



ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ

полковник полиции
Базаржапов Бато Баторович



МВД по Республике Бурятия



**МОШЕННИК
ЗВОНИТ ЖЕРТВЕ,
ПРОСИТ СООБЩИТЬ
СМС КОД, ПОД
ПРЕДЛОГОМ**



Сотрудника здравоохранения:

- Предлагает продлить срок действия страхового полиса;
- Запись по электронной очереди.

Сотрудника коммунальных служб:

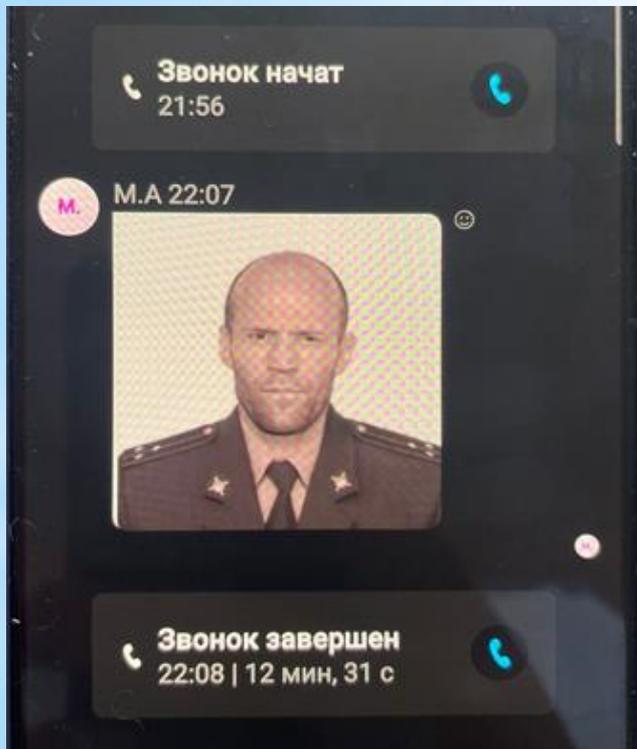
- Предлагает замену электросчетчиков;
- Скачать приложение.

Сотрудника Госуслуг

- Сообщает о взломе личного кабинета.



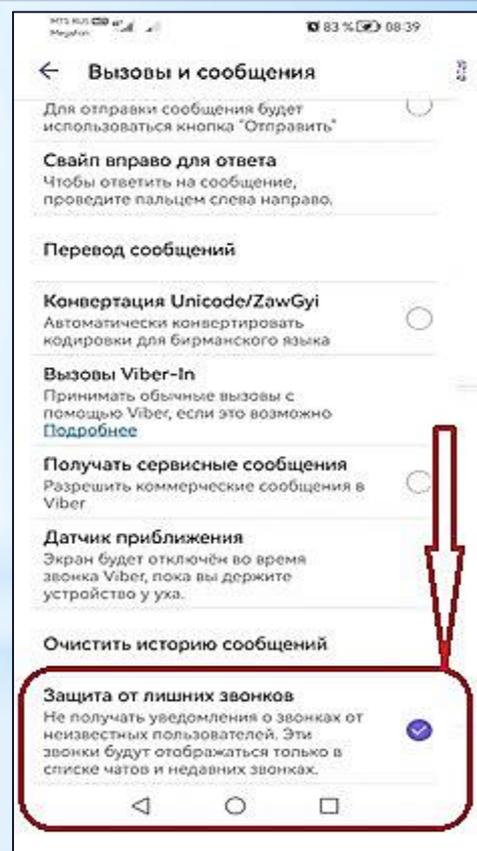
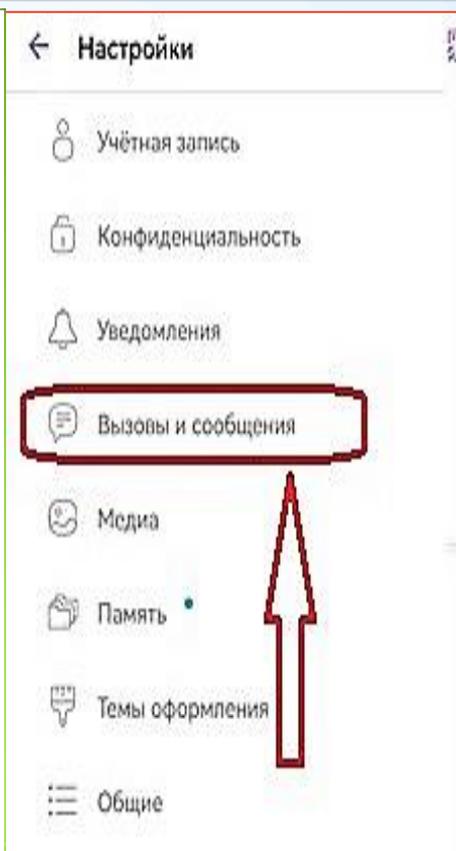
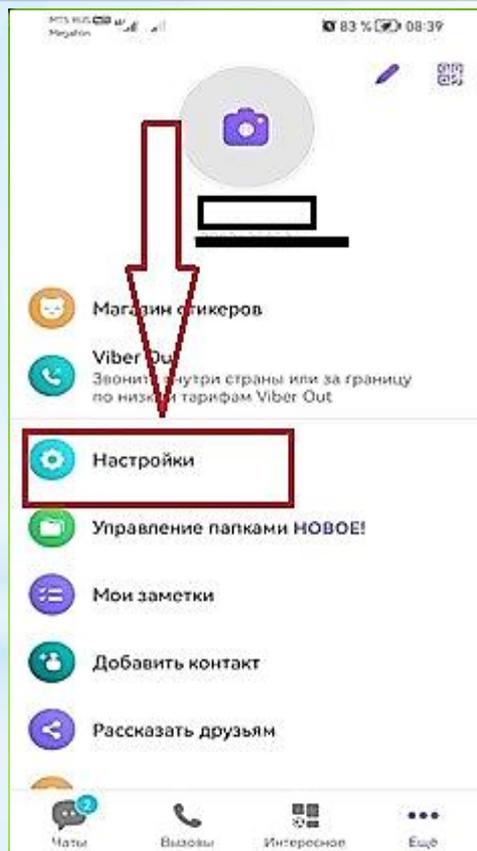
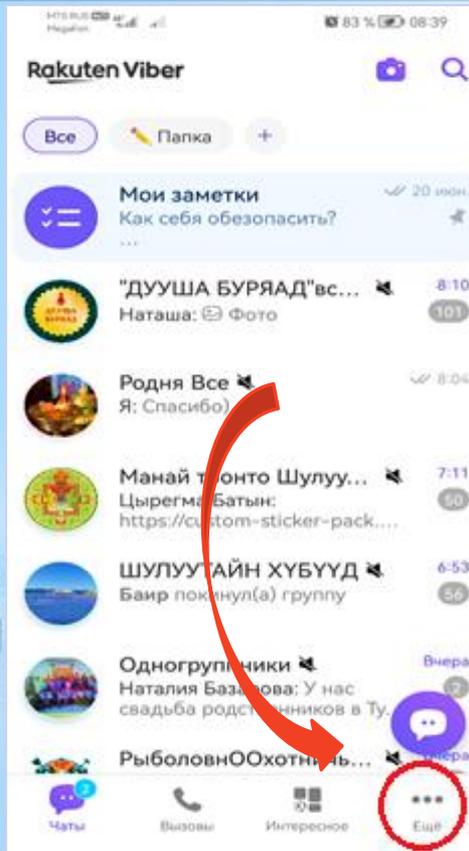
Пример мошеннических действий посредством различных мессенджеров



Общий ущерб составляет более **145 млн. руб.** посредством различных мессенджеров.
(на 01/11/2024)

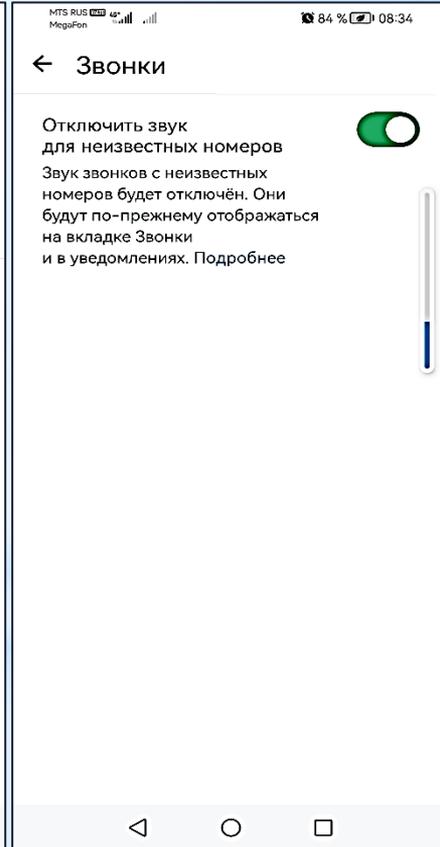
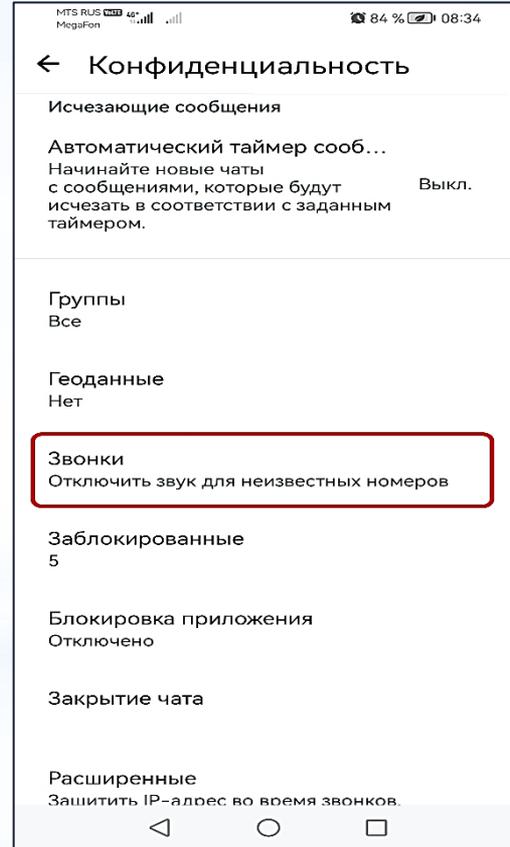
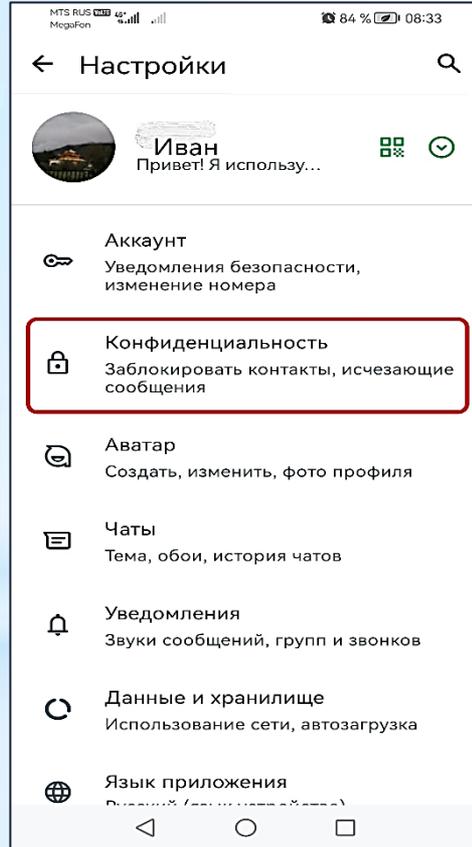
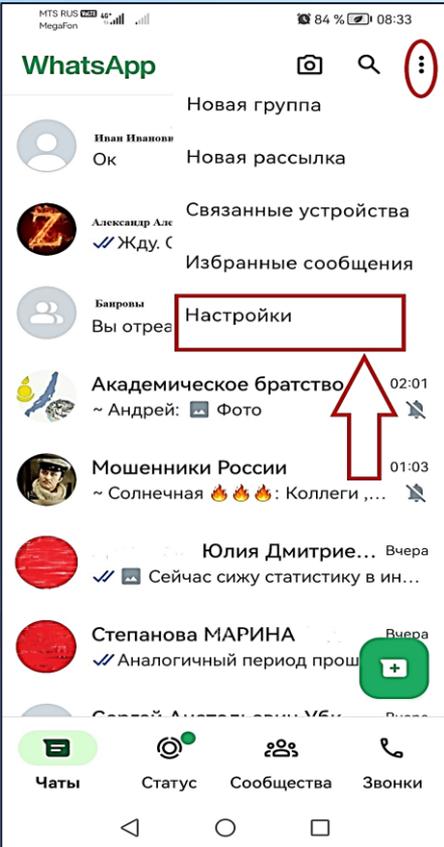


Защита от звонков в Viber



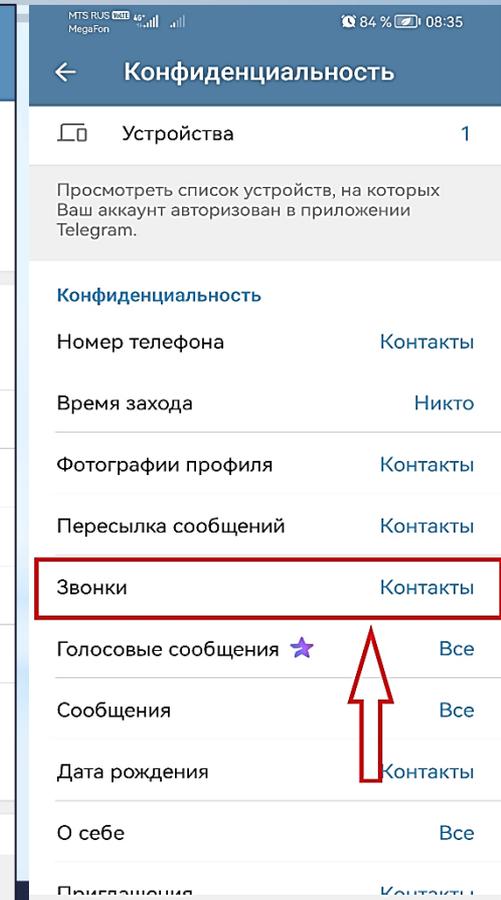
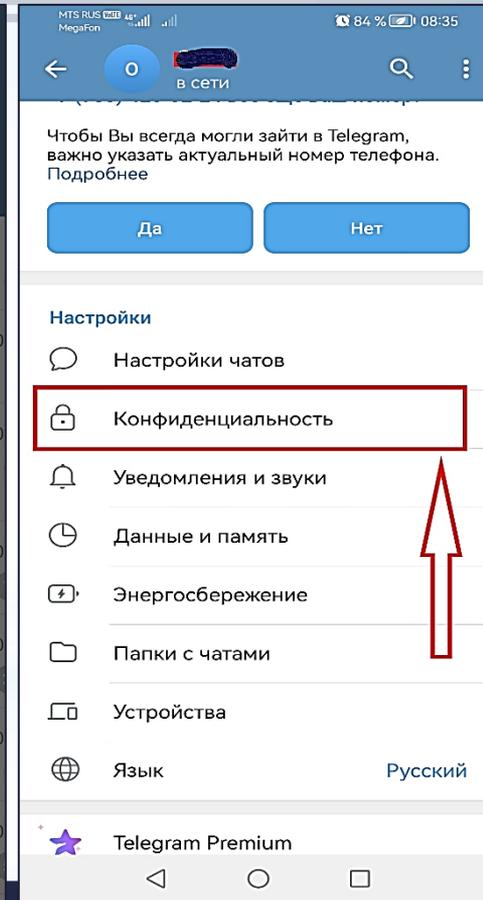
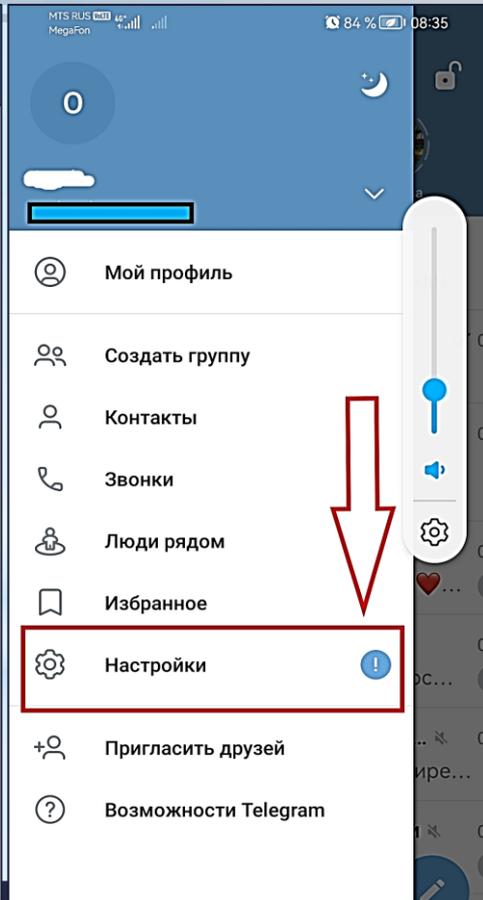
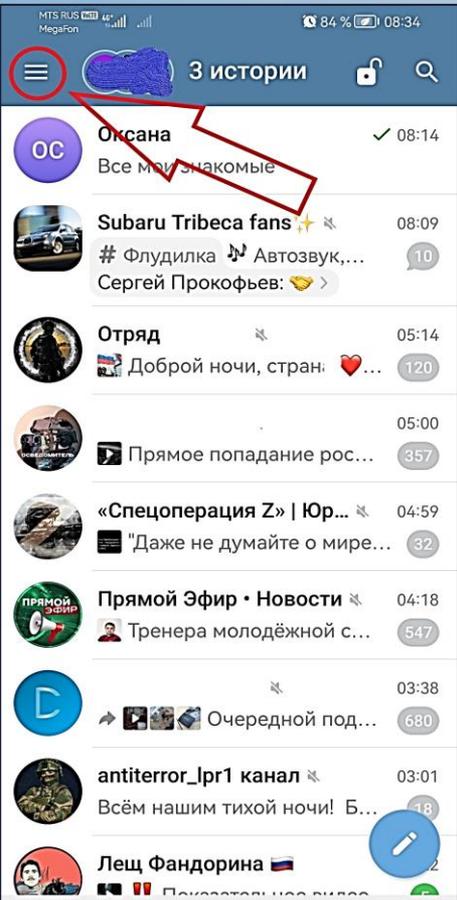


Защита от звонков в WhatsApp



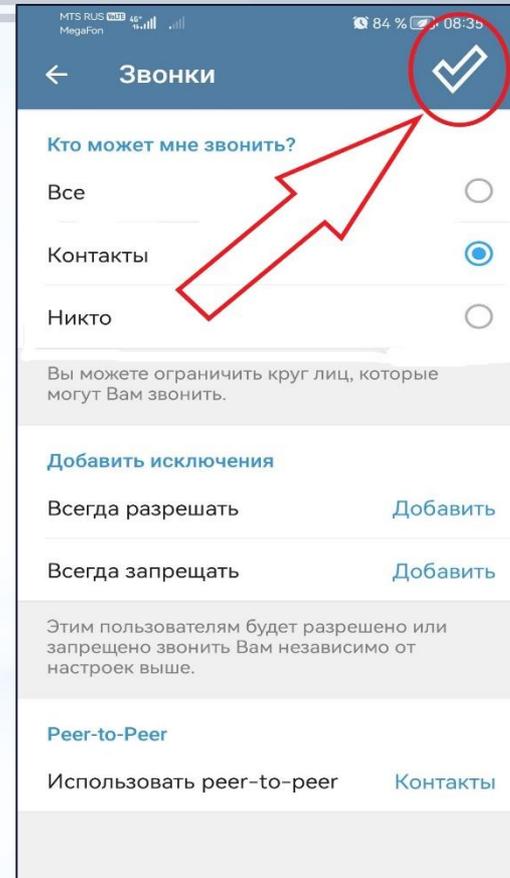
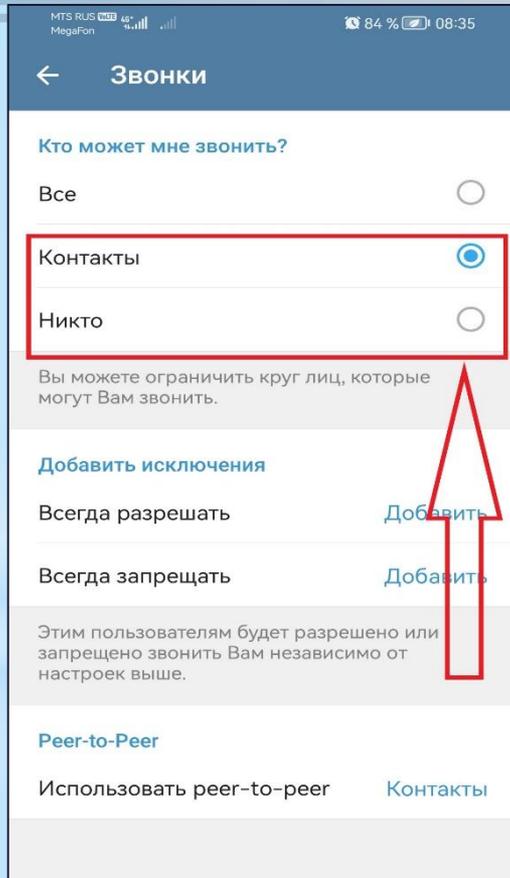


Защита от звонков в Telegram



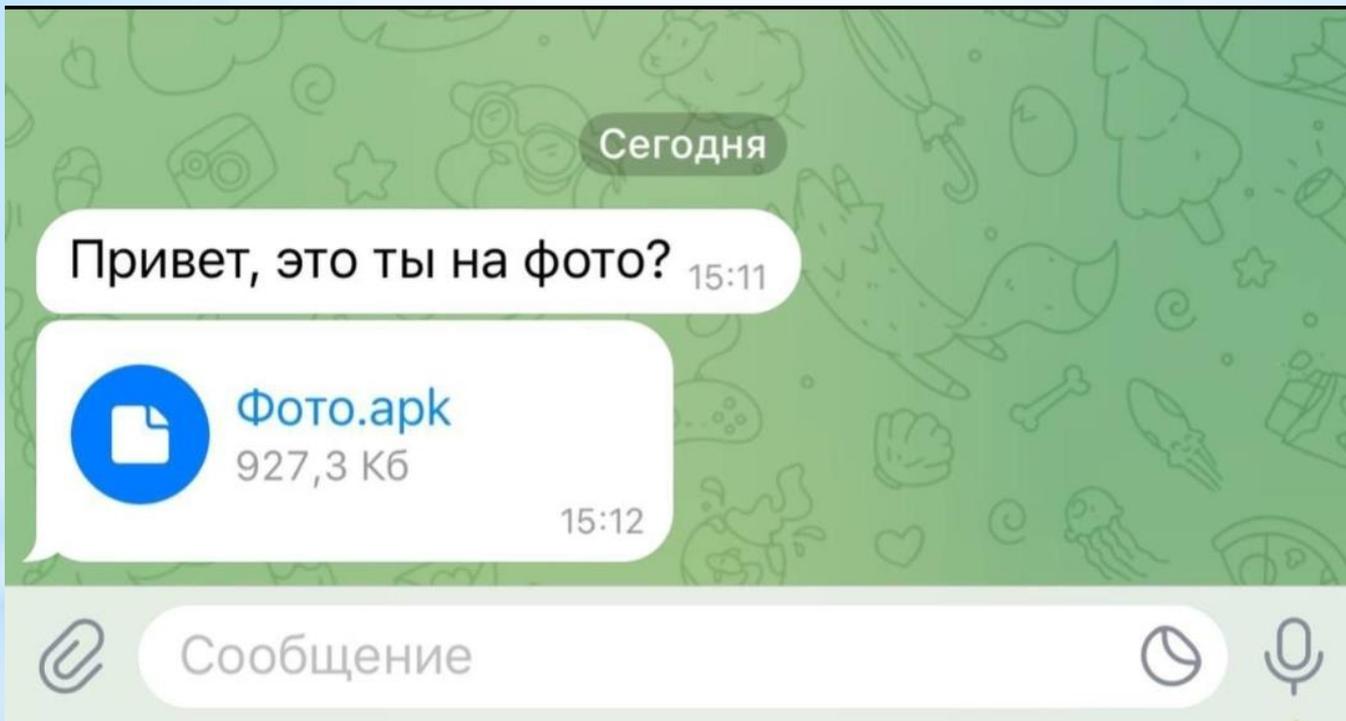


Защита от звонков в Telegram





Новый вид мошенничества в мессенджерах



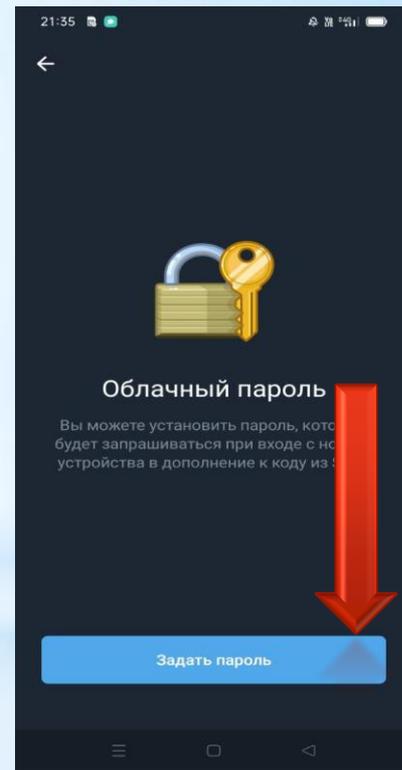
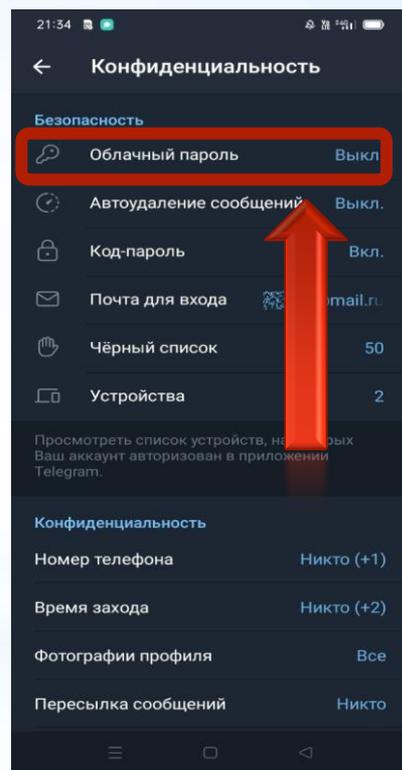
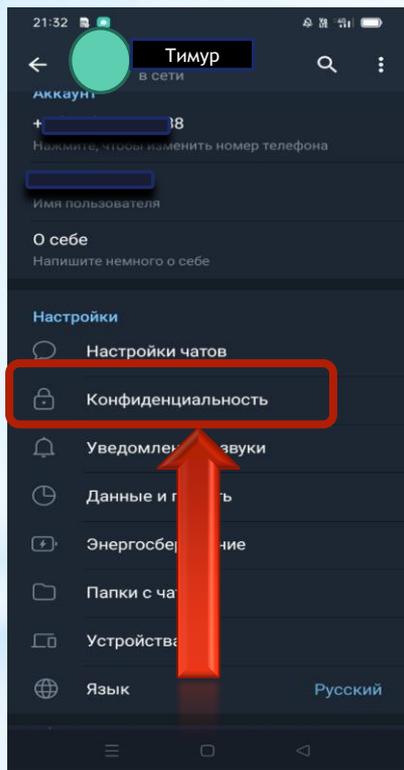
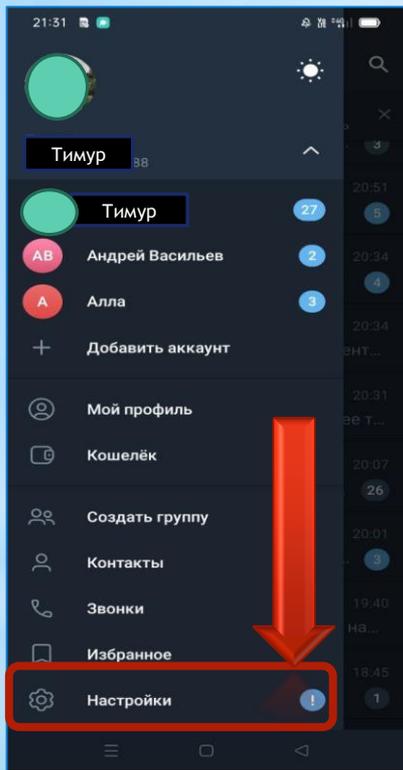


Как настроить двухфакторную аутентификацию (проверку) в мессенджерах



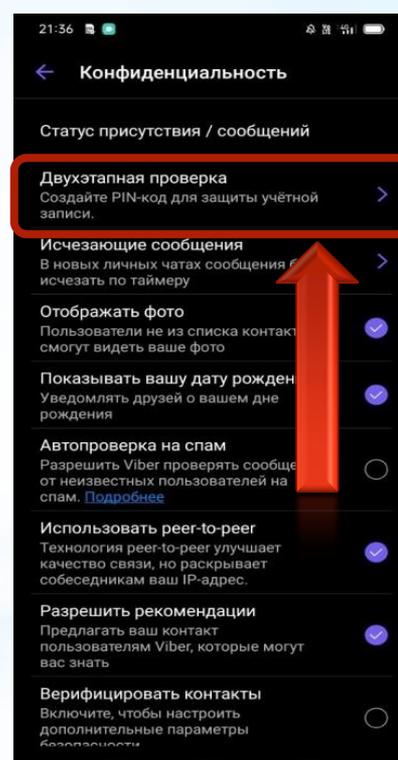
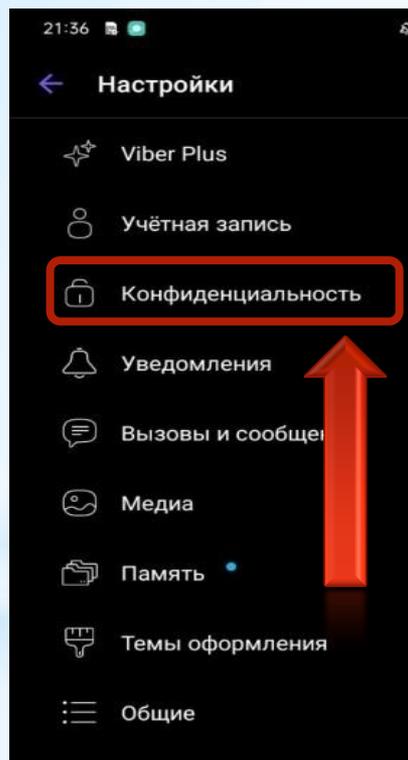
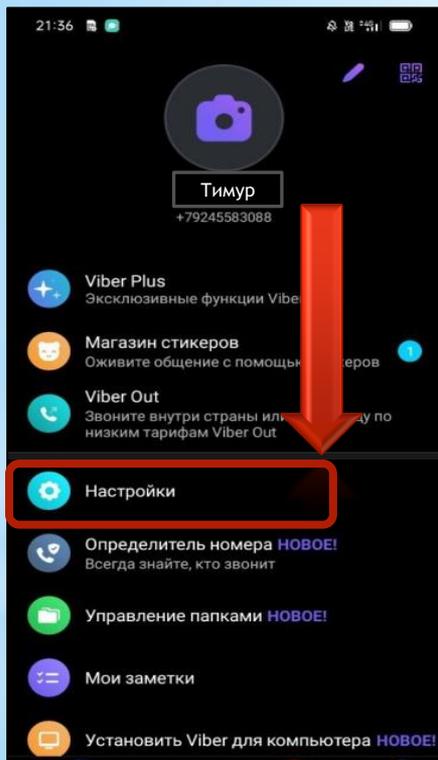


Как настроить двухфакторную аутентификацию в *Telegram*:



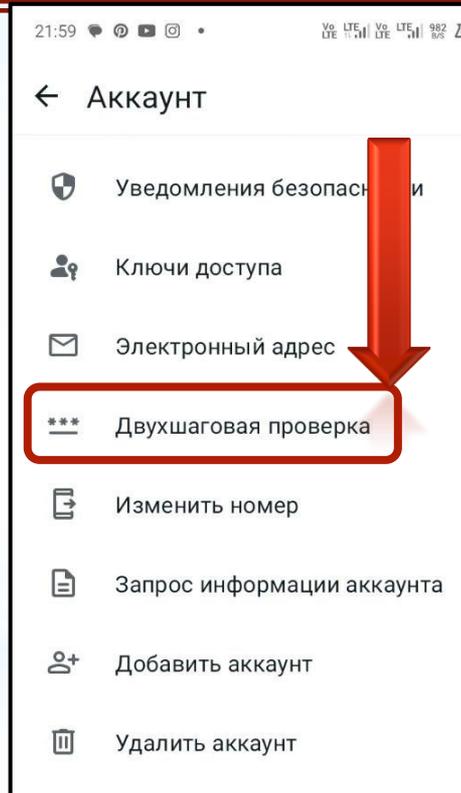
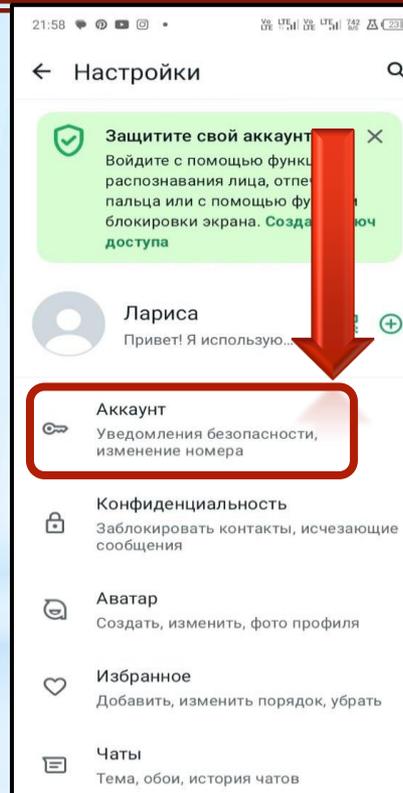
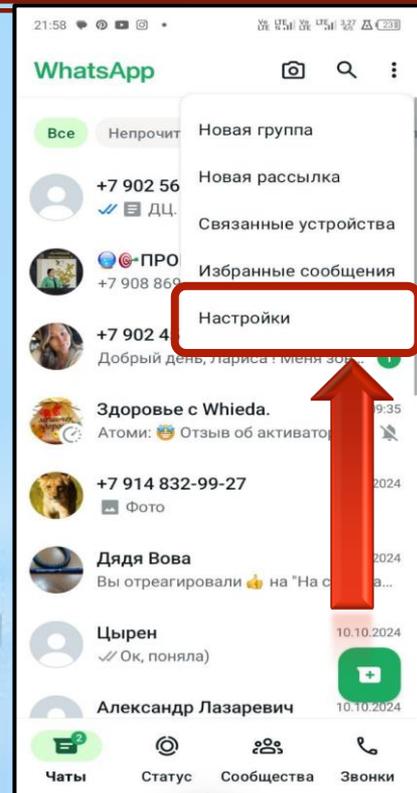


Как настроить двухфакторную аутентификацию в *Viber*:





Как настроить двухфакторную аутентификацию в *WhatsApp*:





Как уберечь ребенка от преступных посягательств в цифровой среде



МВД по Республике Бурятия

Как уберечь ребенка от преступных посягательств в цифровой среде

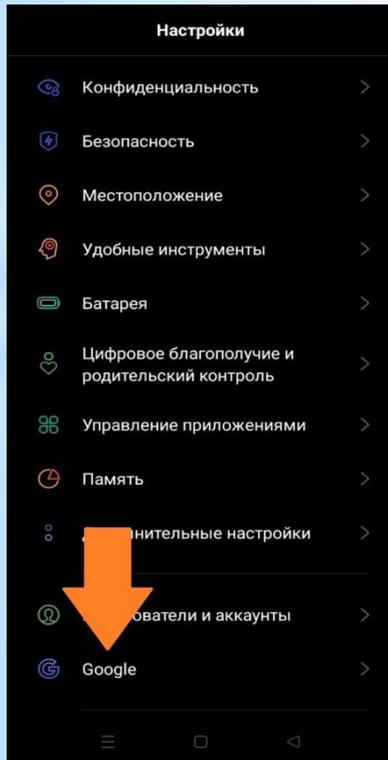
Уделяйте больше внимания своему ребенку
Чаще разговаривайте с ним, чтобы он делился с Вами о своем окружении, как прошел его день и внимательно следите за изменением в его поведении



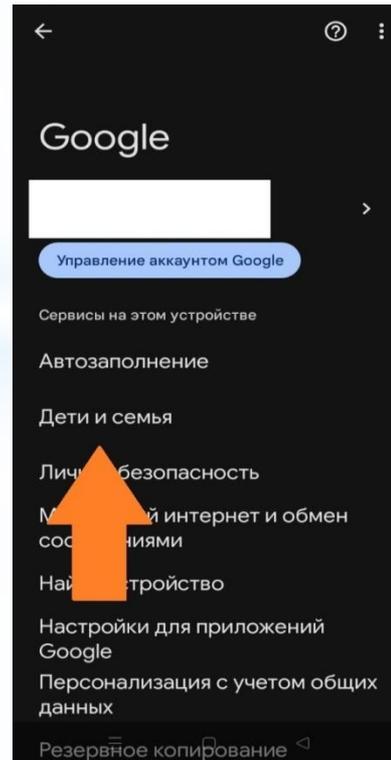
Установите дома родительский контроль на телевизор и его аккаунты в интернете.

1. Откройте «Настройки» на устройстве ребенка.

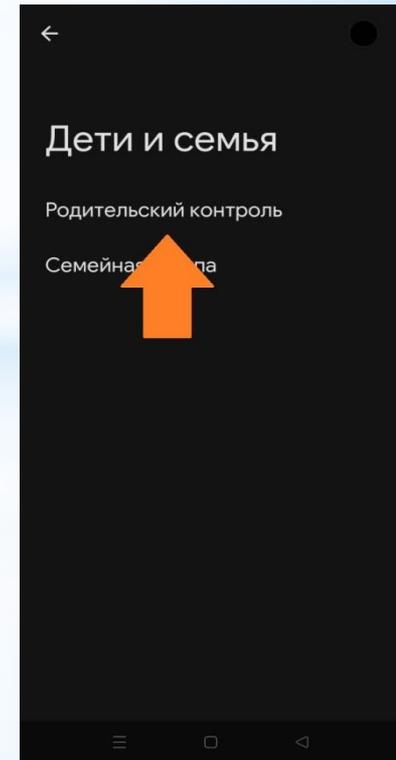
2. Выберите «Google»



3. «Дети и семья»



4. «Родительский контроль»



Нажмите «Приступить»»

Google

Настройте родительский контроль

Вы зададите возрастные ограничения, настройки конфиденциальности и время использования для этого устройства и аккаунта Google своего ребенка.



↓

Приступить

Выберите аккаунт ребенка или создайте новый.

Google

Вход

Используйте аккаунт Google.
Узнать больше об использовании аккаунта

Телефон или адрес эл. почты

Забыли адрес электронной почты?

Создать аккаунт

Далее

Войдите в свой «родительский»»

Google

Аккаунт родителя

Переход в приложение "Family Link"

Войдите в аккаунт Google, с помощью которого вы будете управлять аккаунтом вашего ребенка.

Телефон или адрес эл. почты

Забыли адрес электронной почты?

Прежде чем начать работу с приложением "Family Link", вы можете ознакомиться с его политикой конфиденциальности и условиями использования.

Далее



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 «l» (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

Four browser address bars are shown, each with a URL and a description of the site's legitimacy:

- 1. URL: `http://click.alphabank.ru` (red underline under 'a'). Description: *мошенники В Альфа.Клик*
- 2. URL: `https://click.alfabank.ru/` (green underline under 'a'). Description: *правильный сайт Альфа.Клик*
- 3. URL: `vkonaktte.ru` (red underline under 't'). Description: *лишняя буква "t" сайт ВКонтакте*
- 4. URL: `rzd.info` (red underline under 'o'). Description: *должно быть rzd.ru сайт РЖД*



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

Скриншот интерфейса «Госуслуги» для восстановления пароля. Вверху логотип «госуслуги». Заголовок: «Восстановление пароля». Поле ввода: «Телефон / Email» с номером «89000000000».

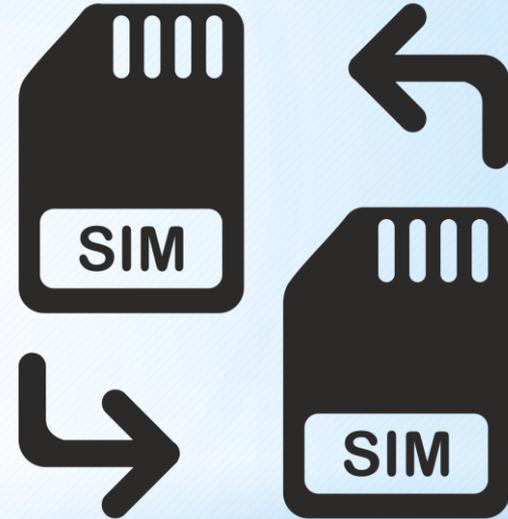
Скриншот интерфейса «Госуслуги» для изменения номера телефона. Вверху логотип «госуслуги». Заголовок: «Изменение номера телефона +7 924». Поле ввода: «Новый номер телефона» с префиксом «+7 () - - -».



2. Переоформление SIM-карты

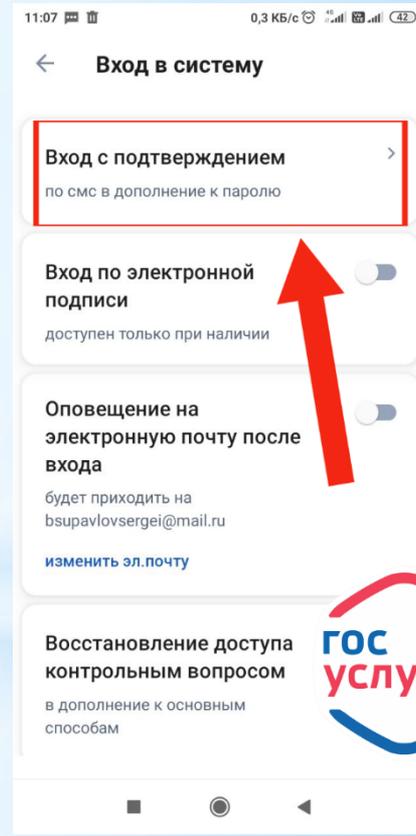
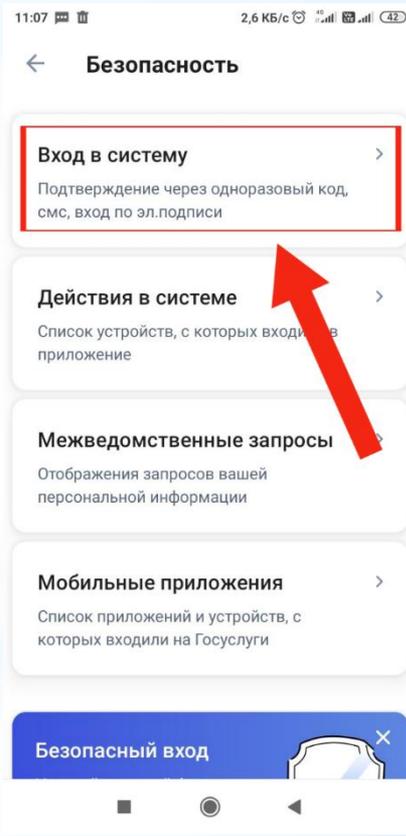
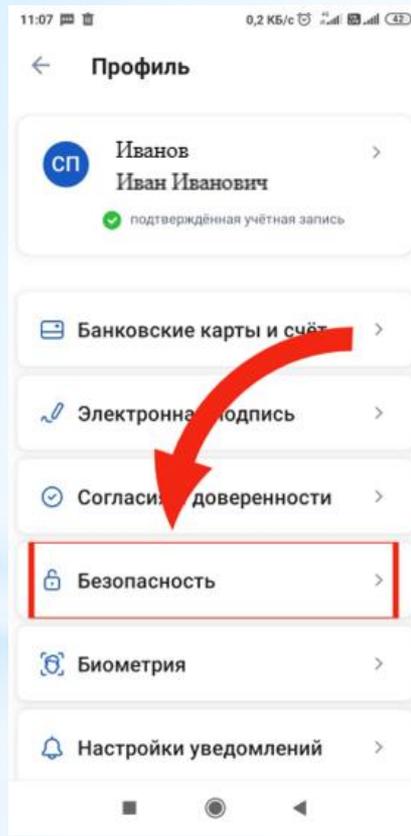
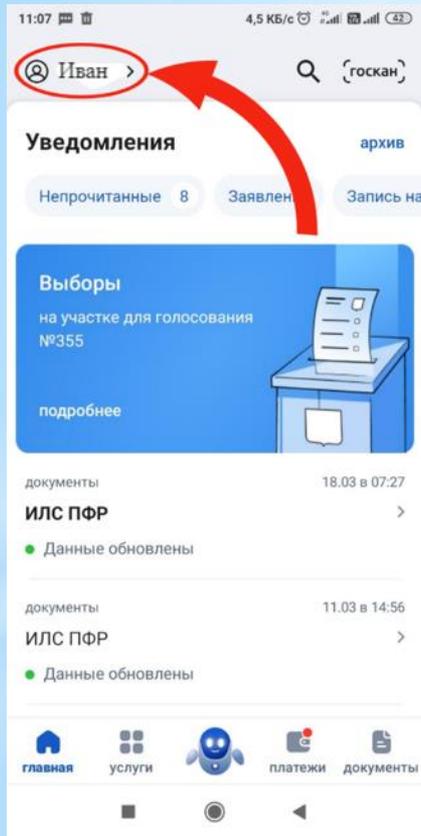
- SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

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.



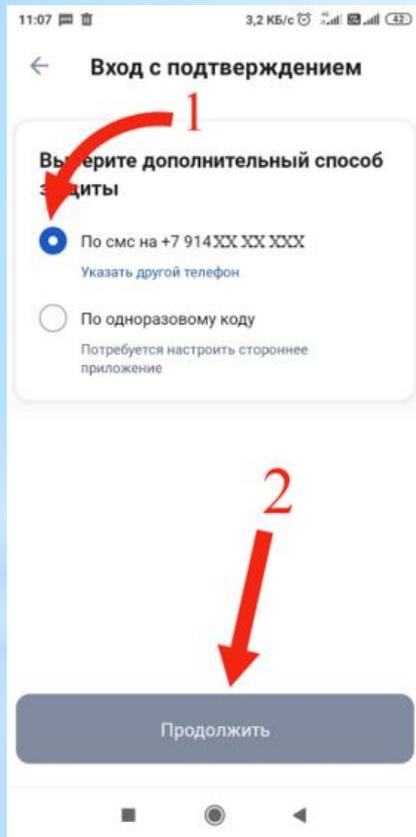


Дополнительная защита личного кабинета





Дополнительная защита личного кабинета



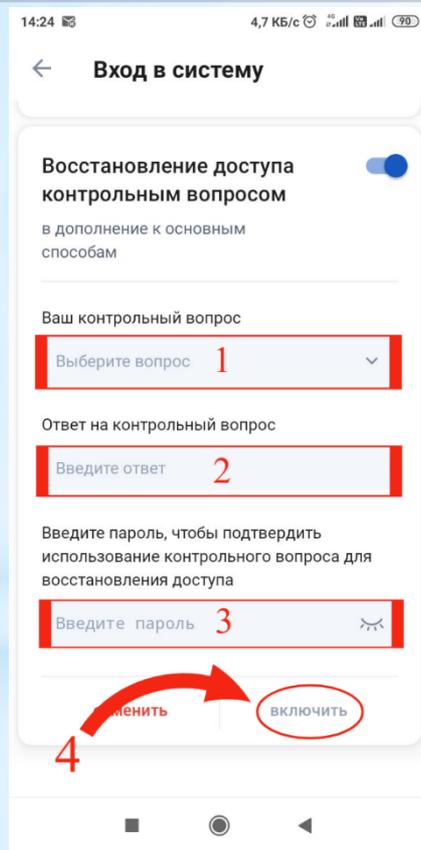
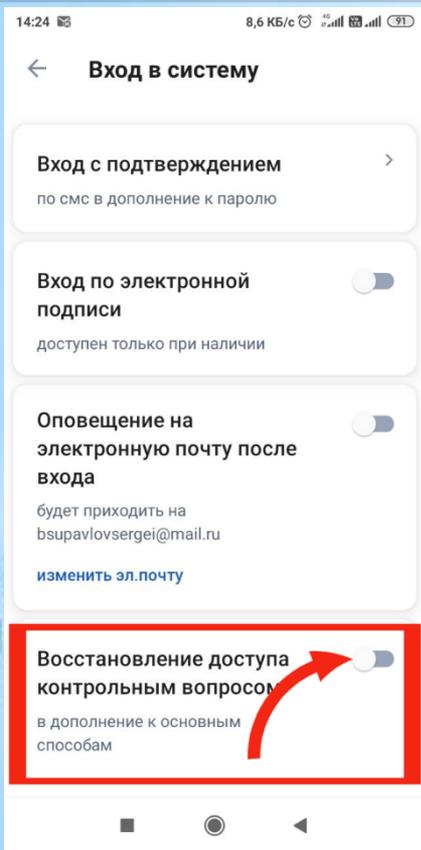
Функция входа с двухэтапной аутентификацией.

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.





**Мошенники
взломали личный кабинет
портала «Госуслуги»**



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.

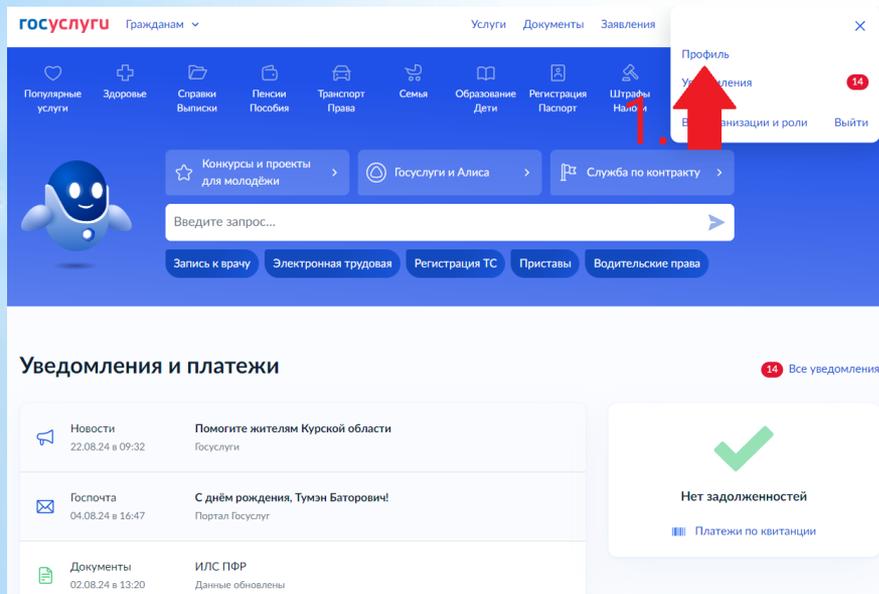
Возьмите с собой паспорт и СНИЛС



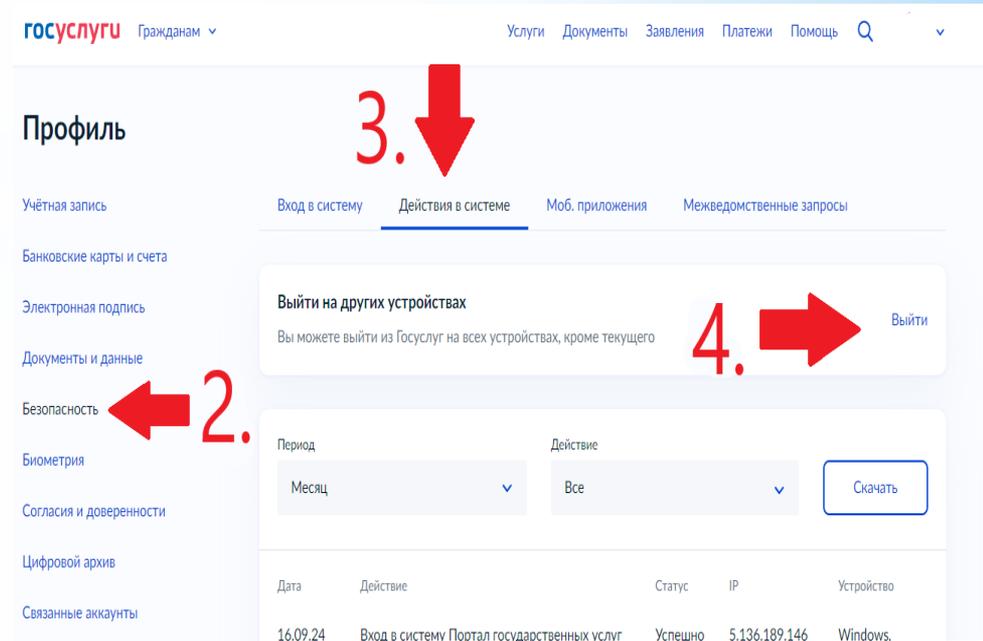
Определите, где использовалась учетная запись

Вы можете выйти одновременно на всех устройствах, кроме текущего

НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ:



The screenshot shows the main interface of the Gosuslugi portal. At the top, there is a navigation bar with 'Услуги', 'Документы', and 'Заявления'. Below it is a grid of service icons. A red arrow points to the 'Профиль' (Profile) icon in the top right corner of the main menu.

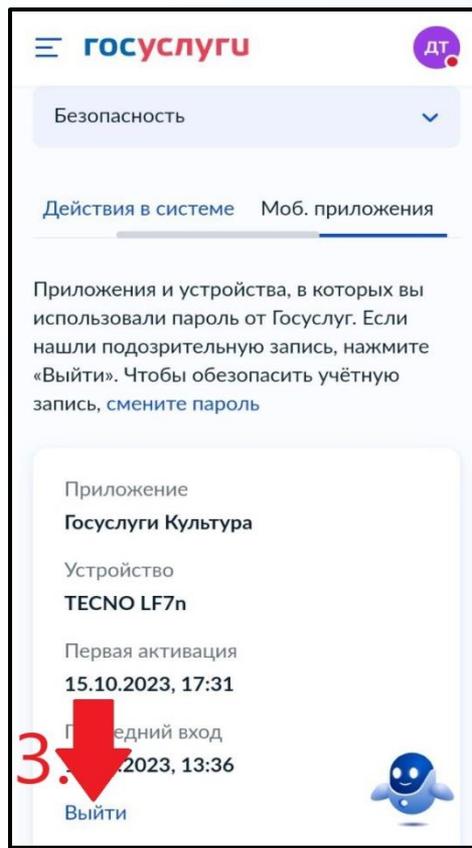
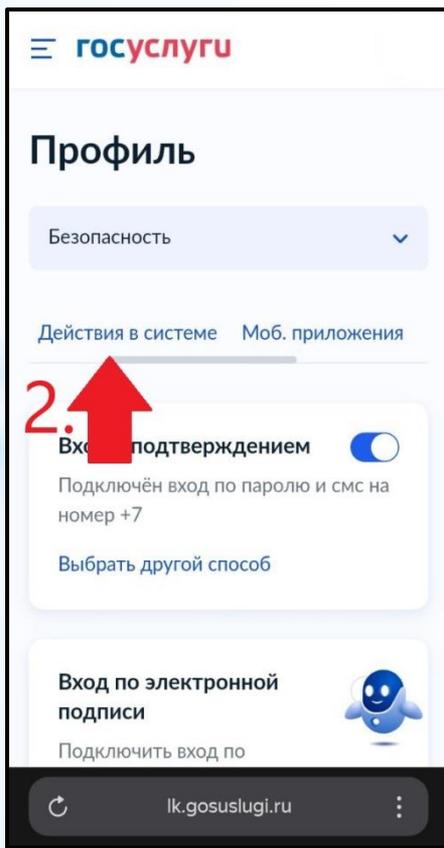
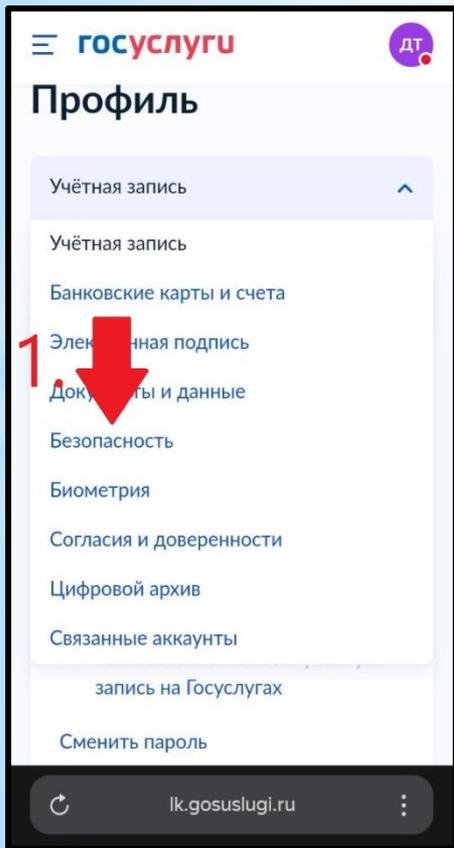


The screenshot shows the 'Профиль' (Profile) page. A red arrow labeled '2.' points to the 'Безопасность' (Security) link in the left sidebar. A red arrow labeled '3.' points to the 'Действия в системе' (System actions) tab. A red arrow labeled '4.' points to the 'Выйти' (Logout) button in the 'Выйти на других устройствах' (Logout on other devices) section.

Выйти на других устройствах
Вы можете выйти из Госуслуг на всех устройствах, кроме текущего

Период	Действие	Статус	IP	Устройство
Месяц	Все			
16.09.24	Вход в систему Портал государственных услуг	Успешно	5.136.189.146	Windows

НА МОБИЛЬНОМ ТЕЛЕФОНЕ



Отзовите разрешения, которые не выдавали.

Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени.



Обратитесь в полицию и подайте заявление.

При наличии данных, указывающих на совершение противоправных действий, в том числе связанных с мошенничеством, подайте заявление в полицию.

Возьмите с собой копию заявления из МФЦ, скриншоты СМС – сообщений и другие доказательства.





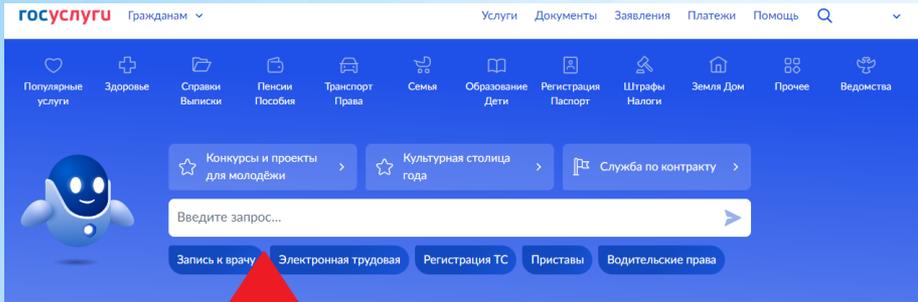
Проверьте кредитную историю и узнайте, направлялись ли от вашего имени заявки на займы

Выясните, в каких бюро хранится ваша кредитная история (их может быть несколько).

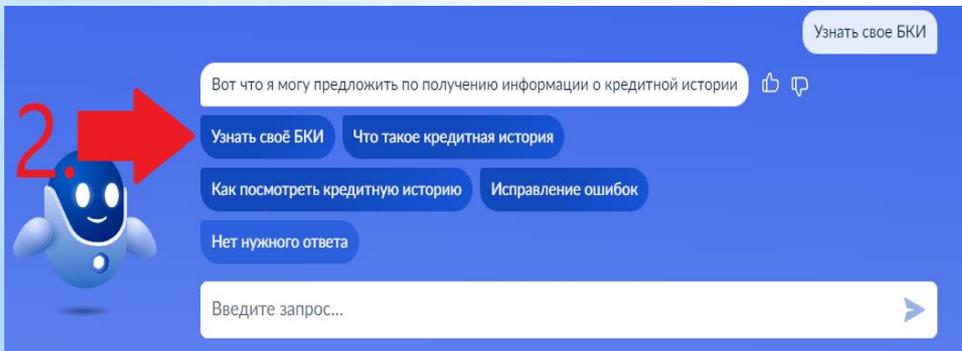
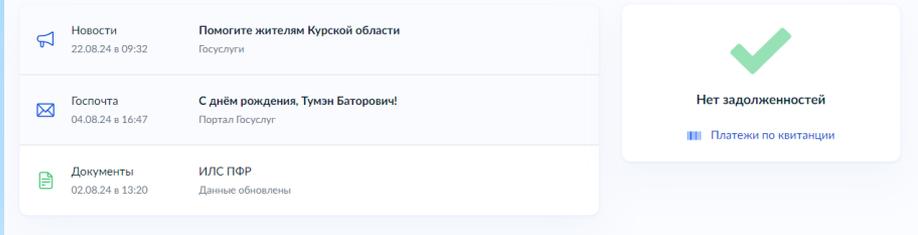
Сделать это можно на портале «Госуслуги»:

1. Введите в строке поиска запрос «узнать свое БКИ».
2. Далее зарегистрируйтесь на сайте каждого бюро* и запросите свою кредитную историю (рекомендуем направить запрос через 2 недели после взлома аккаунта).

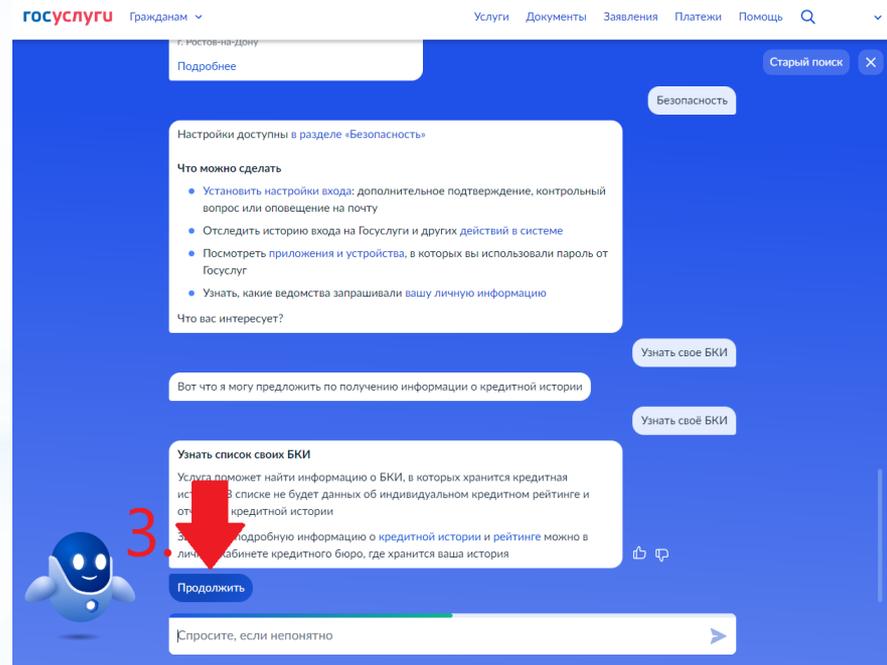
*Можно авторизоваться с помощью учетной записи «Госуслуги».



Уведомления и плат



Узнать на портале «Госуслуги» в каких бюро хранится ваша кредитная история.





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.

