступ к онлайн-банкингу и платежным картам дропперам — людям, которые занимаются выводом и обналичиванием похищенных денег. Сведения о них поступают в базу данных регулятора как от самих банков, так и от МВД России. **Только в первый день действия закона банки заблокировали доступ примерно к 30 тыс. платежных средств.**

Благодаря этой мере возможности мошенников вывести средства снижаются, а их издержки растут

Банки стали быстрее реагировать на мошенников

Банк России в 2024 году обязал банки вносить в свои системы безопасности реквизиты злоумышленников практически сразу после их попадания в базу регулятора о подозрительных счетах: **теперь крупные банки должны делать это в течение часа, остальные — в течение трех часов**.

Противодействие мошенническим телефонным звонкам и интернет-ресурсам

В 2024 году Банк России инициировал блокировку

172 тыс. номеров злоумышленников

46 тыс. мошеннических сайтов и страниц в социальных сетях

ПРОФИЛАКТИЧЕСКИЕ

Одна из ключевых задач Банка России — повышение киберграмотности людей. Важно, чтобы граждане умели распознавать финансовое мошенничество и противостоять злоумышленникам.

Федеральная кампания Клади трубку

Банк России в партнерстве с МВД России и Генеральной прокуратурой провел федеральную информационную кампанию по борьбе с кибермошенничеством «Клади трубку». Распространено свыше 690 тыс. печатных материалов более чем на 10,8 тыс. точек.

Социальная реклама

В 2024 году **социальный ролик Банка России о рисках телефонного мошенничества транслировался по всем федеральным телеканалам** (более 84 млн просмотров), а также на рекламных конструкциях по всей стране. Вторая серия вышла в эфир федеральных телеканалов в январе 2025 года.

Онлайн-проекты

- Раздел сайта Банка России с информацией о распространенных уловках мошенников и способах защиты от них
- Телеграм-бот, который учит распознавать мошеннические (дропперские) вакансии и избегать вовлечения в преступные схемы
- Социальные сети Банка России: видеокомментарии с советами, диалоги с пользователями по вопросам киберзащиты
- Видеоконтент для популярных онлайн-кинотеатров
- Дистанционный курс по финансовой киберграмотности

ВЫЗОВЫ

Злоумышленники мигрируют в мессенджеры

Банк России и кредитные организации инициируют блокировку операторами связи телефонных номеров злоумышленников. Помимо этого, Правительство РФ запретило звонки через Интернет на мобильные и стационарные телефоны. Однако **растет активность кибермошенников в мессенджерах и социальных сетях**, где противостоять им сейчас сложно.

Рост дипфейков

Кибермошенники чаще используют технологии для создания дипфейков (подделка голоса, видеоизображения), особенно против доверчивых людей. Доступных для широкой аудитории инструментов защиты от этой угрозы пока нет.

Уязвимость подрядчиков финансовых организаций

В 2024 году Банк России выявил 17 атак злоумышленников на организации, предоставляющие ИТ-услуги более чем для 70 компаний финансового рынка, включая системно значимые кредитные организации. **Наблюдается рост атак на подрядчиков финансовых организаций для получения персональных и финансовых данных клиентов**. В отличие от банков, к их партнерам не применяются требования по обеспечению информационной безопасности.

КЛЮЧЕВЫЕ ЗАДАЧИ И СПОСОБЫ РЕШЕНИЯ

Борьба с мошенническими кредитами и займами

1 сентября 2025 года

Устанавливается период охлаждения для кредитов и займов

- От 50 тыс. до 200 тыс. рублей – 4 часа
- Свыше 200 тыс. рублей – 48 часов

---

1 сентября 2025 года

МФО дополнительно проверят заемщиков

Микрофинансовые организации будут зачислять деньги на счет, только если сведения о заемщике и получателе денег совпадают. Если информация о человеке есть в базе данных Банка России, то МФО откажут ему в выдаче займа

---

31 декабря 2026 года

Ускорится обмен информацией между кредиторами и бюро кредитных историй практически до онлайн-режима

Это поможет избежать случаев, когда человек под влиянием мошенников в короткий срок оформляет сразу несколько кредитов и займов в разных банках и МФО

Борьба с дропперами

Утверждены новые меры противодействия тем, кто помогает выводить похищенные деньги

29 марта 2025 года	**Родители проконтролируют операции детей** **Банки должны уведомлять родителей** или законных представителей **несовершеннолетних** клиентов в возрасте от 14 до 18 лет **о выдаче им карты, а также обо всех операциях по счету ребенка**. Информирование и его способ прописываются в договоре с банком
15 мая 2025 года	**Начнет действовать лимит на переводы** **Злоумышленники**, сведения о которых попали в базу данных Банка России, **не смогут переводить себе и другим людям** больше 100 тыс. рублей в месяц
1 сентября 2025 года	**Запрет на выдачу новых карт** **Банки не будут выдавать карты дропперам**, информация о которых находится в базе данных Банка России
1 октября 2025 года	**Спецкнопка в мобильных приложениях крупных банков для пострадавших** **Она позволит клиентам оперативно заявить о мошенническом переводе**, а также получить электронную справку о нем для обращения в полицию. В приложении человек также сможет ответить на вопрос банка, была ли операция мошеннической, если такой запрос поступил в Банк России из МВД России. Такой порядок взаимодействия возможен в случаях, когда пострадавший напрямую обращается в полицию, которая запрашивает данные у регулятора

ОБЩИЕ ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ

Не сообщайте никому и никогда личные и финансовые данные, в том числе данные банковской карты, коды из СМС или пуш-уведомлений

Используйте антивирусные программы на своих устройствах и **регулярно обновляйте** средства защиты

Не совершайте какие-либо действия по счету по просьбе незнакомых лиц

Будьте осторожны с электронными письмами и СМС-сообщениями: **не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы** или программы

Для покупок в Интернете **заведите отдельную банковскую карту**

ЕСЛИ СТАЛИ ЖЕРТВОЙ ФИНАНСОВОГО МОШЕННИЧЕСТВА

1

Немедленно заблокируйте карту в мобильном приложении, отделении банка или контакт-центре

2

В течение суток подайте заявление в банк о несогласии с операцией

3

Как можно скорее **обратитесь с заявлением в ближайшее отделение полиции**

ДЛЯ ЗАМЕТОК

Распространенные схемы
мошенничества и способы защиты от них

Обзор операций, совершенных
без добровольного согласия клиентов
финансовых организаций в 2024 году

Не наступайте на грабли:
истории о мошенничестве