ИНФОРМАЦИЯ

о возможности установления гражданином запрета (ограничения) на онлайн-операции, в том числе на заключение кредитными организациями с ним договоров потребительского займа (кредита), в целях предупреждения мошеннических действий со стороны третьих лиц

Пунктом 7.1. Положения «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», разработанного Центральным банком Российской Федерации от 17 апреля 2019 г. № 683-П определено: *«В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) договора об использовании электронного средства платежа, на основании их заявлений устанавливают в отношении операций, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций через информационно-телекоммуникационную сеть «Интернет», ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе видов операций».*

Центробанк обязал банки с 1 октября 2022 года предоставить клиентам возможность собственноручно накладывать запрет на онлайн-операции и ограничивать их параметры (как при кредитовании, так и при денежных переводах).

Самозапрет на кредиты, что это?

Это ограничение, которое банк по заявлению клиента накладывает на операции, осуществляемые с помощью удаленного доступа через интернет. Запретить можно как отдельно кредитование, так и другие банковские операции или установить максимальную сумму.

Принят федеральный закон[1], по которому граждане могут устанавливать самозапрет на выдачу кредитов, который начнет действовать с 1 марта 2025 года. Можно будет устанавливать запрет на заключение договоров потребительского займа с банками и микрофинансовыми организациями (МФО). Гражданам дадут право подать во все квалифицированные бюро кредитных историй заявление через единый портал госуслуг, а также запросить информацию о наличии в кредитной истории сведений о таком ограничении. К заявлению нужно будет прикрепить данные СНИЛСа.

Снять запрет можно будет в любое время, но взять кредит получится только после того, как данные попадут в кредитную историю. Депутаты считают, что такой «период охлаждения» позволит исключить риск мошенничества с одномоментным снятием запрета и заключением кредитного договора.

В каких случаях стоит оформить самозапрет на кредит?

Категорий людей, которым рекомендуют оформить такой самозапрет, нет. В настоящее время юристы рекомендуют делать это лично, в присутствии сотрудника банка и самого клиента, с обычной подписью (целесообразно написать заявления о запрете во все крупные банки, а как минимум в те, где вы когда-либо обслуживались по дебетовой карте, кредитной карте, кредиту.

Как оформить самозапрет на кредиты через «Госуслуги»?

С 1 марта 2025 года самозапрет на кредиты можно будет выставить на «Госуслугах», с 1 сентября 2025 года – в МФЦ. Эти данные автоматически попадут в бюро кредитных историй. Банки, которые запрашивают информацию в бюро, увидят выставленные ограничения на кредитование. Пока эта опция недоступна.

Можно ли оформить самозапрет через банки, микрофинансовые и другие организации?

Пока это единственный вариант и он уже вступил в силу и действует с октября 2022 года.

[1] Федеральный закон от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)» (вступает в силу 01.03.2025)

В отдельных банках можно написать заявление о запрете онлайн-кредитования конкретно в них. Такая опция есть практически во всех крупных банках, но есть те, которые будут против (к ним необходимо относится скептически, т.к. они не соответствует рекомендациям Центробанка что повышает риски заемщика).

Условия и порядок оформления такого запрета сегодня устанавливает банк.

Аналогичные запреты можно направить и в микрофинансовые организации, но технически сделать это будет сложнее т.к. их слишком много, зарегистрированы они в разных регионах, а о существовании некоторых можно просто не знать.

Можно ли снять самозапрет?

Да. Можно запретить выдавать кредиты на свое имя, потом отозвать запрет, потом запретить снова. Центробанк никак не ограничивает количество таких процедур.

Плюсы и минусы самозапрета на кредиты.

Плюс очевиден – самозапрет на кредиты поможет защититься от мошенников. А возможно, и от спонтанных покупок – кредиты выдаются онлайн за несколько минут. Но если придется ехать в банк, чтобы снимать самозапрет, велик шанс передумать.

Минус только в том, что если вы сами соберетесь взять кредит, то придется потратить время и сходить в отделение банка. Большой проблемы в этом нет, особенно если вы живете в городе, где есть отделение банка. Но если вы проживаете в маленьком городке, где отделений нет и не хочется никуда ехать, то это проблематично.

В принципе, онлайн-кредит – это удобно, но система будет хороша только тогда, когда каждый гражданин будет обладать своей квалифицированной электронной цифровой подписью. Не простой, а именно квалифицированной, как, например, у судей.

Обезопасит ли самозапрет полностью от мошенников?

Полностью – нет, однако он существенно усложнит мошенникам задачу и как минимум защитит от некоторых схем и от потери крупных сумм.

Как обезопасить себя, пока закон не начал действовать?

Если вы хотите оформить именно самозапрет на кредитование или переводы, это можно сделать непосредственно в банке. Конечно, потребуется время, чтобы обратиться во все кредитные организации, но для начала можно подать заявления в банки, услугами которых вы когда-либо пользовались.

Сейчас у некоторых банков есть специальная последовательность действий для онлайн-кредитования, чтобы избежать мошенничества. Например, счет заемщика могут заблокировать, если он пытается сразу же после получения кредита снять или перевести деньги. Для разблокировки счета придется связаться с банком или посетить отделение лично.

Рекомендации:

Юристы советуют раз в год или полгода запрашивать отчет из бюро кредитных историй. Это уже сейчас можно сделать на «Госуслугах» - через сайт заказать выписку из всех БКИ, в которых содержится информация о клиенте.

Также можно периодически проверять себя через систему судебных приставов на сайте ФССП. Достаточно указать ФИО, дату рождения и выбрать регион, по которому будет производиться проверка.

Не пересылайте никогда фотографии паспорта – в некоторых случаях займ могут оформить по фото или копии документа. Если куда-то нужно отправить данные, лучше не полениться и переписать их. Если вам стало известно, что эти данные уже куда-то попали целесообразно менять паспорт. При этом, если паспорт украли или вы его потеряли, следует обратиться в полицию.

Возьмите там справку о том, что паспорт утерян, с указанием даты. Если паспорт попадет в руки мошенников, эта справка будет основным доказательством того, что кредит или займ брали не вы.

Иногда мошенникам достаточно только паспортных данных, поэтому их тоже стоит беречь. Не сообщайте данные по телефону или в соцсетях, не вводите данные на непроверенных и незащищенных сайтах (в адресной строке должно быть изображение закрытого замка). В случае звонка «из банка» не разговаривайте со звонящими – общайтесь в чате поддержки на официальном сайте или в приложении либо перезвоните в банк самостоятельно

Как не поддаться на уловки кибермошенников

Кибермошенничество - один из видов преступлений в Интернете, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Злоумышленники для достижения целей воздействуют на эмоции, страхи и рефлексы людей и побуждают перейти по вредоносной ссылке.
При переходе по ссылке человек попадает на фишинговый сайт, где его просят ввести персональные или банковские данные.
Очень часто в сообщениях содержатся ссылки на вредоносное ПО.

Наиболее распространенные схемы онлайн-мошенничества

ВАША УЧЕТНАЯ ЗАПИСЬ БЫЛА ИЛИ БУДЕТ ЗАБЛОКИРОВАНА / ОТКЛЮЧЕНА

Перед угрозой блокировки аккаунта пользователь теряет бдительность, переходит по ссылке в письме и вводит свои логин и пароль.

В ВАШЕЙ УЧЕТНОЙ ЗАПИСИ ОБНАРУЖЕНЫ ПОДОЗРИТЕЛЬНЫЕ ИЛИ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ. ТРЕБУЕТСЯ ОБНОВЛЕНИЕ НАСТРОЕК БЕЗОПАСНОСТИ

В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Пользователь паникует и забывает о бдительности.

Наиболее распространенные схемы онлайн-мошенничества:

ВАШ ДРУГ ОСТАВИЛ ВАМ СООБЩЕНИЕ. ПЕРЕЙДИТЕ ПО ССЫЛКЕ, ЧТОБЫ ПРОЧИТАТЬ

В подобных письмах злоумышленники скрываются за маской людей/организаций, которые входят в ваш доверенный круг, чьи письма и сообщения не должны у вас вызвать подозрений. Люди склонны идти навстречу тем, кому доверяют: переходят по ссылке в письме и вводят свои личные данные.

ПИСЬМА ОТ ГОСУДАРСТВЕННЫХ СЛУЖБ

Фишинговые письма приходят от имени различных госорганов с информацией о претензиях, которые возникли к пользователю со стороны государства. Чаще всего в письмах фигурируют МВД, ФНС и ФМС, а также организации системы здравоохранения.

Наиболее распространенные схемы онлайн-мошенничества

СОЦИАЛЬНАЯ ПОДДЕРЖКА

Благотворительность и меценатство — любимые темы злоумышленников. Чем эмоциональнее обращение к вам, тем больше оснований подозревать мошенничество.
Популярные темы писем: благотворительность после стихийных бедствий, человек в беде, сборы на лечение.

ВЫ ВЫИГРАЛИ

Сообщение о выигрыше и ссылкой на сайт, где якобы можно получить приз.

Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Используйте только лицензионное ПО, регулярно его обновляйте и включайте антивирусную защиту на всех устройствах.

- Важные файлы храните не только на жестком диске компьютера, но и на внешних жестких дисках или в облачном хранилище.

- Используйте двухфакторную аутентификацию, например, для защиты электронной почты. Обязательны сложные пароли из незначащих комбинаций букв, цифр и знаков, не менее 8 символов. Не используйте один и тот же пароль для разных систем. Меняйте пароли хотя бы раз в полгода.

Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Проверяйте вложения, полученные по электронной почте, с помощью антивирусного ПО. С осторожностью относитесь к сайтам с некорректными сертификатами. Будьте внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами.

- Не переходите по ссылкам на незнакомые ресурсы, особенно если браузер предупреждает о рисках. Игнорируйте ссылки из всплывающих окон, даже если компания или продукт вам знакомы. Не загружайте файлы с подозрительных веб-ресурсов.

- Заведите отдельную карту для оплаты товаров в Интернете и подключите оповещения по операциям на счете карты.