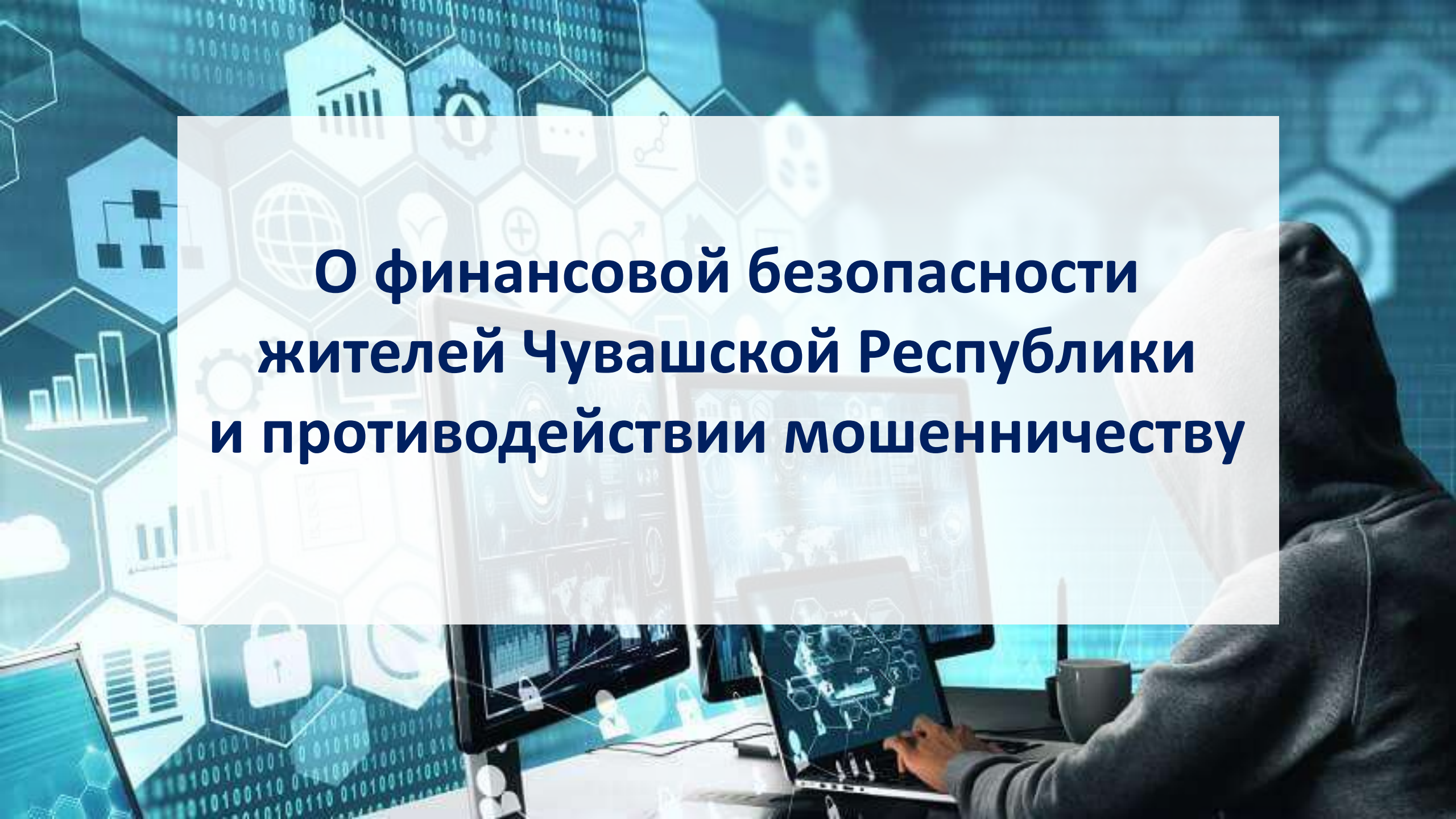


О финансовой безопасности жителей Чувашской Республики и противодействии мошенничеству

Угроза №1

Дистанционные хищения – самый актуальный тип мошенничества

более 90% от всех фактов хищения

2025 год:

30 млн попыток

телефонного мошенничества

в сутки

(2022 год - 5 млн попыток в сутки)

Угроза №1

в 2025 году

более 1 млрд рублей

жители Чувашии

отдали украинским мошенникам,

из них

около 600 млн рублей

ушло на вооружение ВСУ

и террористические удары

по России

Предлоги, с которыми мошенники обращаются к жертве

- ✓ **«Попытка хищения средств или имущества», «попытка получения кредита», «продление договора сотовой связи», «переоформление кредита (в т.ч. под залог недвижимости)» , «оформление сделки с объектом недвижимости»,** с дальнейшим переводом денег на «спец.счет», «безопасный счет» и иные счета, указанные преступниками

- ✓ **«Оказание помощи полиции (прокуратуре, следственному комитету и т.п.)», «участие в спецоперации по поимке злоумышленников в банке или на объекте преступления»** для «задержания работников банка или преступника с поличным»

- ✓ **«Расследование по факту финансирования ВСУ»** и компенсация отправленных сумм путем оформления кредитов или снятия со вкладов и направления денег на «безопасный счет»

- ✓ **«Родственник «попал в беду»,** когда надо «срочно направить или передать деньги для «решения вопроса», для «операции» или «для проверяющих из вышестоящей организации»

- ✓ **«Блокировка карты», «проблемы» с личным кабинетом на сайте Госуслуг, у оператора мобильной связи и т.п. ,** когда нужно подтвердить реквизиты (номера карт, пароли и коды, поступившие смс и т.п.)

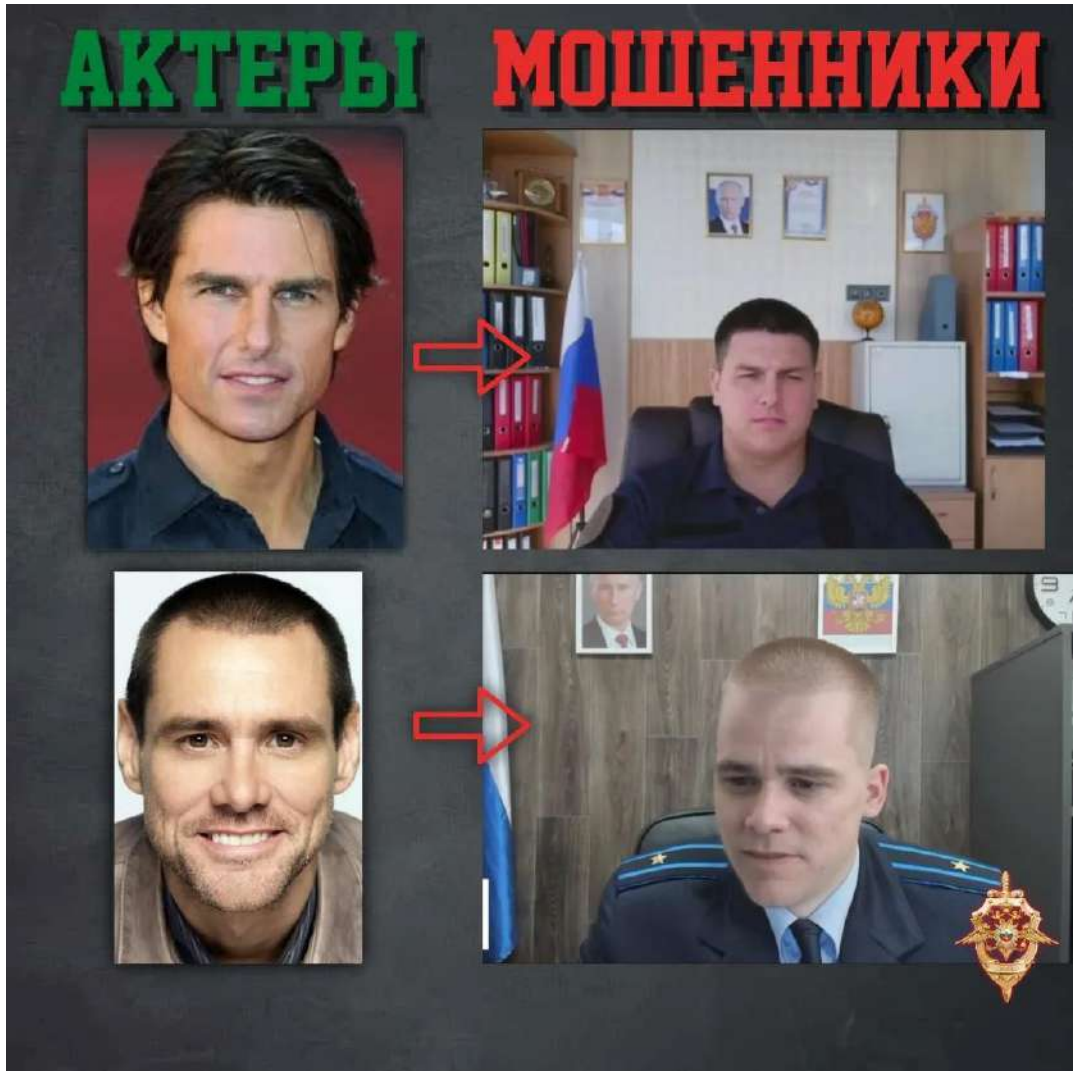
- ✓ **«Компенсации» («страховки», «социальные выплаты»),** «перерасчет пенсии, продление услуг связи, замена домофона или счетчика, доставка цветов или товаров, голосование в интернете» и т.п. (цель мошенников - получить код доступа из СМС к госуслугам, социальным сетям или банковским приложениям жертвы)

Технологии, которые используют мошенники

- ✓ **Оформление дубля СИМ-карты жертвы** (цель мошенников - получить коды доступа из СМС к госуслугам, социальным сетям или банковским приложениям жертвы)
- ✓ **Мошенничество в сети Интернет под видом выгодных инвестиций, в т.ч. с предложением «легкого заработка»**
- ✓ **Звонки или видеозвонки через мессенджер** (при таком звонке на аватарке виден логотип известного банка или эмблема МВД, ФСБ, Следственного комитета, Госуслуги, МФЦ или другие легко узнаваемые логотипы)
- ✓ **Звонки или сообщения от имени руководителя организации**
- ✓ **Использование нанятых курьеров для доставки фиктивных писем или повесток от «Госорганов», для получения денег от жертвы.**
- ✓ **Технология DeepFake или подмена изображения и голоса** (позволяет мошенникам создавать голосовые сообщения или видеозвонок от имени друзей и родственников, либо общаться с жертвой по видеосвязи в образе знакомого лица)
- ✓ **Мошенники могут присылать фото поддельных или нарисованных на компьютере документов и служебных удостоверений** (**настоящие сотрудники** правоохранительных органов, центробанка и других структур **так никогда не делают!**)

Примеры DeepFake – видеозвонков с изображением и голосом киноактеров

(психологический эффект знакомого лица)



Как они нас обманывают?

Принципиальная схема социальной инженерии

- **«Задавить авторитетом»** с использованием технологии подмены номера и специфической терминологии
- **Вывести жертву из душевного равновесия** (страх, эйфория)
- **Закрепить, подтвердить «достоверность» информации из «другого источника»,** в т.ч. с использованием фиктивных документов
- **Нагнетание «срочности»**
- **Запрет на общение с другими лицами, инструктаж о «легенде»**
- **Длительное удержание жертвы «на телефоне»**
- **Управление по телефону действиями жертвы**

Дополнения:

- Воздействие с отлагательным эффектом: **разделение звонков от «разных источников» по времени**
- **Побуждение к совершению теракта, хулиганских, иных противоправных действий**
- **Имитация «похищения» человека** (с хищением денег у жертвы) **и вымогательство денег** (у родственников)

Государство защищает

Какие меры введены

- ✓ Маркировка звонков
- ▪ Запрет на получение сообщений от Госуслуг во время разговора
- ✓ Самозапрет на получение кредитов и займов
- ▪ Запрет на действия с недвижимостью без личного участия
- ✓ Самозапрет на заключение новых договоров об оказании услуг связи (на приобретение сим-карт)
- ✓ Период охлаждения при обращении за кредитом или займом
- ▪ Ограничения при снятии наличных в банкоматах
- ✓ Сервис «второй руки»
- ▪ «Спецкнопка» для жалоб в банковском приложении
- ✓ Защита от мошенников в микрофинансовых организациях (МФО)

ЧТО ДЕЛАТЬ?

✓ НИЧЕГО НЕ ДЕЛАТЬ!

- ✓ НЕ сообщать кодов из СМС и вообще никаких сведений
- ✓ НЕ совершать никаких действий с деньгами и имуществом
- ✓ НЕ устанавливать никаких программ из неизвестных источников и не включать демонстрацию экрана на телефоне или ином гаджете
- ✓ НЕ переходить по интернет-ссылкам в сообщениях
- ✓ НЕ совершать противоправных действий

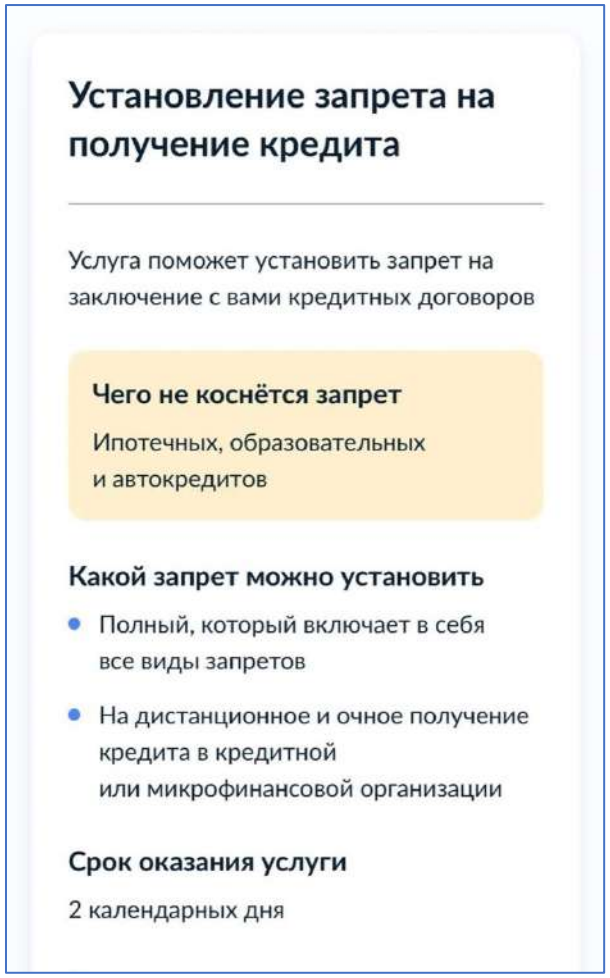
Если Вы все же успели назвать код из СМС, сообщить какие-то сведения о себе, своих счетах и т.п.:

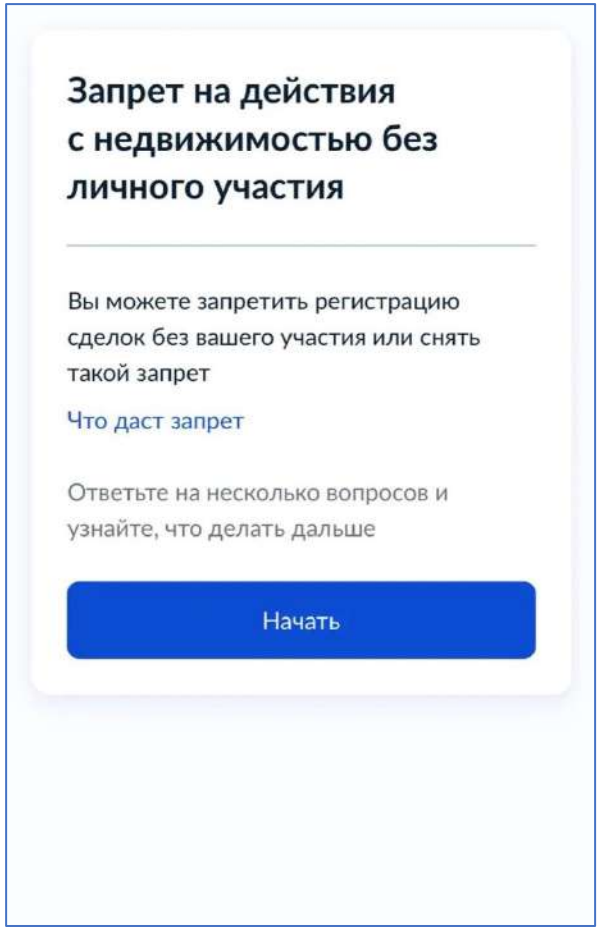
- **Немедленно прервите общение с мошенником**
- **Поменяйте пароль на Госуслугах**
- **Срочно сообщите в банк о случившемся и инициируйте блокировку своих карт (счетов) и прекращение каких-либо сделок от Вашего имени**
- **Сообщите о случившемся в полицию** (сохранив номер звонившего или текст переписки с мошенником)

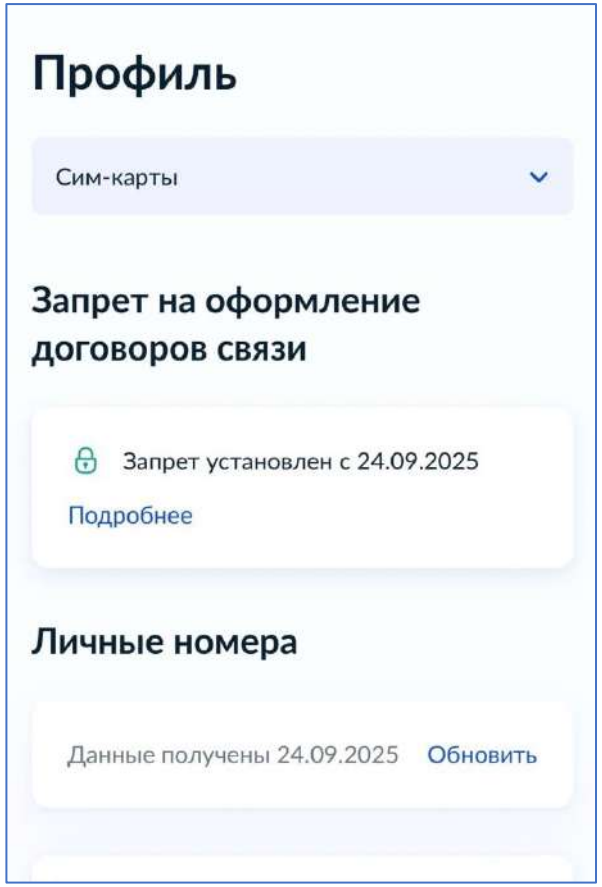
ЧТО ДЕЛАТЬ?

Установить САМОЗАПРЕТ:

- ✓ **На получение кредита**
- ✓ **На сделки с недвижимостью без личного участия**
- ✓ **На активацию сим-карты (договора связи)**







Больше полезной информации: