ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ

МВД по Республике Бурятия

БУДЬТЕ БДИТЕЛЬНЫ!!!

Мошенники могут представляться следующими личностями:

- *Сотрудниками правоохранительных органов (полиция, ФСБ, прокуратура, следственный комитет, и т.д.);*
- *Сотрудниками банков (Центробанка);*
- *Сотрудниками МФЦ;*
- *Сотрудниками социального и пенсионного фонда;*
- *Сотрудниками брокерских организаций;*
- *Сотрудниками операторов связи;*
- *Работниками коммунальных служб, Почты России;*
- *Сотрудниками Росфинмониторинга.*

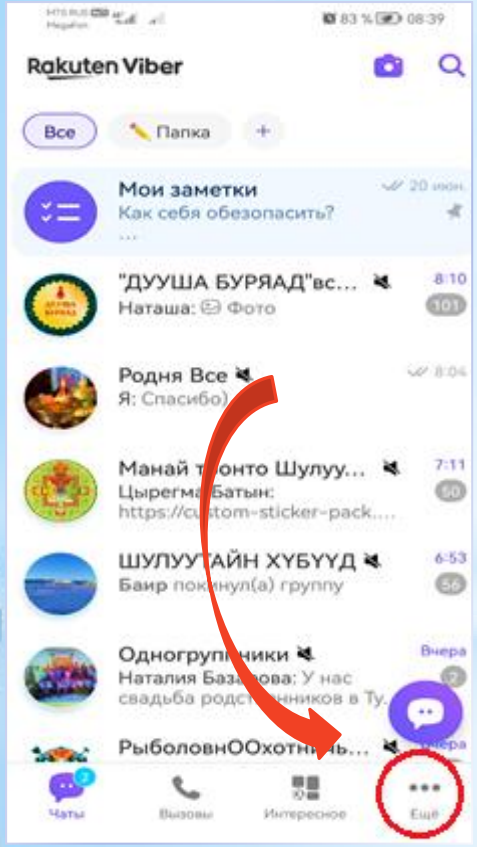
ВНИМАНИЕ!
МОШЕННИКИ!

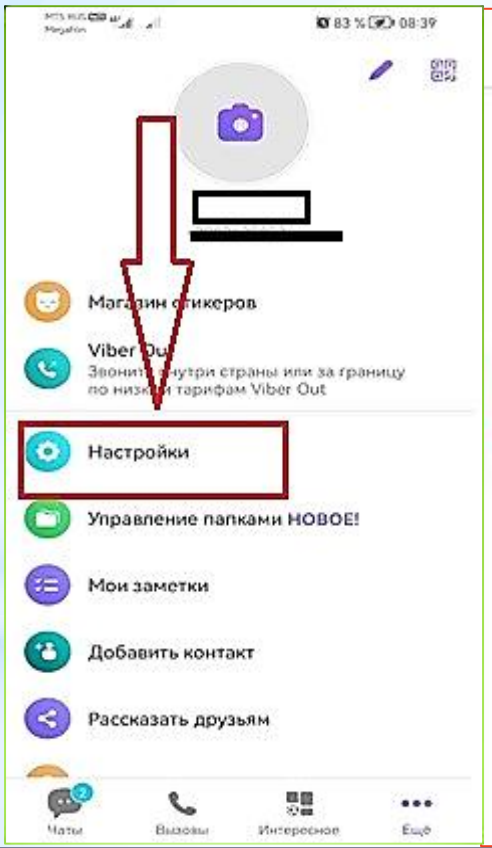
КЛЮЧЕВЫЕ ФРАЗЫ:

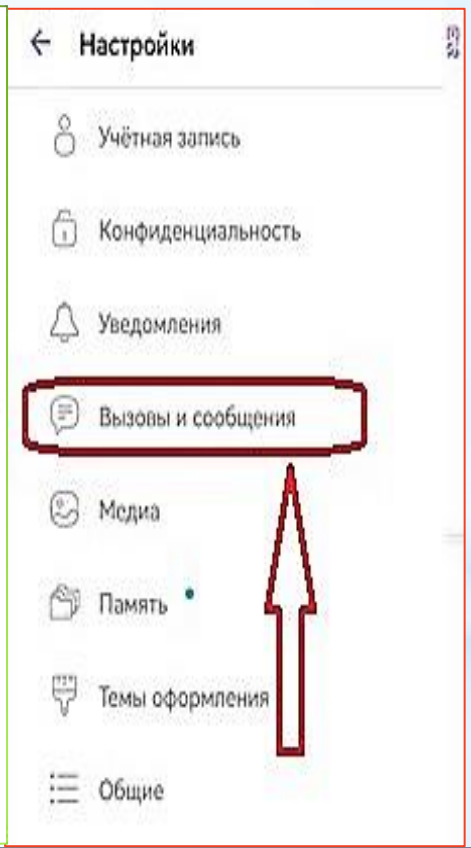
1. ***«По вашему банковскому счету происходят подозрительные операции»;***
2. ***«Необходимо продлить срок действия сим-карты, продиктуйте код из смс-сообщения»;***
3. ***«Ваш личный кабинет «Госуслуги» пытаются взломать»;***
4. ***«Переведите деньги на безопасный или специальный счет»;***
5. ***«Поучаствуйте в операции по поимке сотрудника банка – мошенника»;***
6. ***«Необходимо осуществить перерасчет трудового стажа»;***
7. ***«Для инвестирования переведите деньги на счет»;***
8. ***«Необходимо заменить полис медицинского страхования на новый»;***
9. ***«Вам необходимо перейти по полученной ссылке»;***
10. ***«У вас на телефоне есть вирусная программа, необходимо скачать наше приложение»;***
11. ***«Ваш сын (дочь, внук, внучка) попали в ДТП и т.д.».***

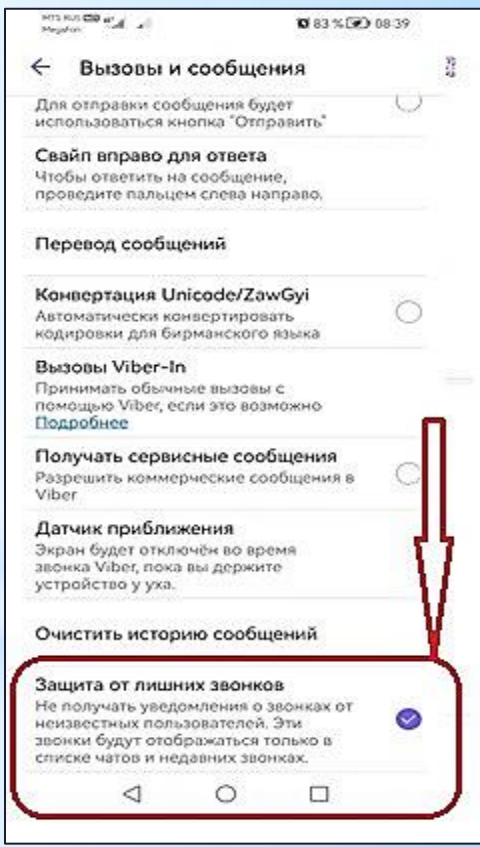
МВД по Республике Бурятия

Защита от звонков в Viber

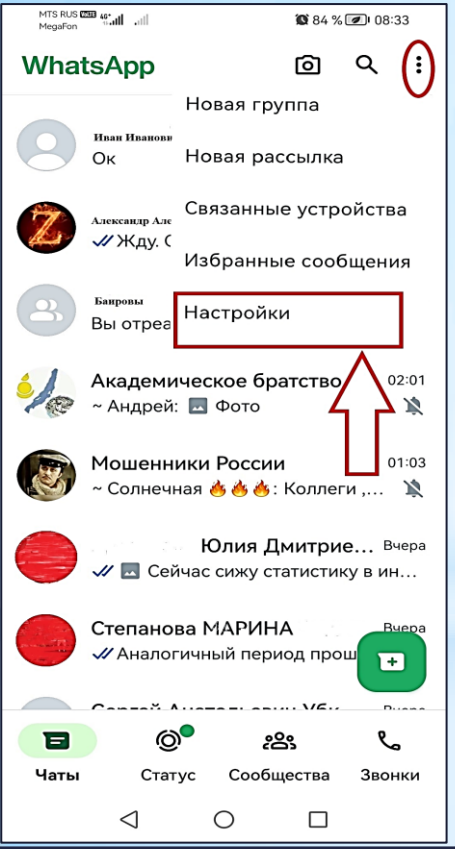


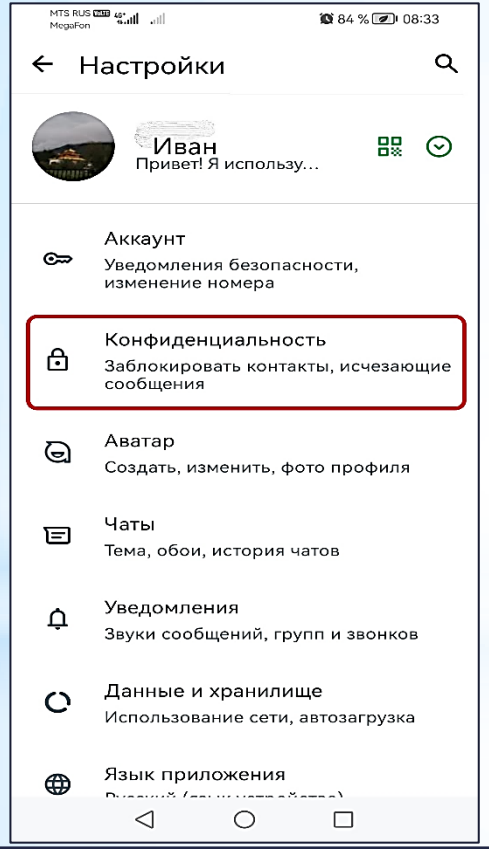


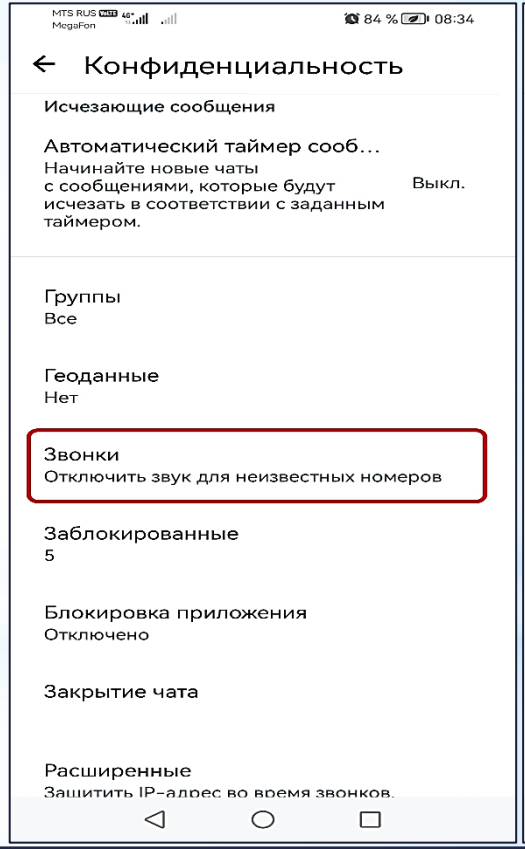


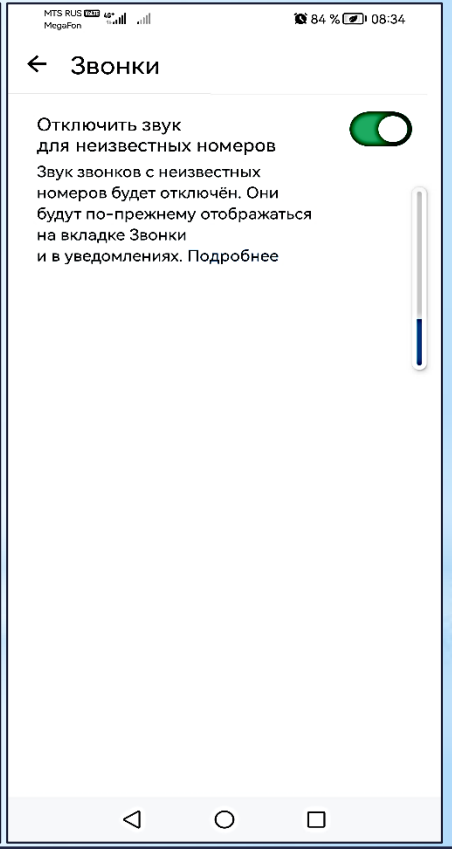


Защита от звонков в *WhatsApp*

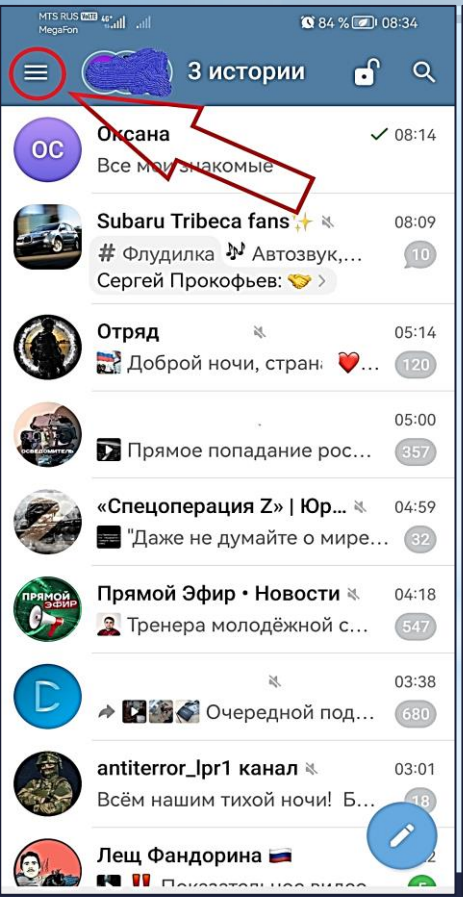


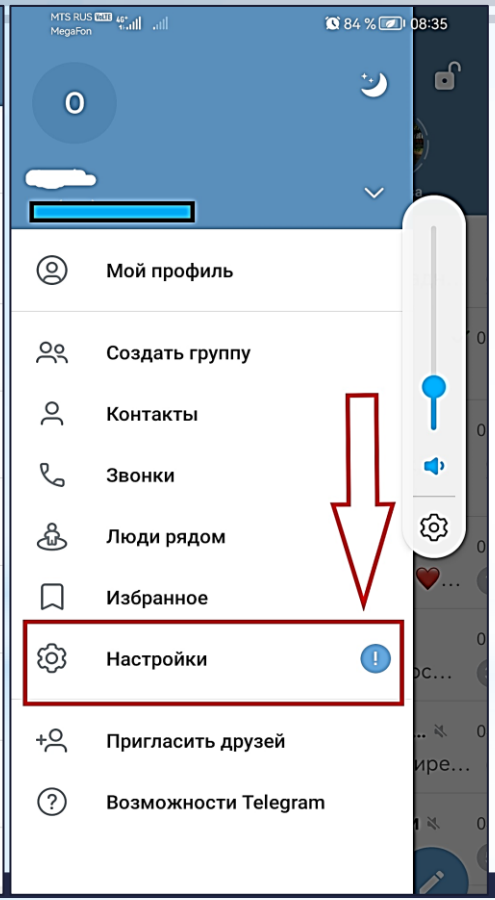


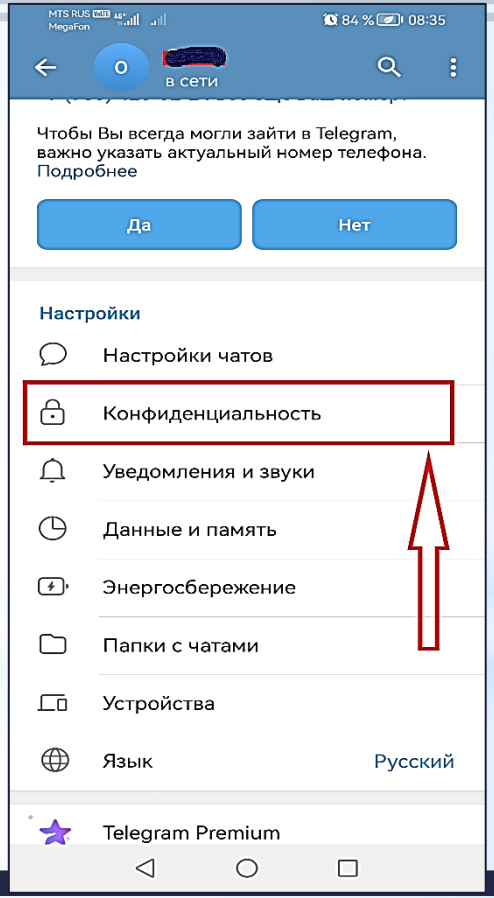


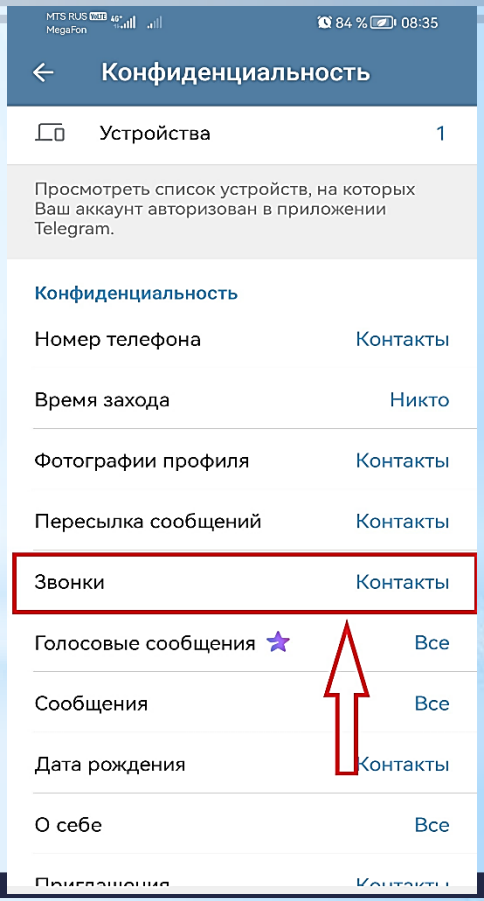


Защита от звонков в *Telegram*

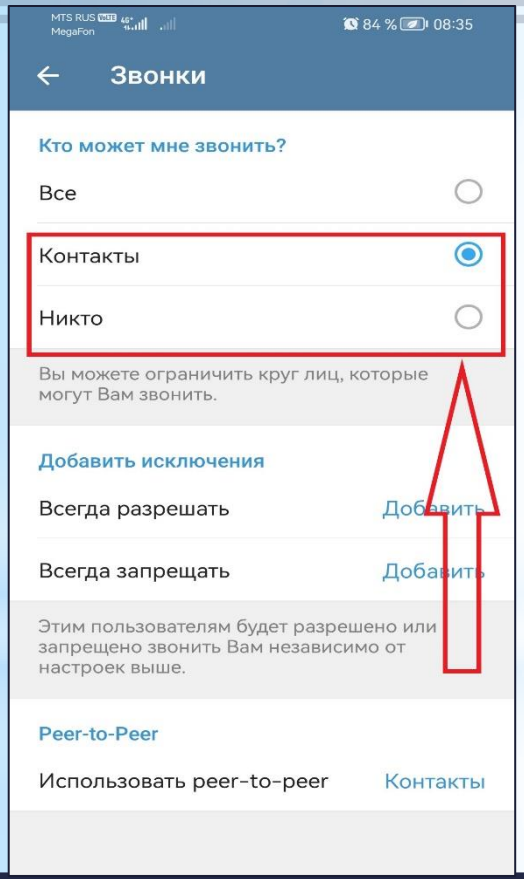


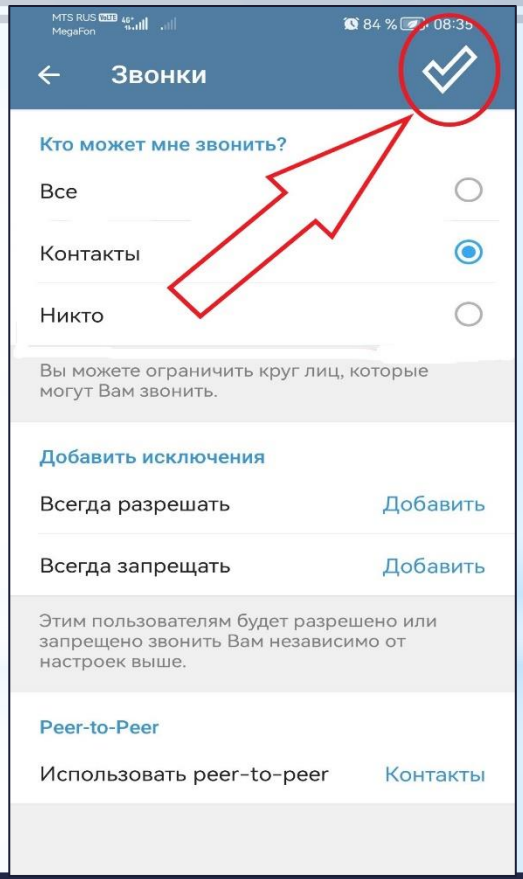




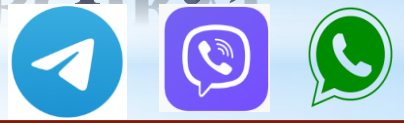


Защита от звонков в *Telegram*



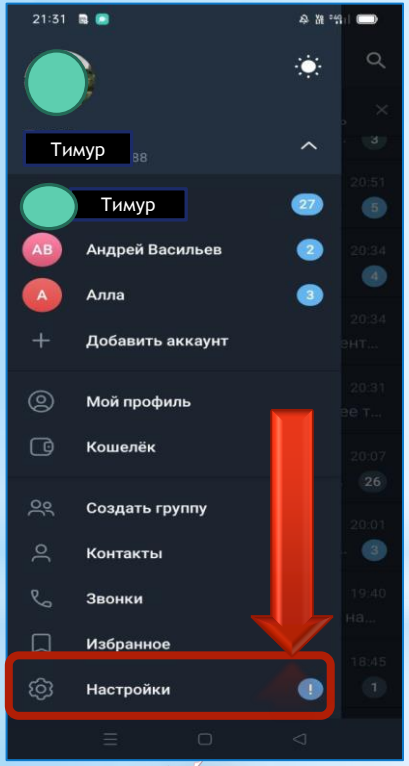


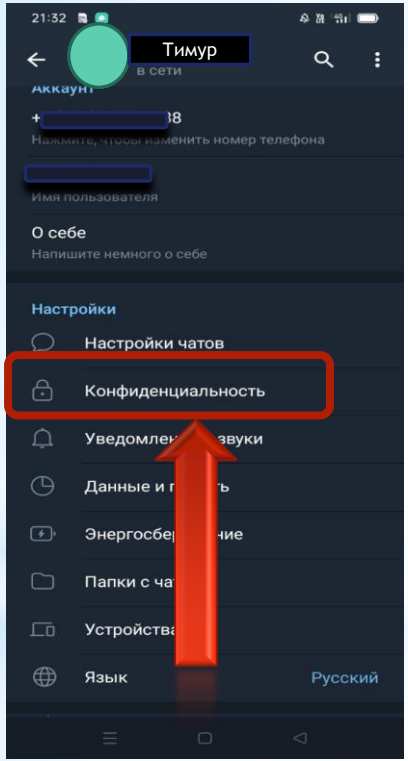
Как настроить двухфакторную аутентификацию (проверку) в мессенджерах

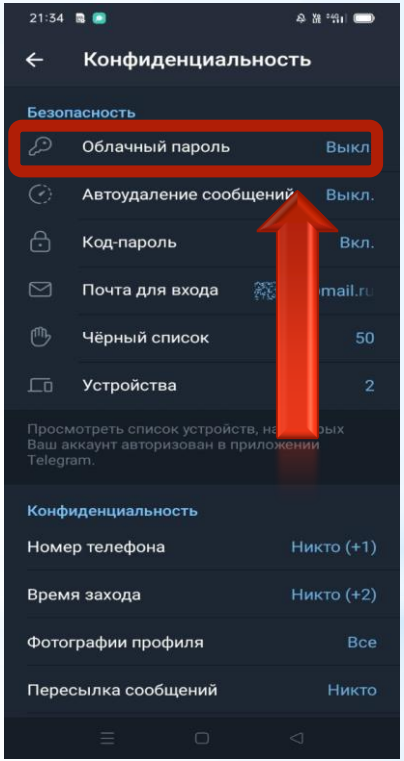


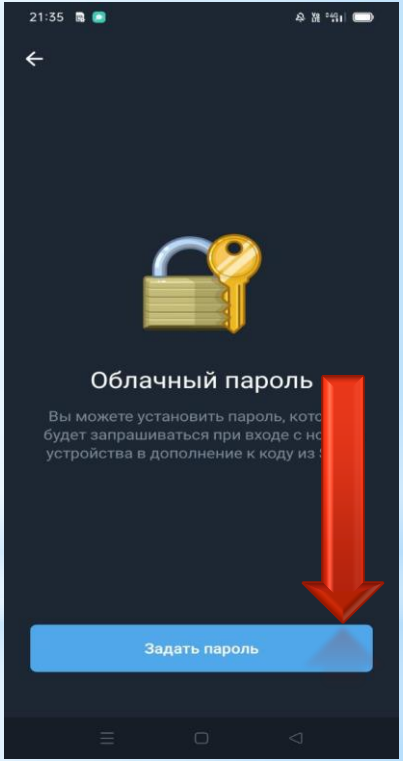
МВД по Республике Бурятия

Как настроить двухфакторную аутентификацию в *Telegram*:

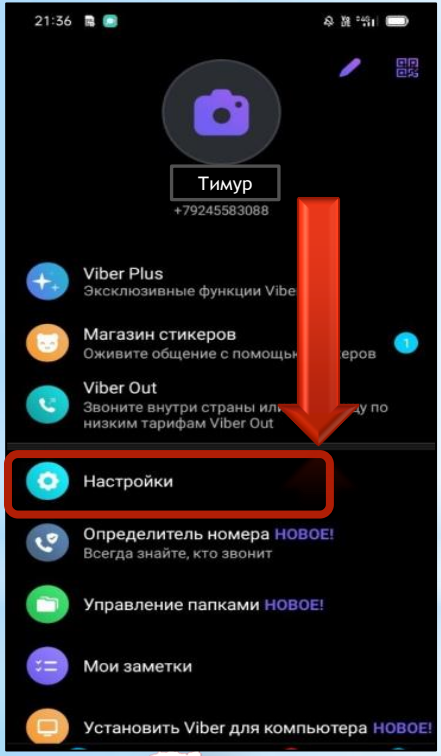


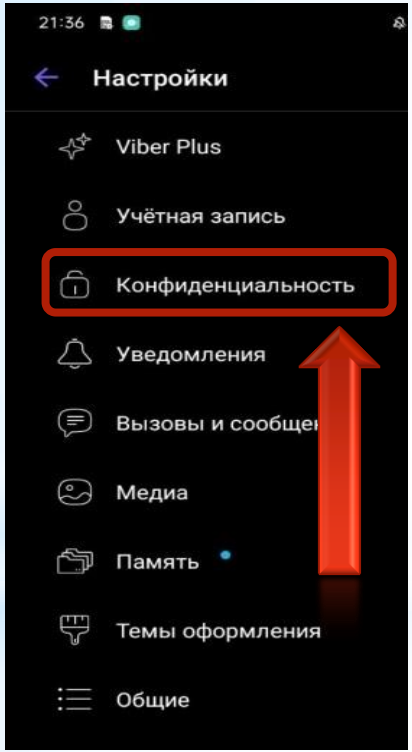


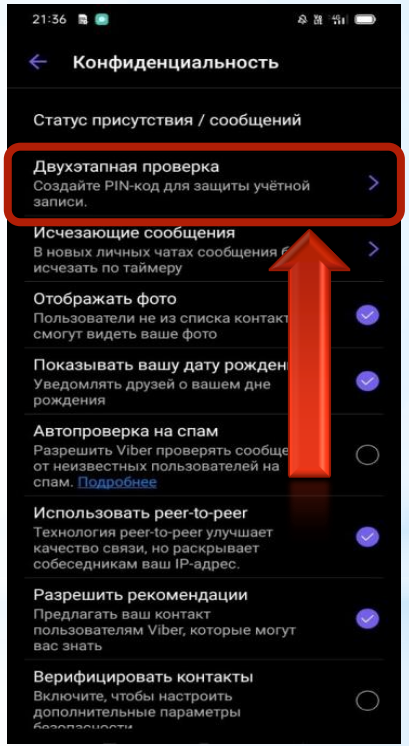




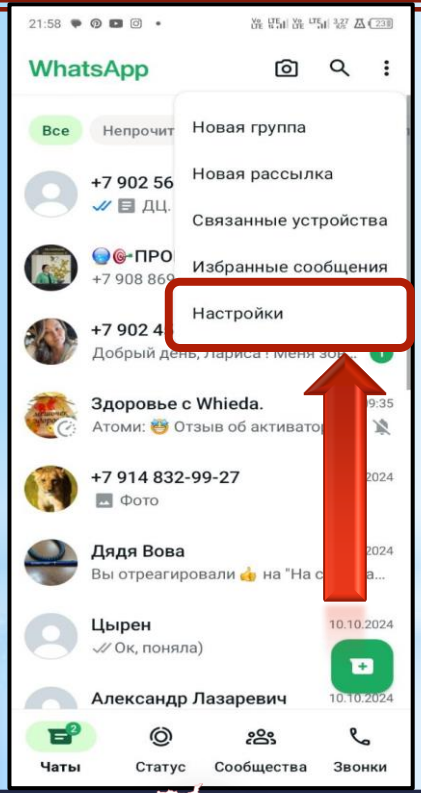
Как настроить двухфакторную аутентификацию в *Viber*:

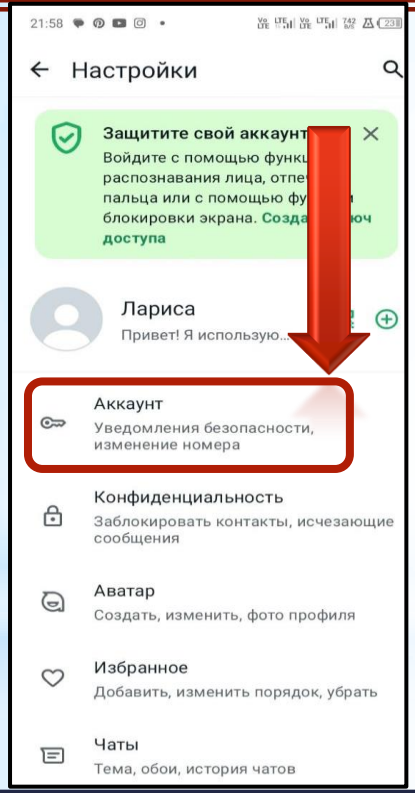


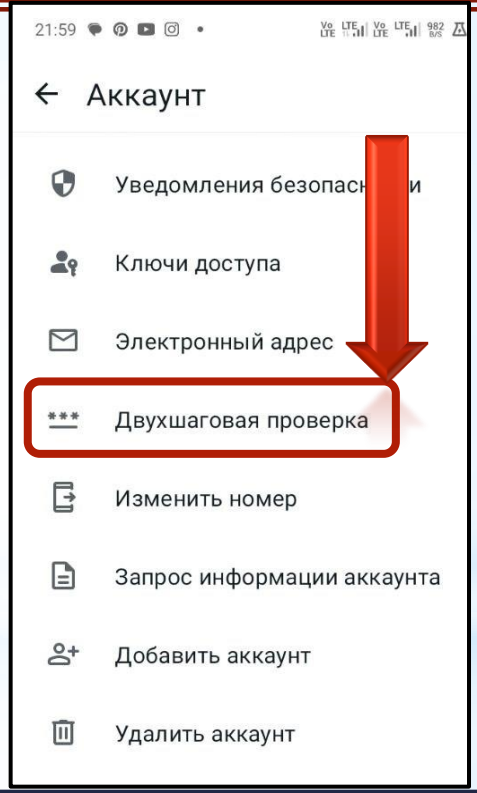


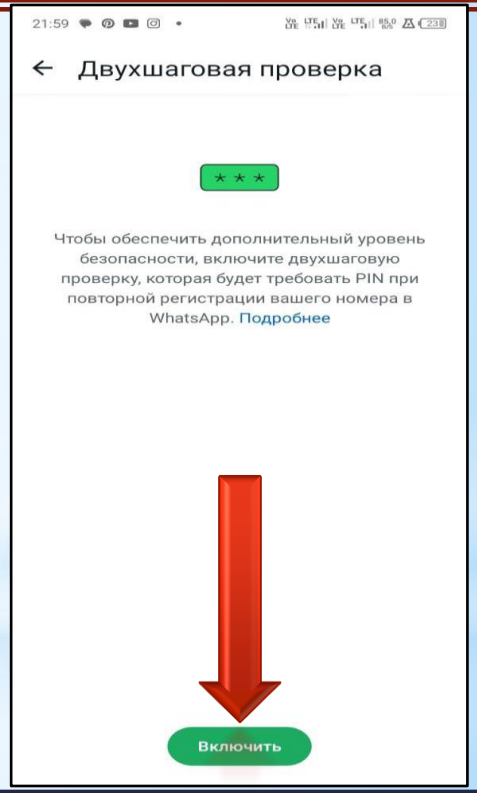


Как настроить двухфакторную аутентификацию в *WhatsApp*:









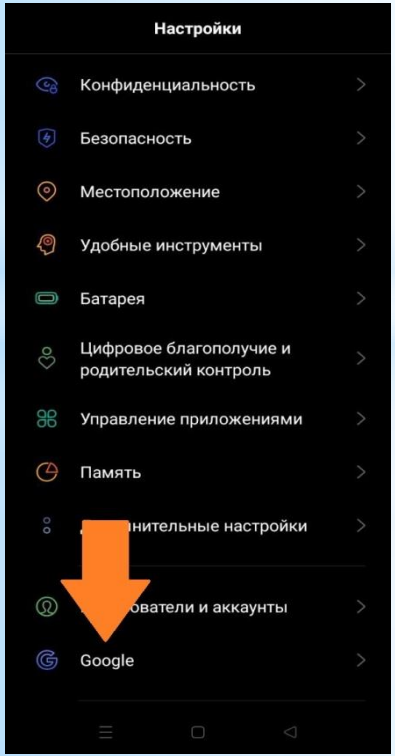
Как уберечь ребенка от преступных посягательств в цифровой среде

МВД по Республике Бурятия

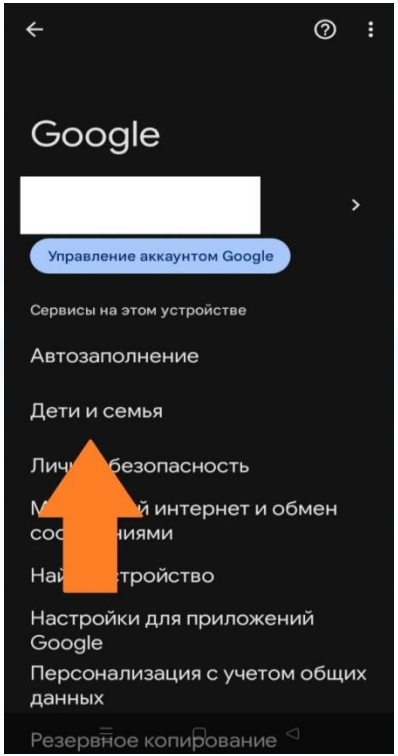
Установите дома родительский контроль на телевизор и его аккаунты в интернете.

1. Откройте «Настройки» на устройстве ребенка.

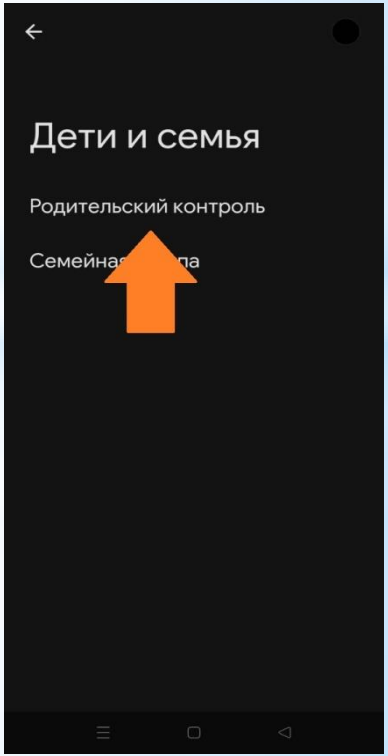
2. Выберите «Google»



3. «Дети и семья»

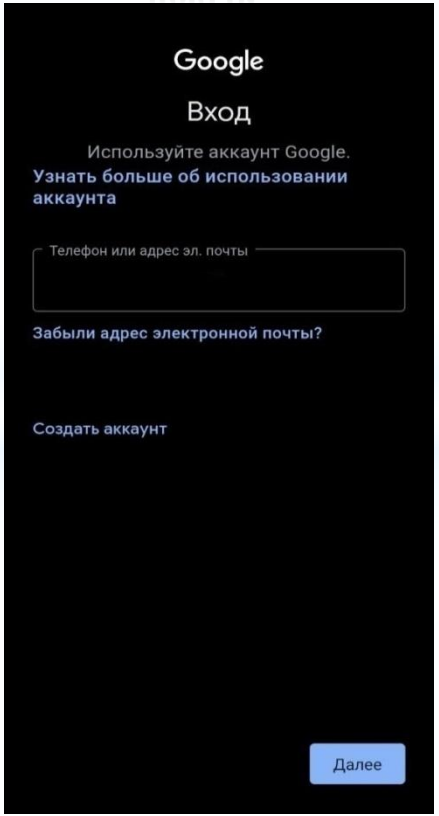


4. «Родительский контроль»

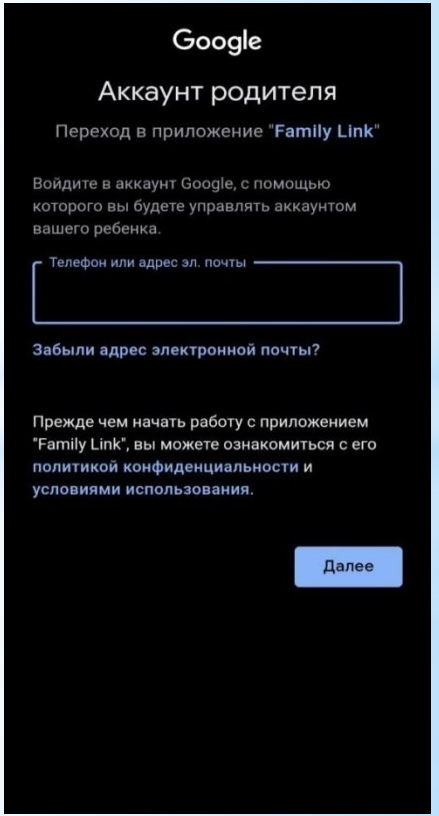


Нажмите «Приступить»

Выберите аккаунт ребенка или создайте новый.



Войдите в свой «родительский»



Будьте бдительны!!!

◊ Контролируйте ребенка в социальных сетях, просматривайте кого он добавляет в друзья и с кем общается.

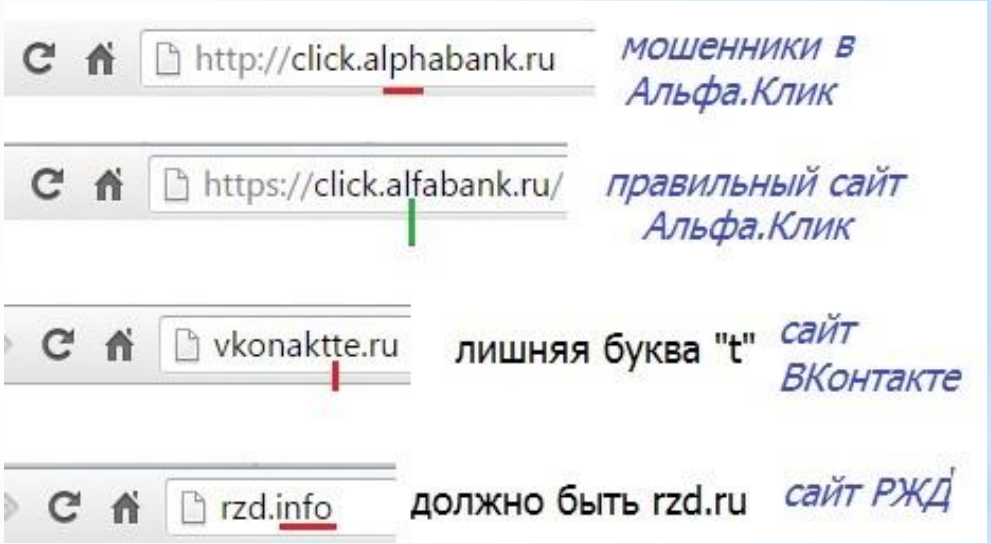
◊ Внимательно следите за финансовыми тратами своего ребенка.

◊ Если у него имеется банковская карта, кому и зачем он переводит денежные средства и какие осуществляет покупки.

◊ Объясните ребенку про цифровую гигиену.

Как распознать сайт двойник?

- **ПРИ ПРОВЕРКЕ ОБРАТИТЕ ВНИМАНИЕ НА ДОМЕН (ИМЯ) САЙТА:**
  - **Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I» (onL1ne вместо onLIne);**
  - **Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);**
  - **В некоторых случаях для написания домена используются буквы похожие на латинские из алфавита другого языка;**
  - **Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU**



Схемы взлома и защита от них

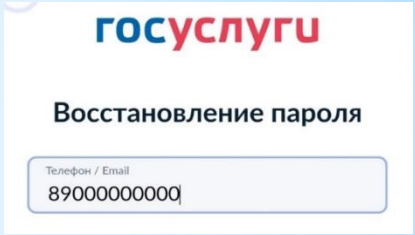
МВД по Республике Бурятия

1. Звонок от работника сотового оператора

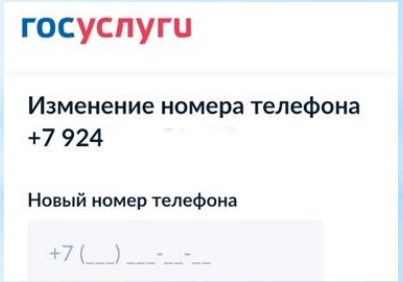
1. Поступает телефонный звонок от оператора сотовой связи, сообщают что необходимо продлить срок действия SIM-карты или обновить паспортные данные.

2. После чего, в целях подтверждения личности, или под другим предлогом просят сообщить / продиктовать SMS-код, поступивший на телефон с портала «Госуслуги»

- В это время мошенники, зная абонентский номер жертвы, на сайте «Госуслуги» открывают вкладку: «Восстановление пароля».
- Указывают номер жертвы и ждут когда им сообщат код из SMS.



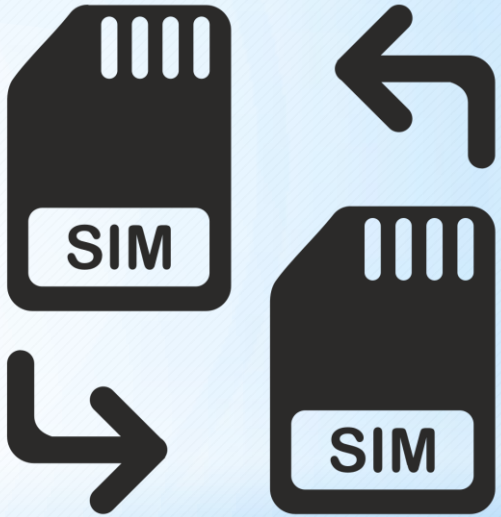
- Для личных кабинетов, где установлен вход на портал по SMS-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. На самом деле повторно приходит КОД для изменения номера телефона.



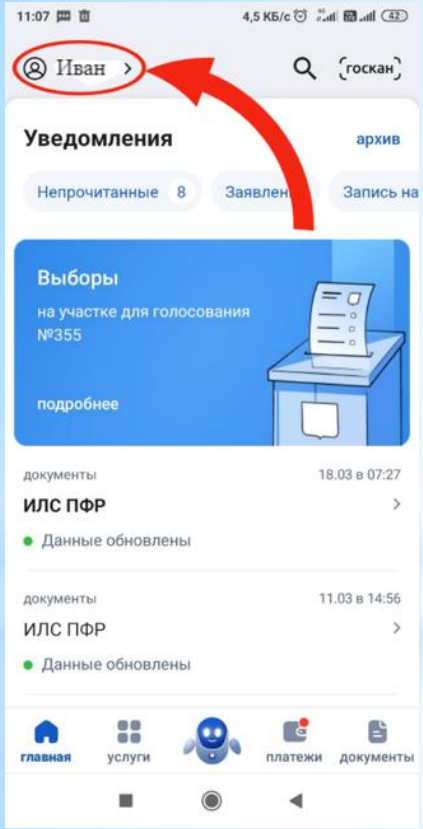
2. Переоформление SIM-карты

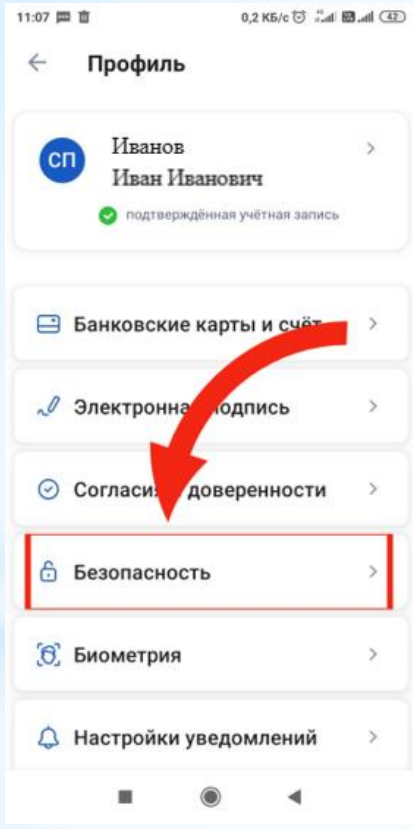
- SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

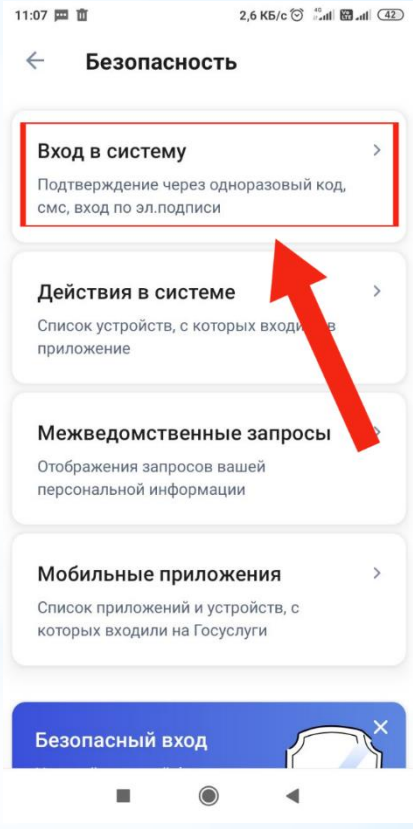
  Тем самым, предоставляя возможность новому пользователю восстановить доступ к личному кабинету от портала «Госуслуги», путем ввода SMS-кодов, поступивших на перевыпущенный номер SIM-карты, что и делают злоумышленники.

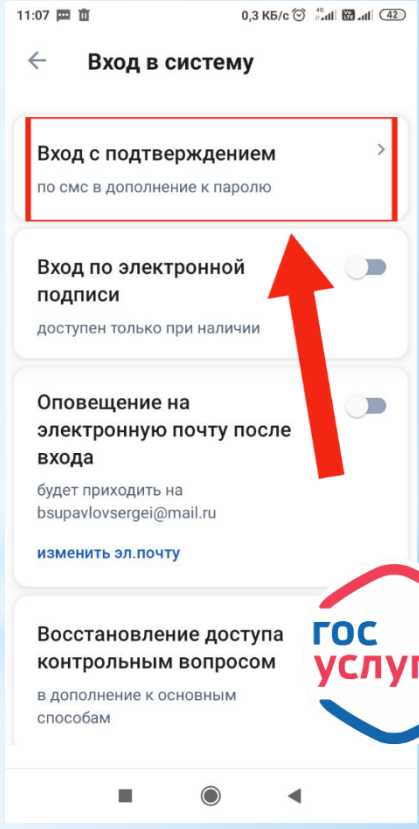


Дополнительная защита личного кабинета

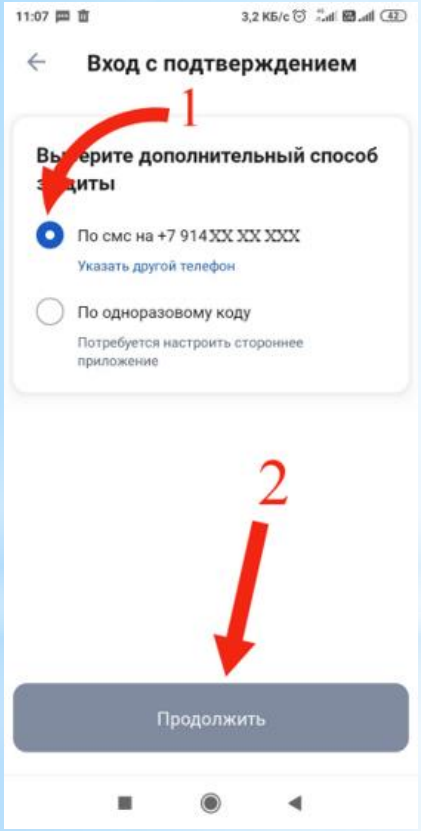








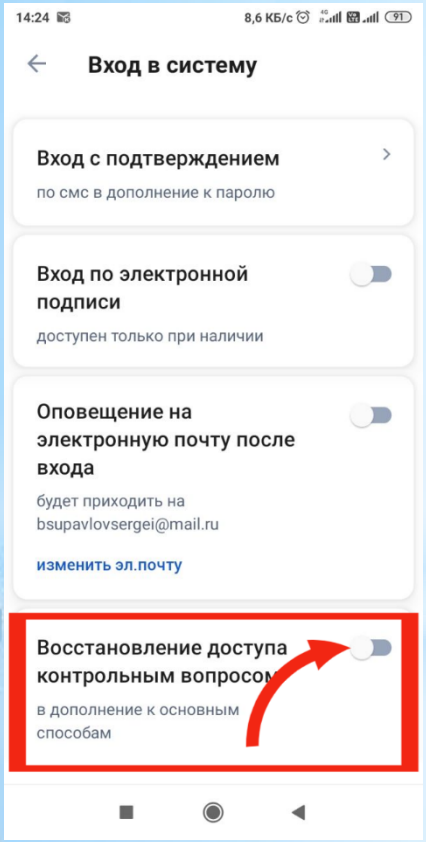
Дополнительная защита личного кабинета

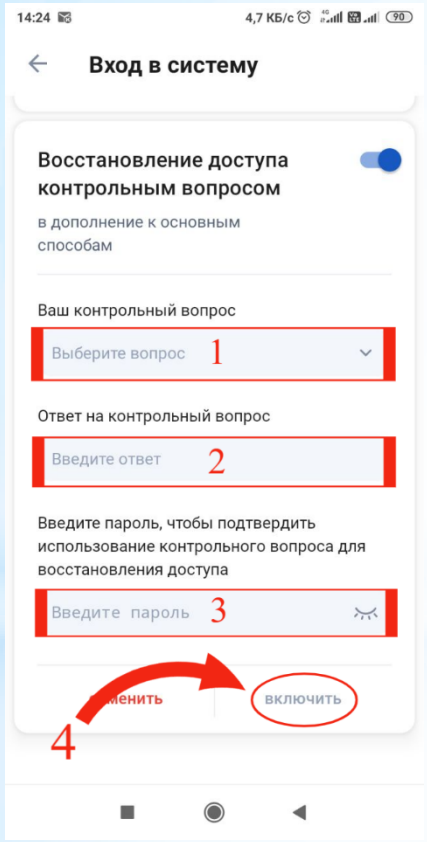


Функция входа с двухэтапной аутентификацией.

Войти в личный кабинет с помощью одного только логина и пароля будет недостаточно, при каждом входе в личный кабинет необходимо вводить одноразовый код, поступающий в виде SMS-сообщения.

Дополнительная защита личного кабинета

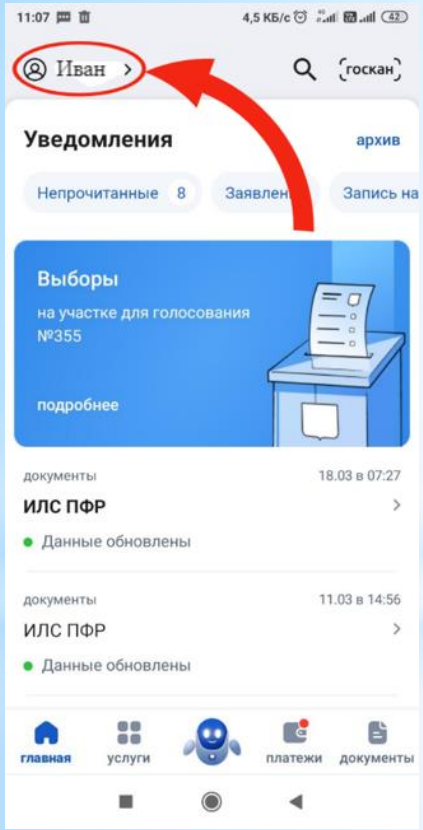


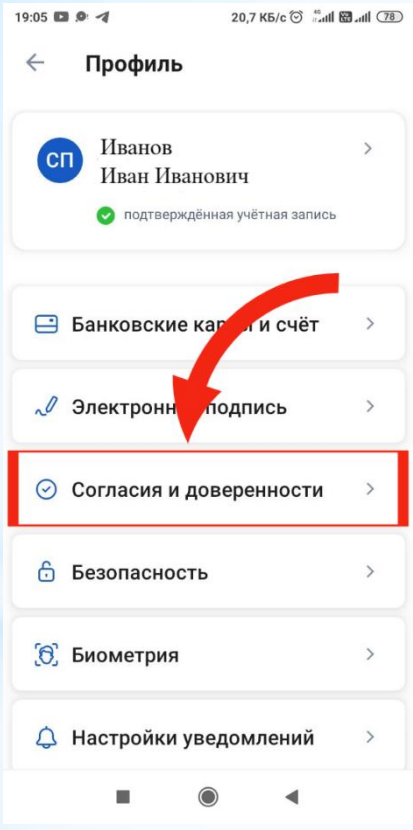


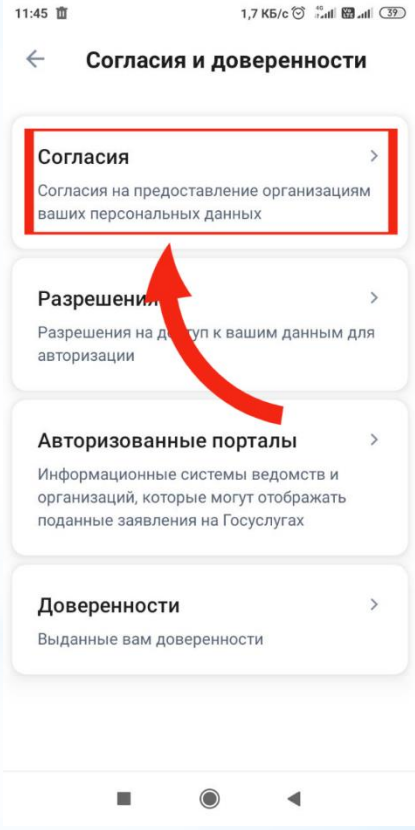
Функция восстановления доступа контрольным вопросом.

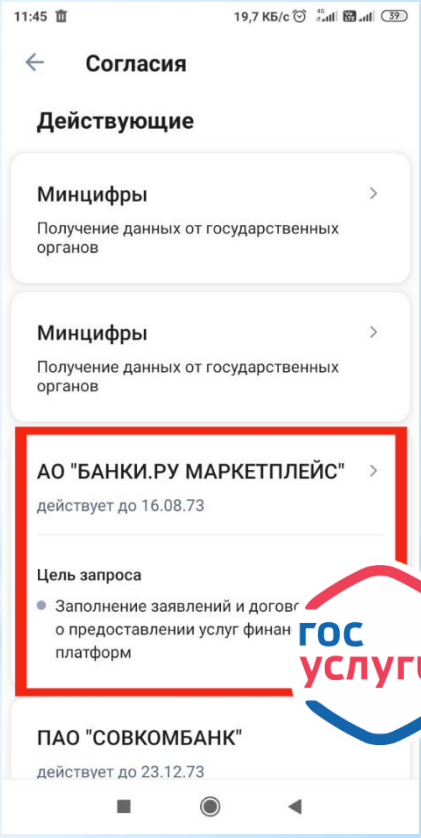
После переоформления SIM-карты, мошенники не смогут восстановить доступ к личному кабинету, так как они не знают ответ на контрольный вопрос.

Отзыв согласий

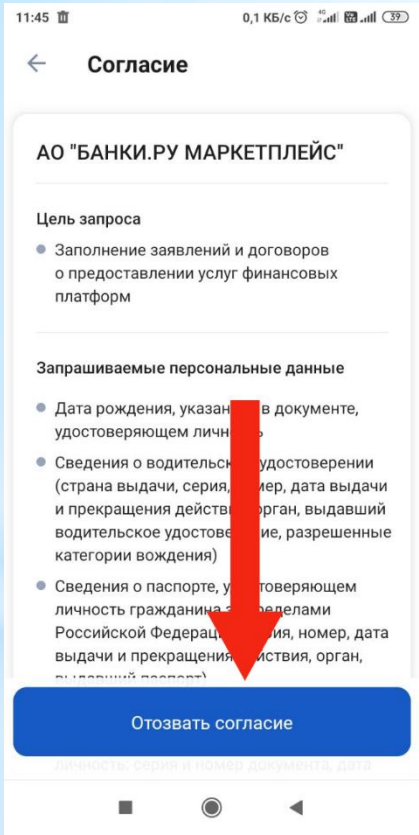


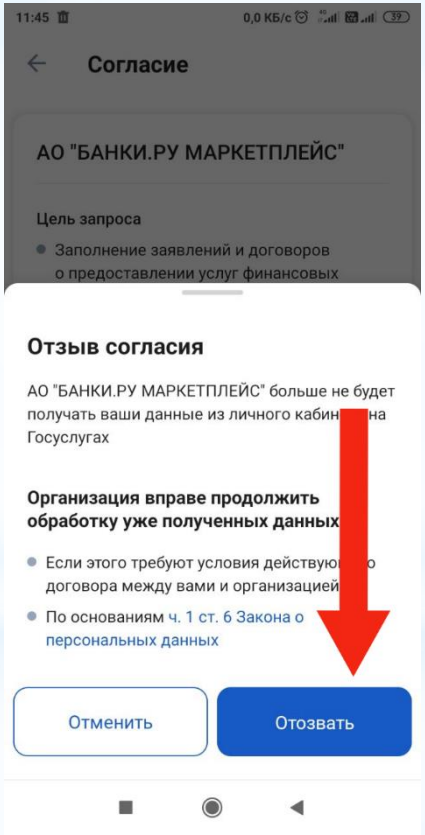


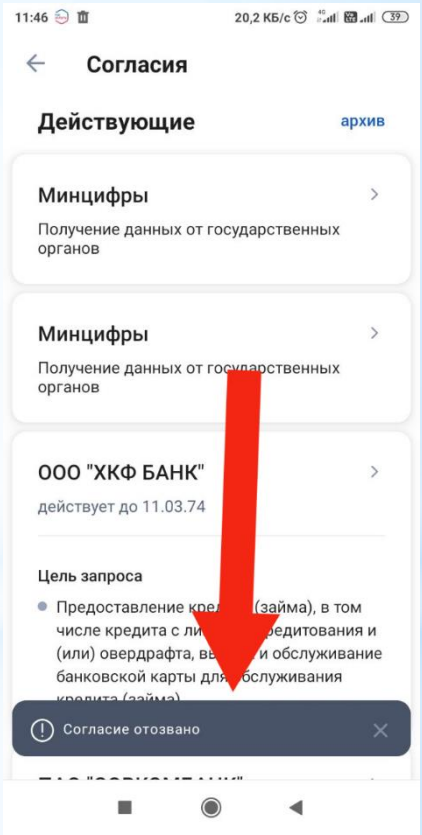




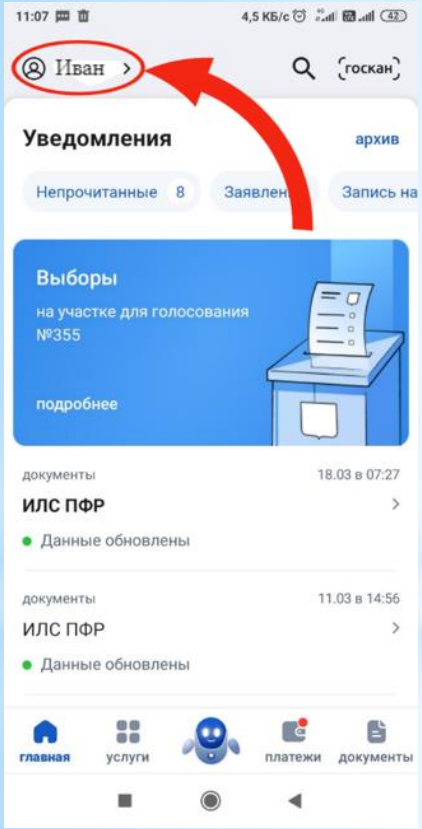
Отзыв согласий

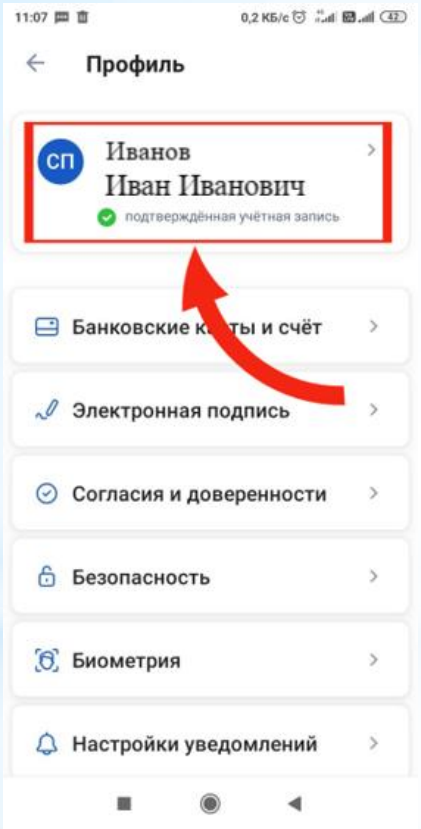


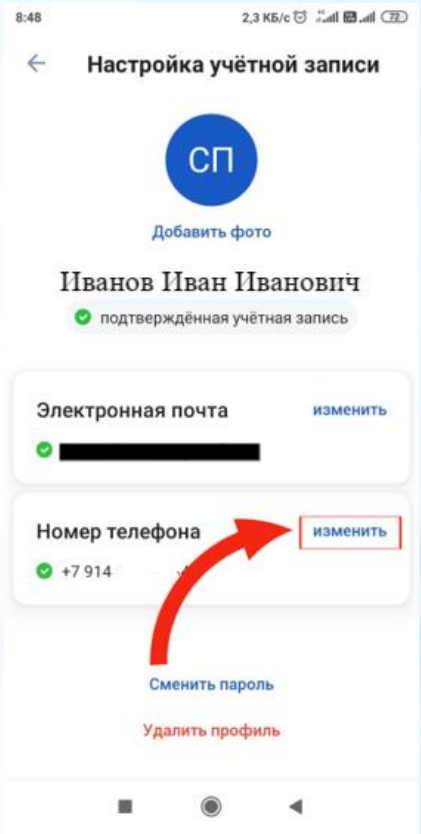


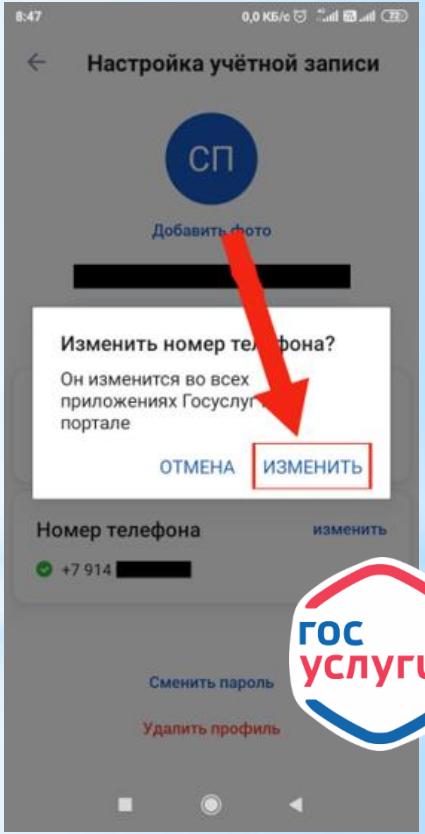


Способ открепления номера телефона









Восстановите пароль от личного кабинета

Перейдите на сайт или в приложение одного из своих банков.

Повторите регистрацию на «Госуслуги» через банк-номер из личного кабинета банка будет перенесен в личный. Банк вышлет пароль для входа в аккаунт.

ИЛИ

Обратитесь в офис МФЦ и попросите оператора восстановить пароль.

Сотрудники проверят вашу личность, помогут восстановить доступ к аккаунту и сменить пароль.

Возьмите с собой паспорт и СНИЛС

QR-код для скачивания материалов по профилактике ИТТ-преступлений

МВД по Республике Бурятия собраны материалы для использования в профилактической деятельности в период проведения оперативно-профилактического мероприятия «Внимание! Мошенники!».

Доступ к ним можно получить по данному QR-коду.