ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ

Популярные схемы мошенничества

«По старинке»

Звонки от имени сотрудников банков, правительственных организаций и компаний — с запросом личной информации, номеров банковских карт

Мессенджеры

Подложная персона, действующая по сценарию. Цель — получение компьютерной информации

Взлом личных кабинетов и аккаунтов

Злоумышленники получают смс-код для взлома и доступа к личному кабинету Госуслуг, моб. банков и соцсетей

Фишинг

Наиболее популярный способ. Получение паролей, пин-кодов, в том числе при помощи подложных ссылок

Иные

в том числе

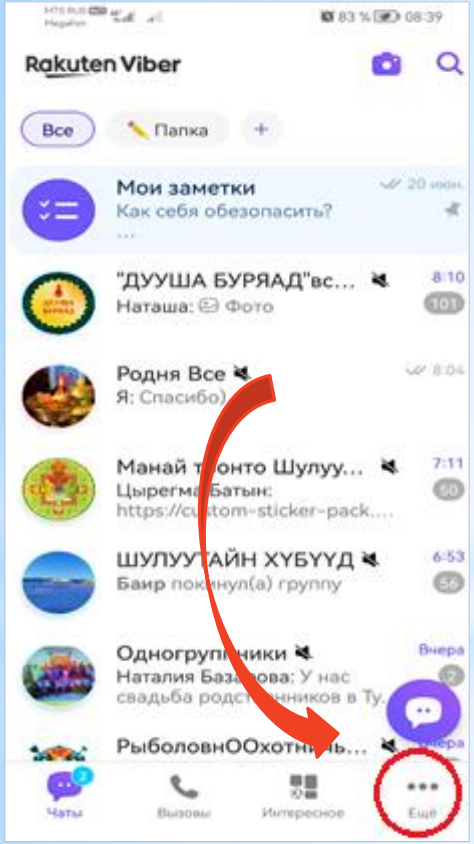
- кражи денеж. средств
- вымогательства
- «ложные» минирования\

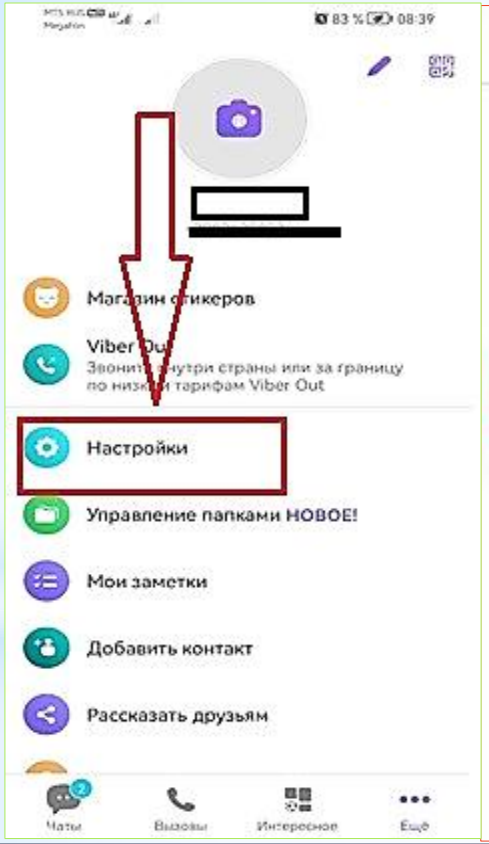
КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

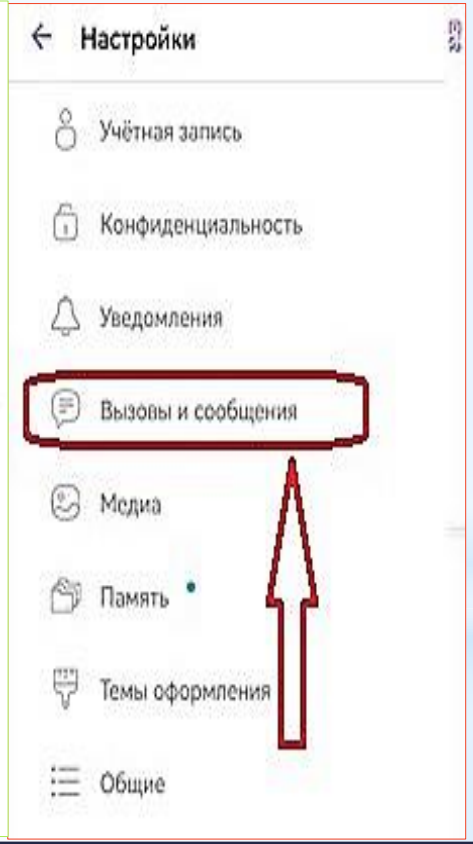
1. **Не отвечайте**
   на звонки с незнакомых номеров
2. **Прервите разговор**
   Если он касается финансовых вопросов
3. **Не торопитесь**
   принимать решение
4. **Проверьте информацию в Интернете**
   или обратитесь за помощью к близким родственникам
5. **Не перезванивайте**
   по незнакомым номерам
6. **Самостоятельно позвоните**
   близкому человеку /в банк / в организацию
7. **Не сообщайте**
   CVV/CVC и иные данные банковских карт

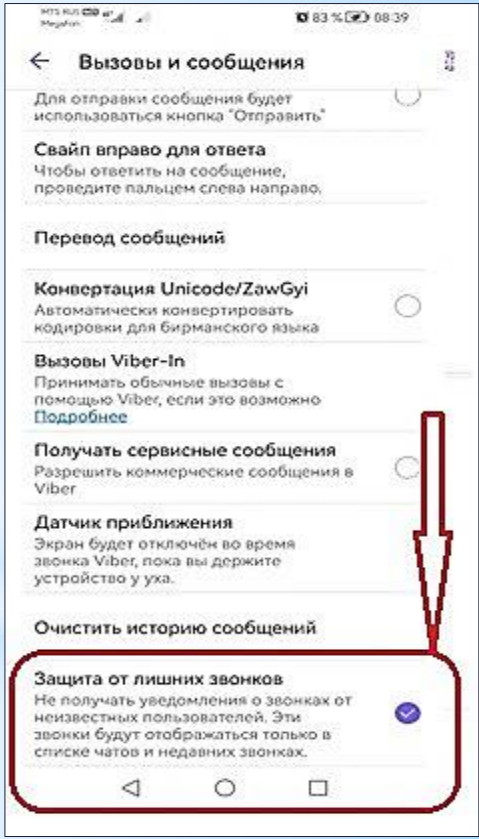
Возьмите паузу и спросите совета у родных и друзей!

Защита от звонков в Viber

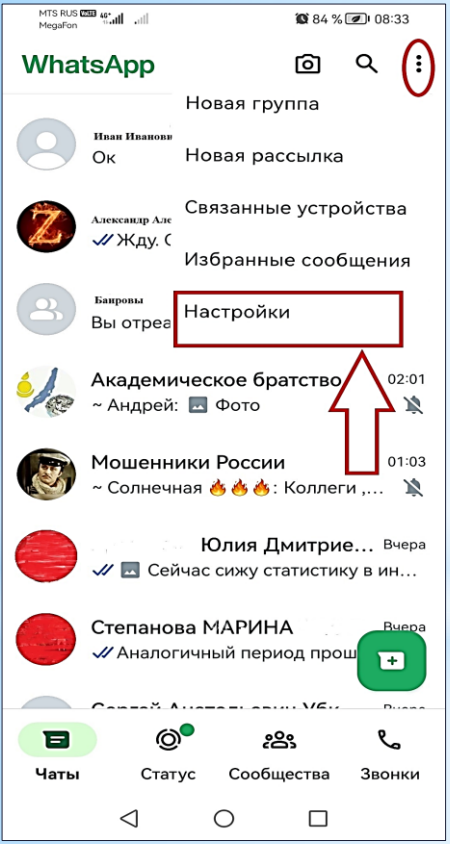


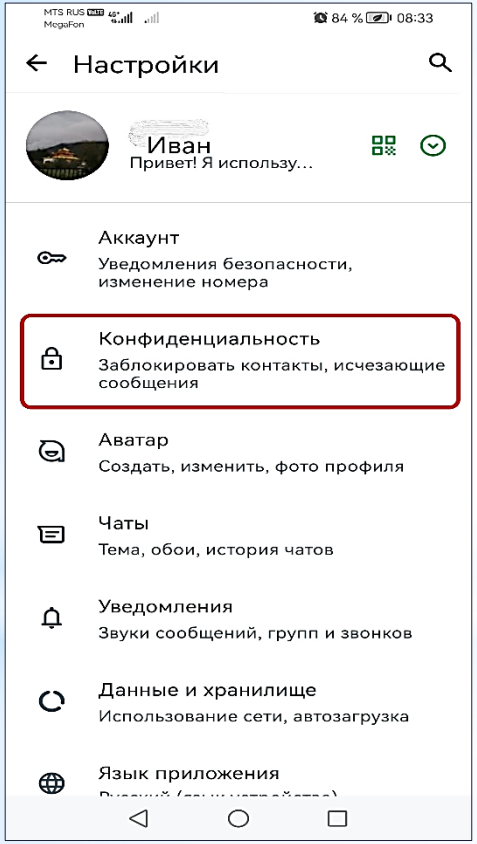


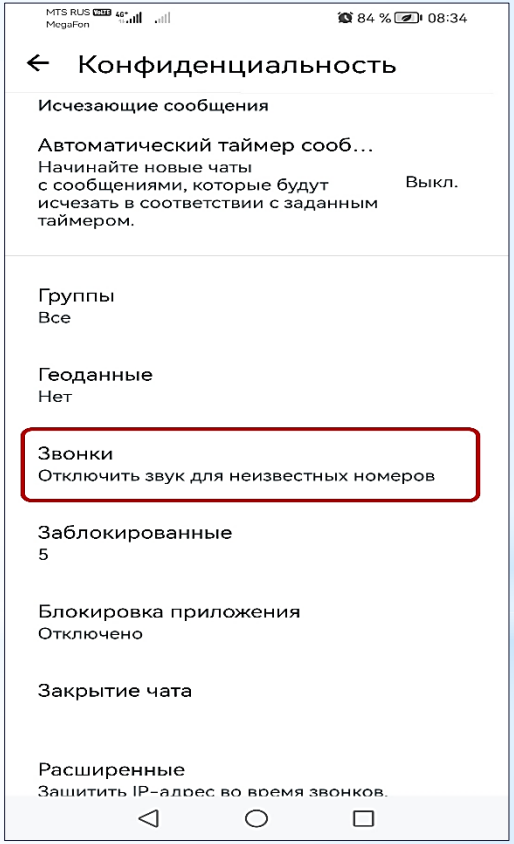


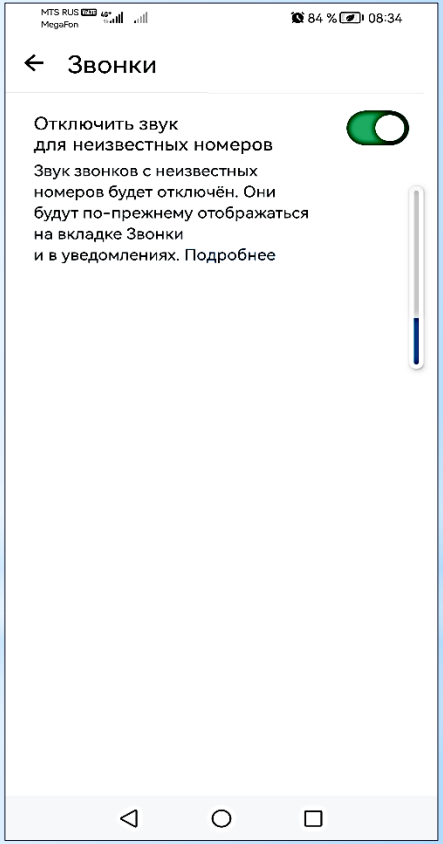


Защита от звонков в WhatsApp

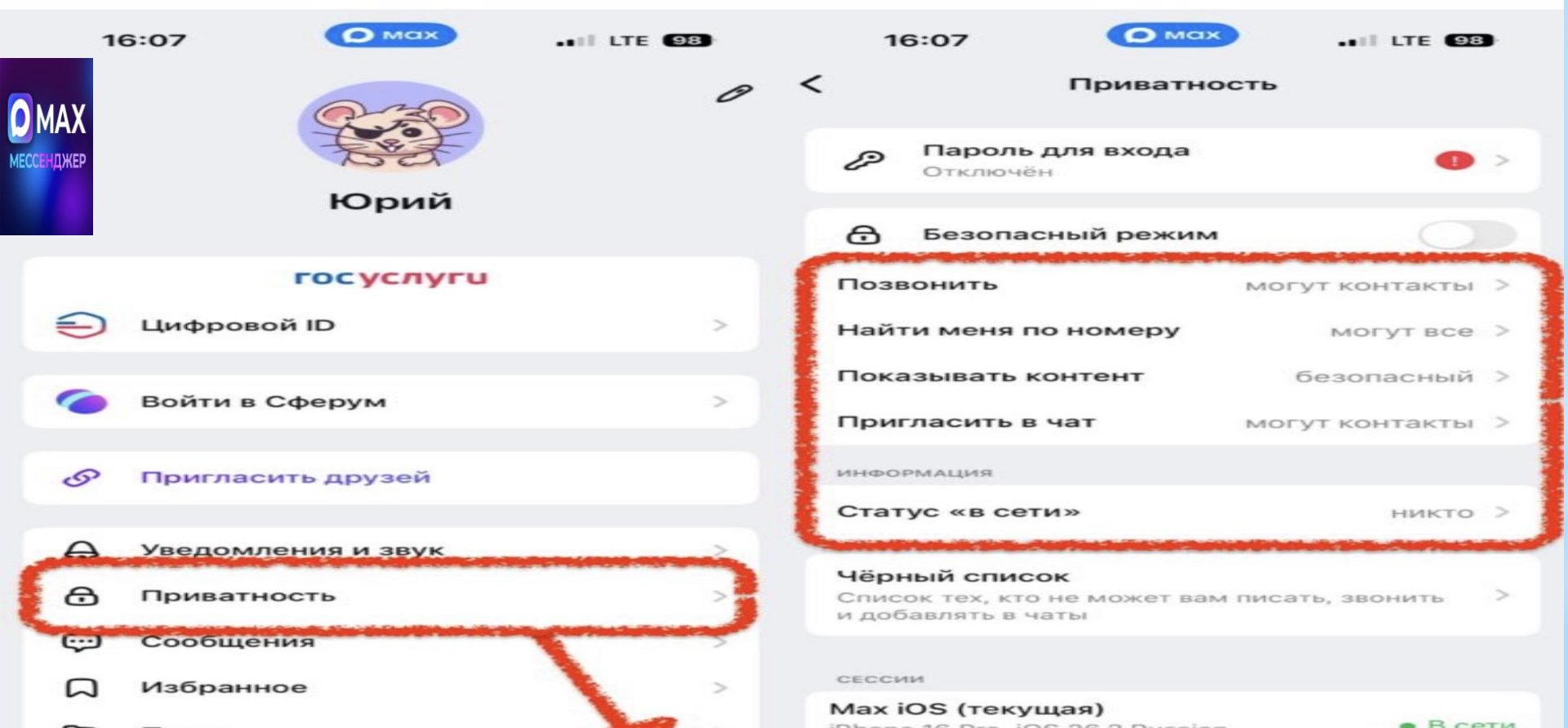




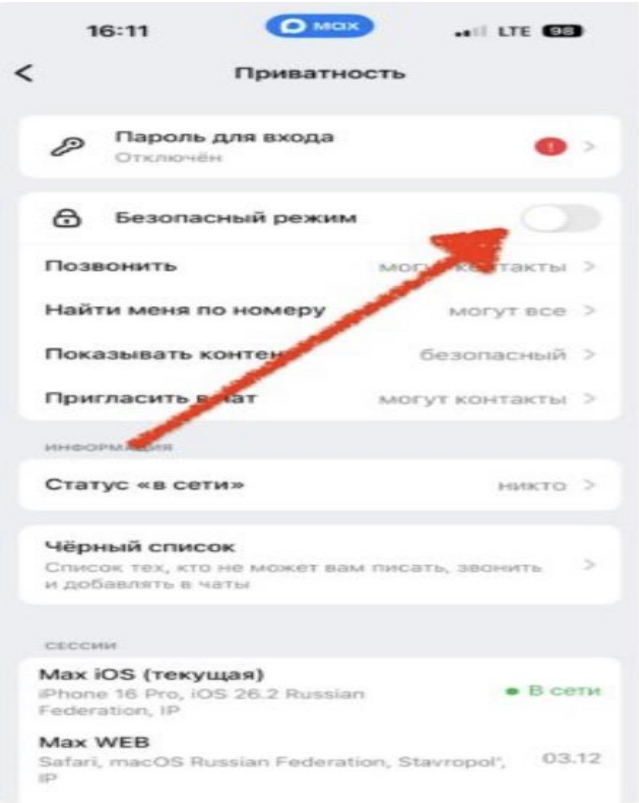


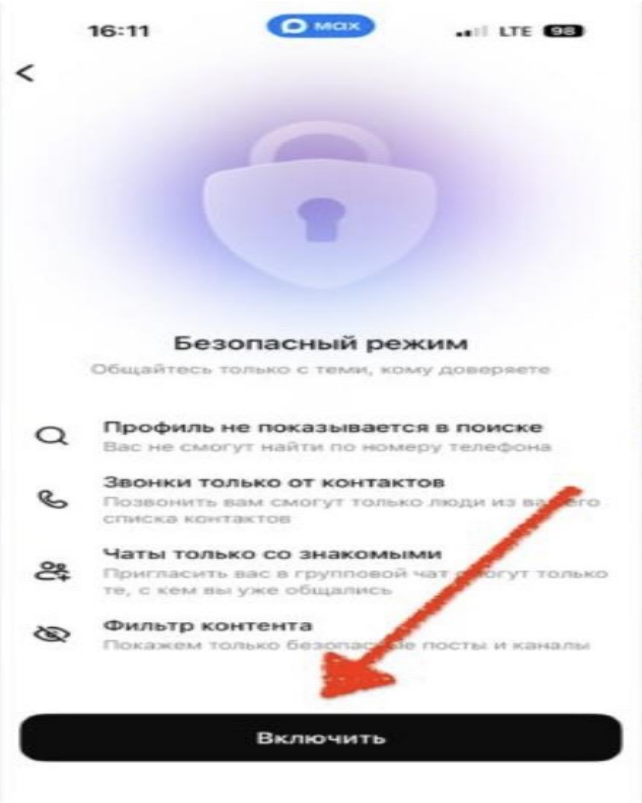


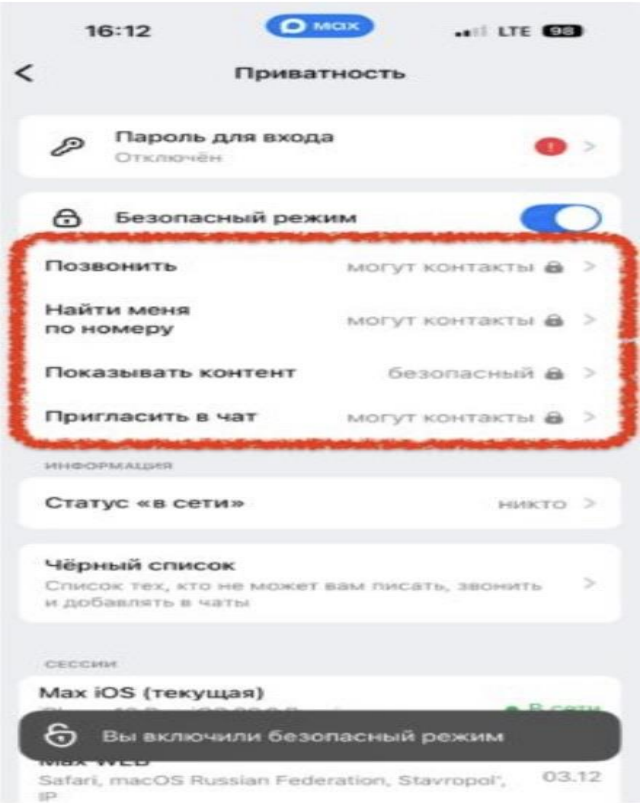
Как сделать общение в MAX безопасным



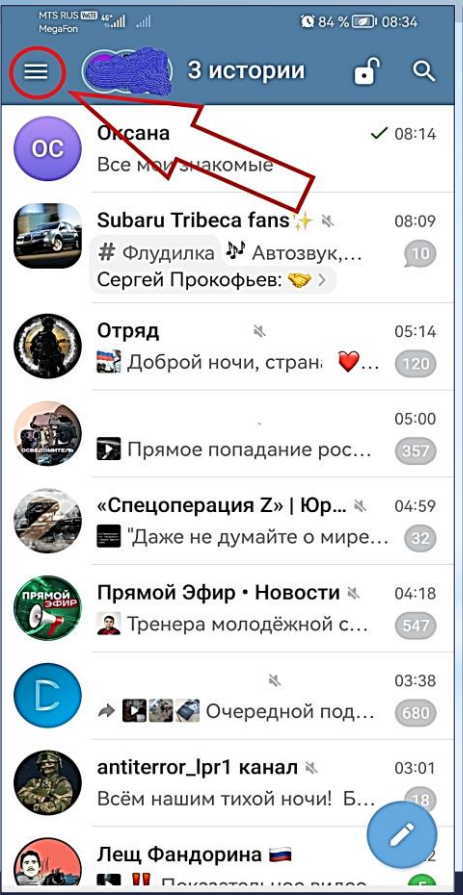
Как сделать общение в MAX безопасным

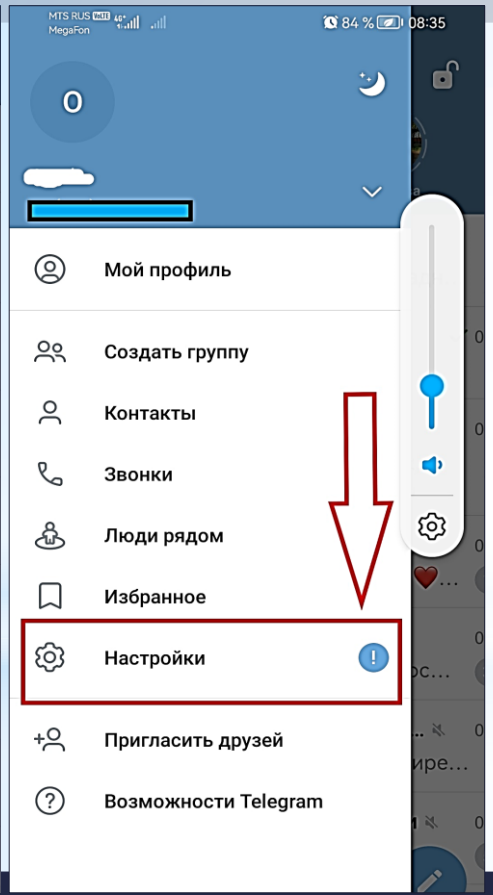


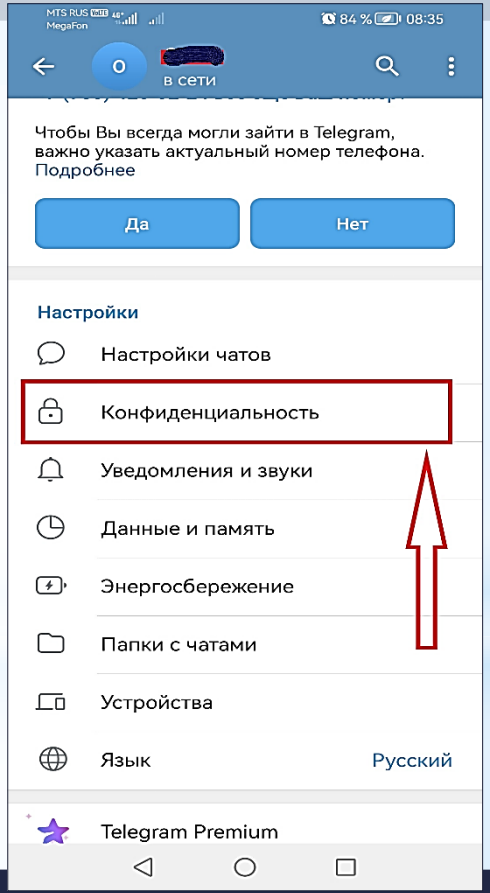


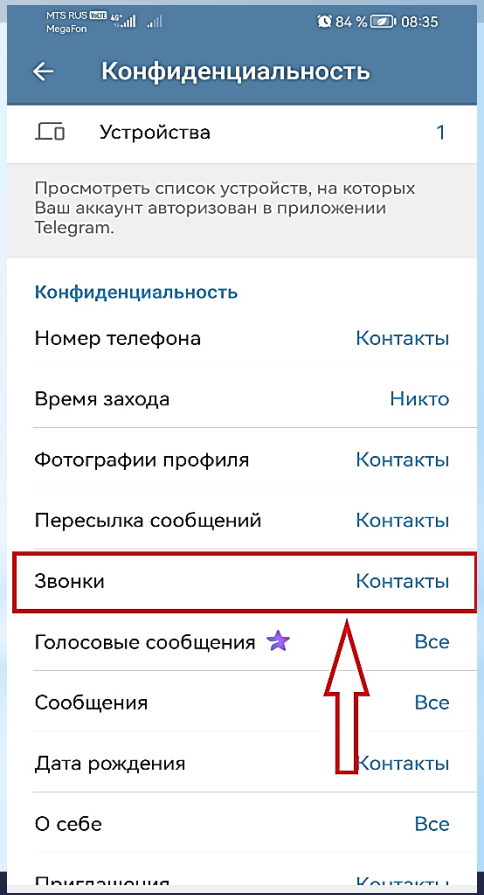


Защита от звонков в Telegram

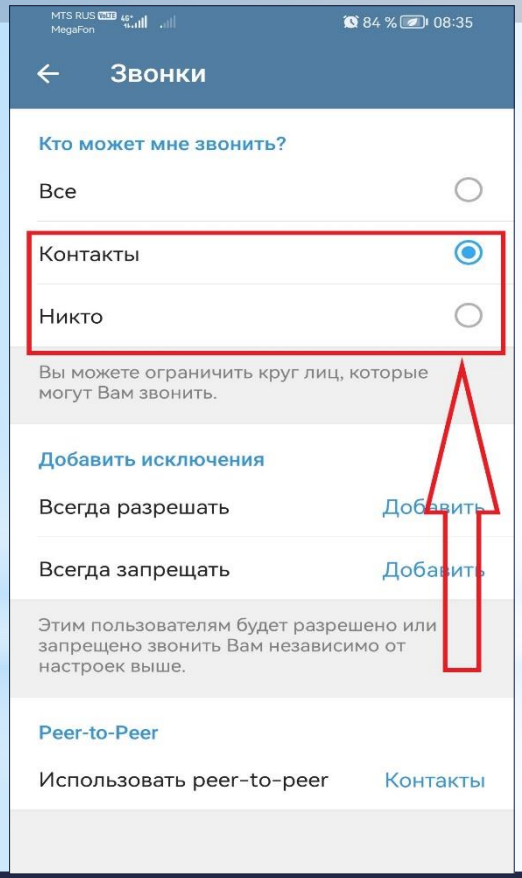


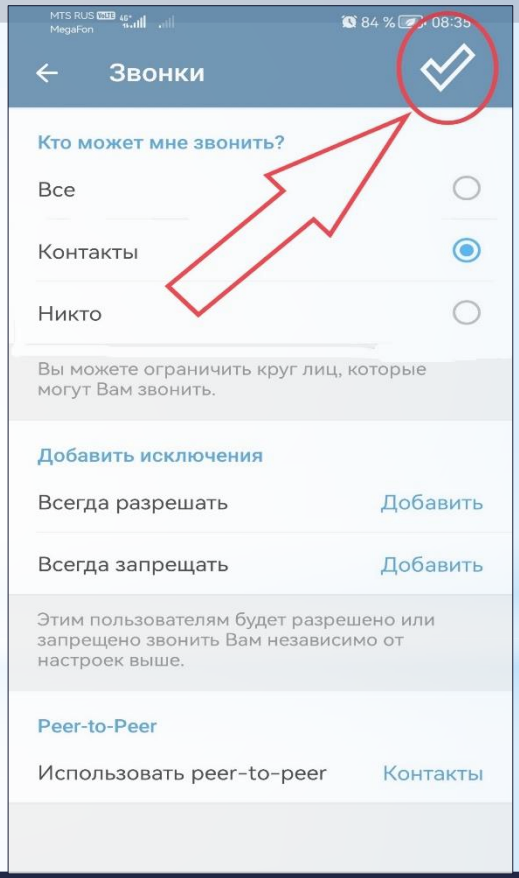




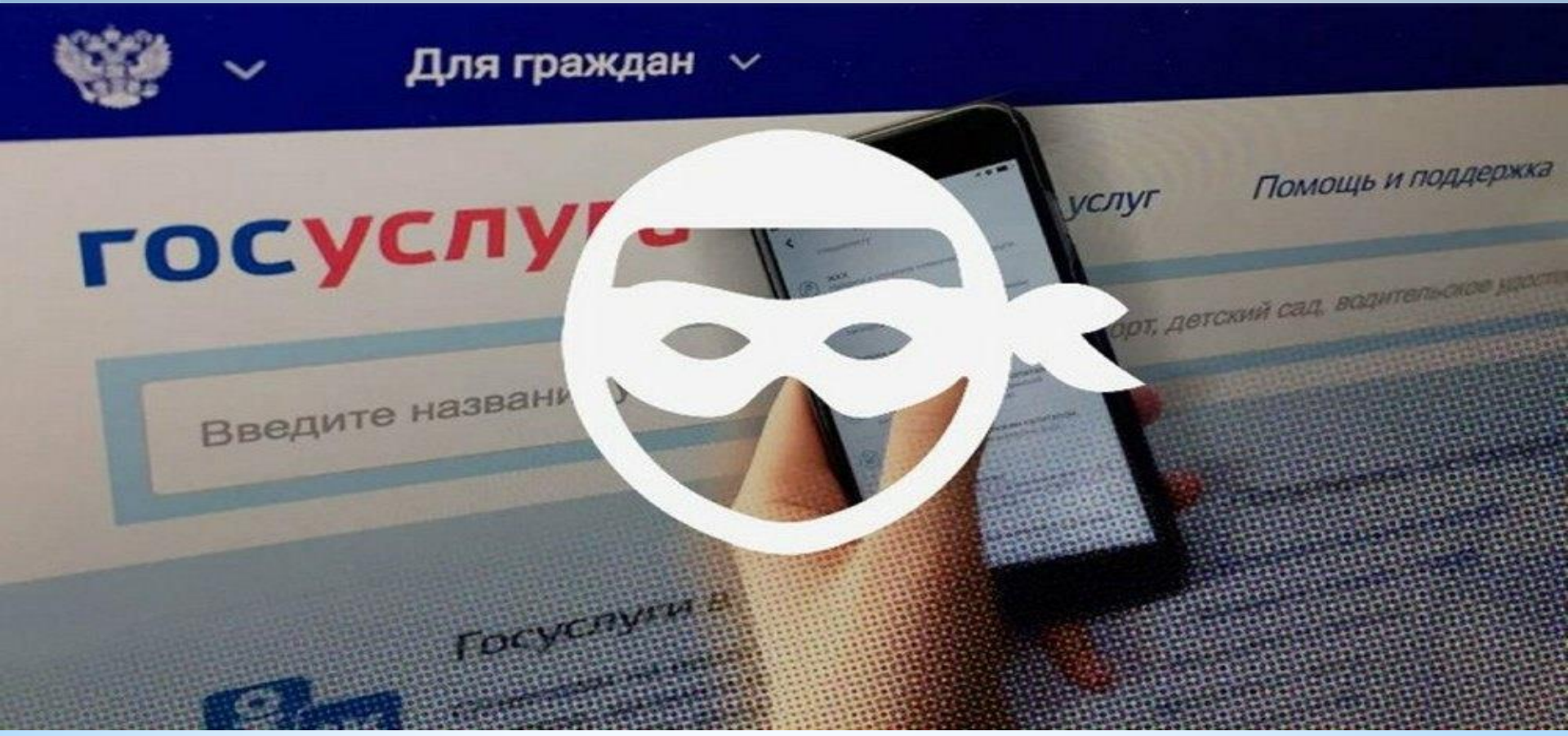


Защита от звонков в *Telegram*





Взлом личного кабинета Госуслуг

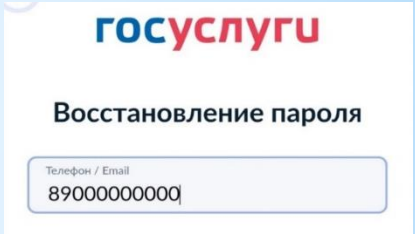


1. Звонок от работника сотового оператора

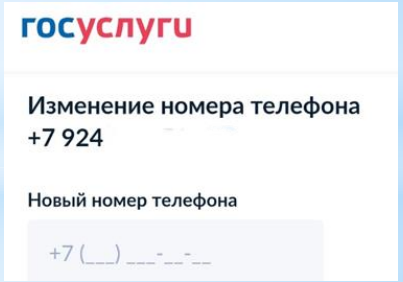
1. Поступает телефонный звонок от оператора сотовой связи, сообщают что необходимо продлить срок действия SIM-карты или обновить паспортные данные.

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.



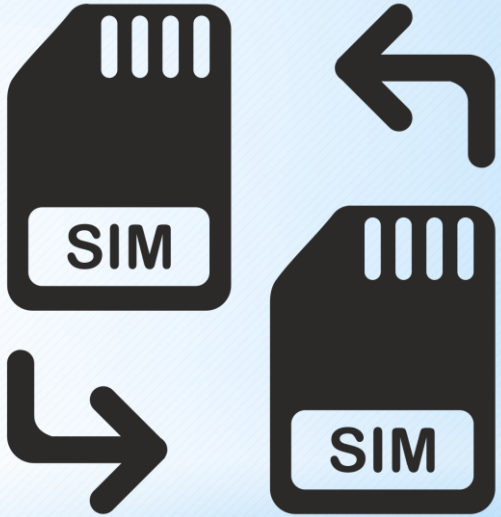
- Для личных кабинетов, где установлен вход на портал по SMS-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. На самом деле повторно приходит КОД для изменения номера телефона.



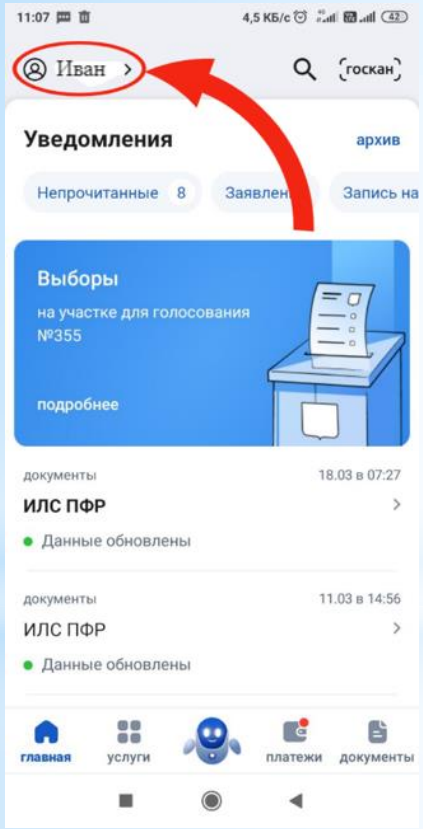
2. Переоформление SIM-карты

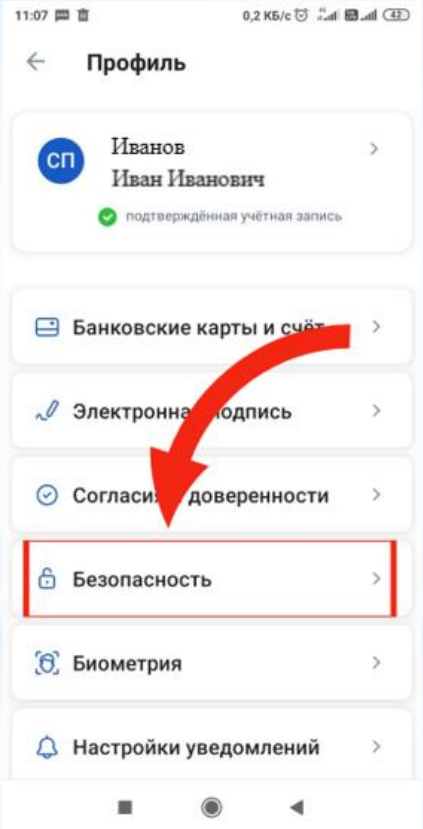
- SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

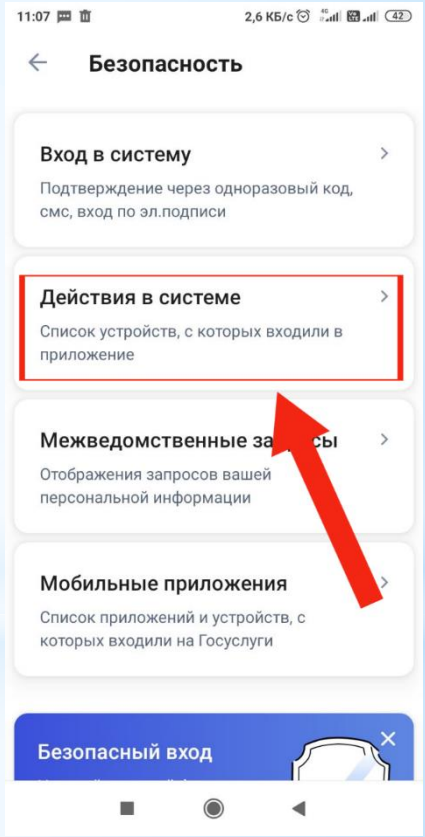
  Тем самым, предоставляя возможность новому пользователю восстановить доступ к личному кабинету от портала «Госуслуги», путем ввода SMS-кодов, поступивших на перевыпущенный номер SIM-карты, что и делают злоумышленники.



Признаки взлома личного кабинета портала «Госуслуги»



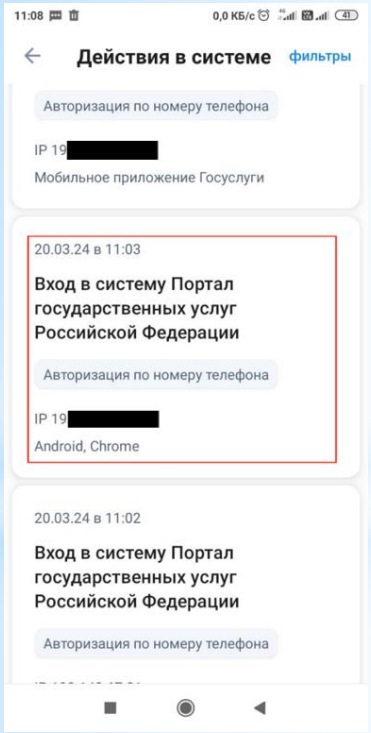




гос услуги

Признаки взлома личного кабинета портала «Госуслуги»

Без признаков взлома



С признаками взлома

2023-09-01T19:06:17.120 +0300	Вход в систему Vivus.SMSFinance. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:54:47.939 +0300	Вход в систему Портал государственных услуг Российской Федерации. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:51:03.165 +0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:45:07.170 +0300	Вход в систему ООО МФК "ВЭББАНКИР". Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:44:10.675 +0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49

Как обезопасить личный кабинет от взлома?

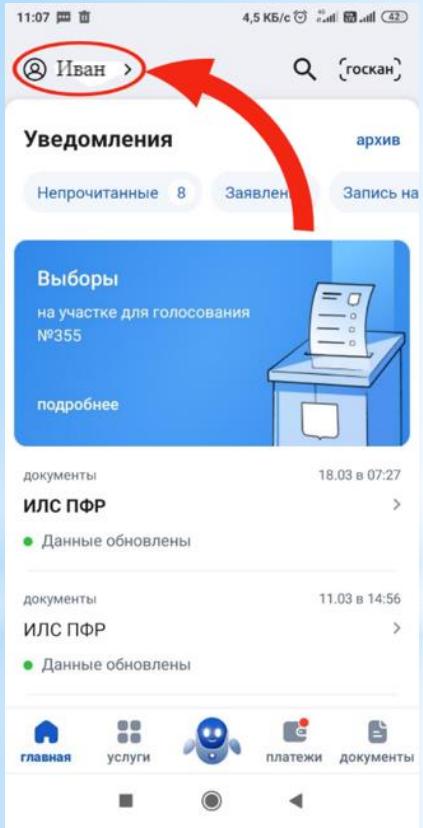
1. Никому не сообщайте код из SMS-сообщения, поступившего с портала «Госуслуги»;

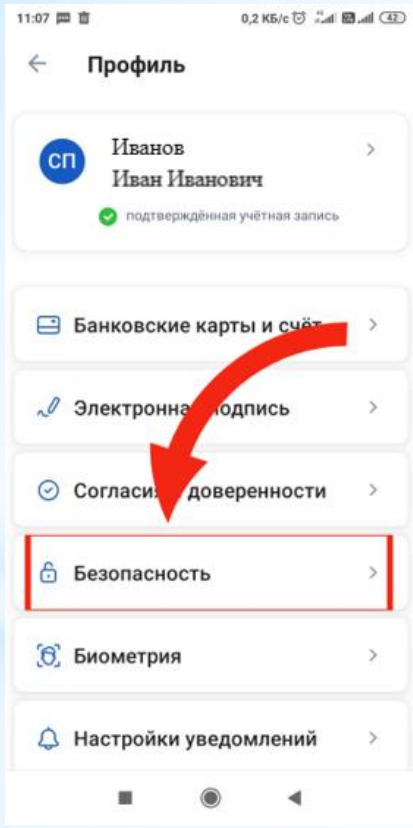
2. Настроить двухэтапную аутентификацию;

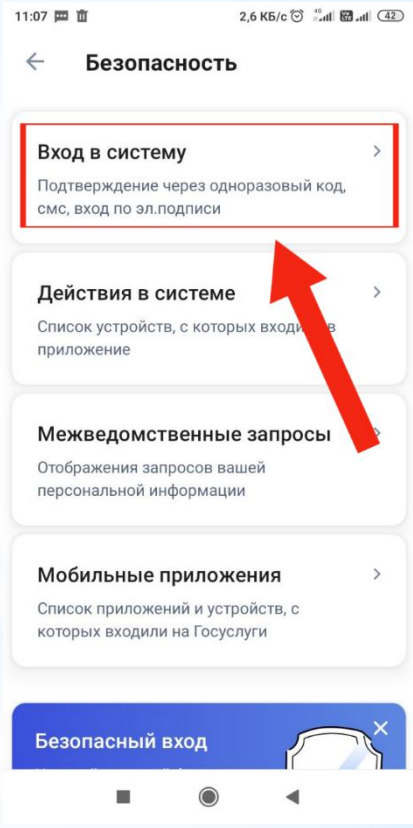
3. Отозвать неизвестные для вас согласия в личном кабинете;

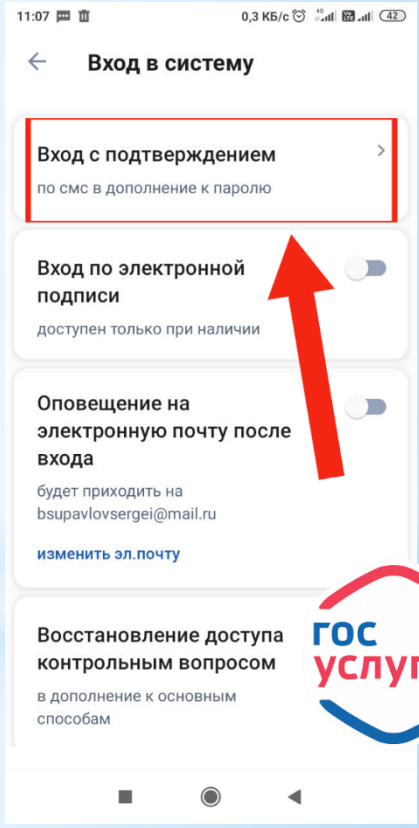
4. Регулярно, раз в полгода необходимо менять пароли доступа.

Дополнительная защита личного кабинета

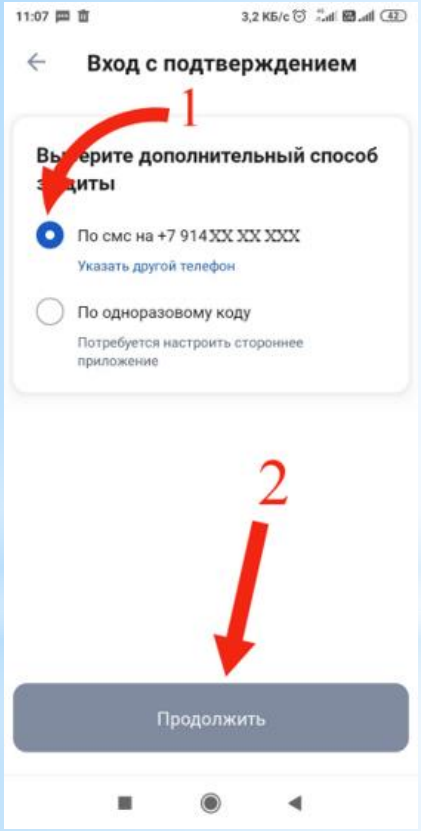








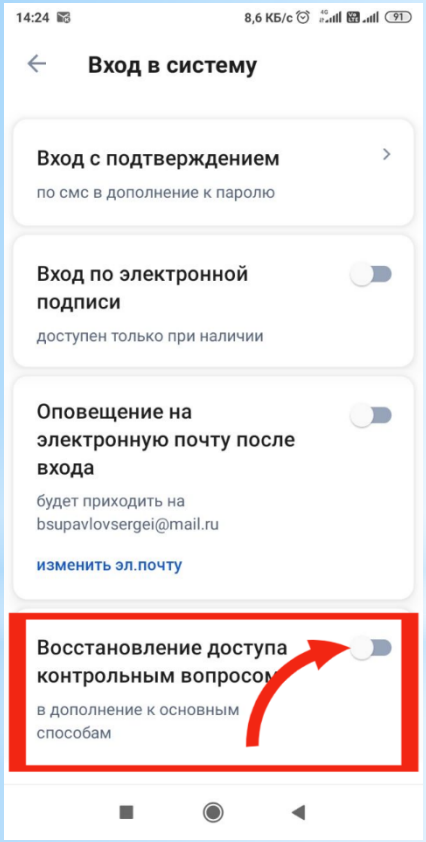
Дополнительная защита личного кабинета

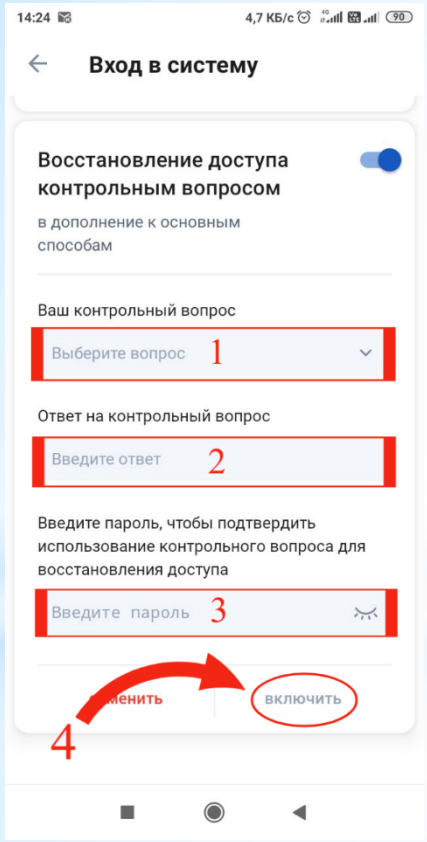


Функция входа с двухэтапной аутентификацией.

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

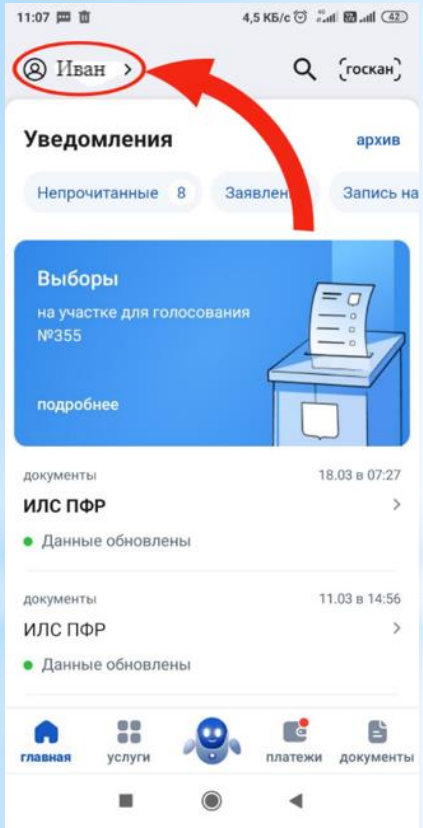


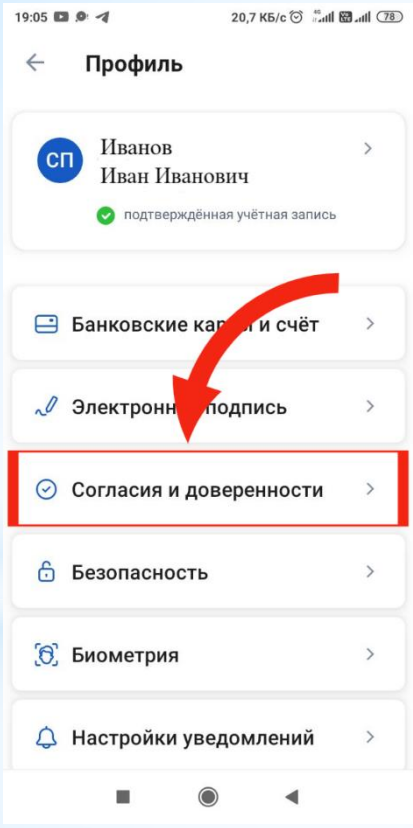


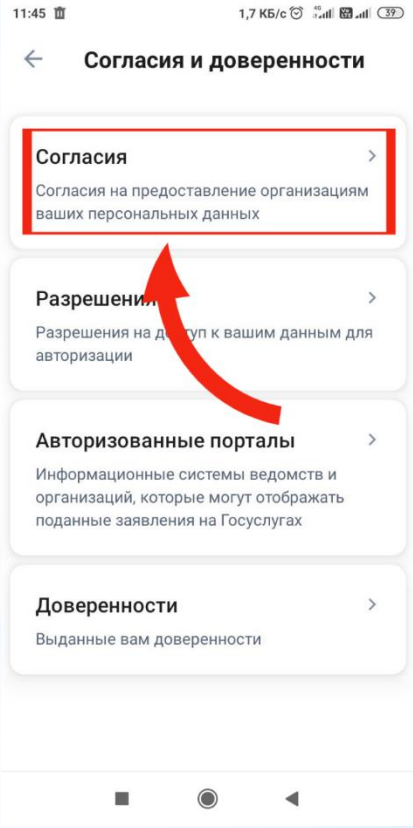
Функция восстановления доступа контрольным вопросом.

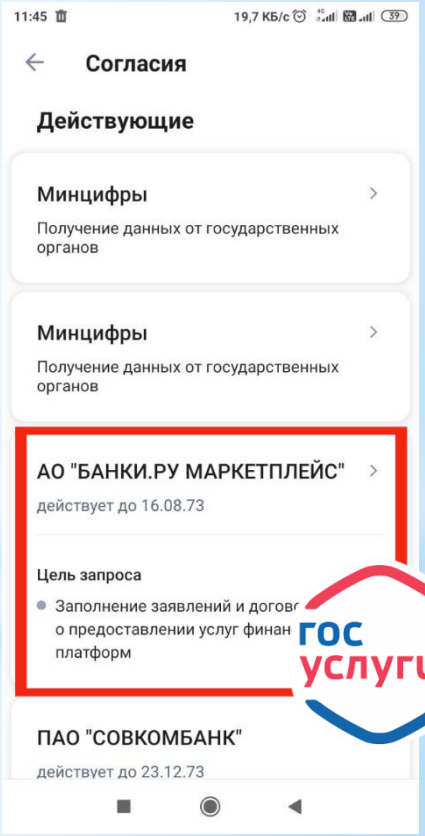
После переоформления SIM-карты, мошенники не смогут восстановить доступ к личному кабинету, так как они не знают ответ на контрольный вопрос.

Отзыв согласий

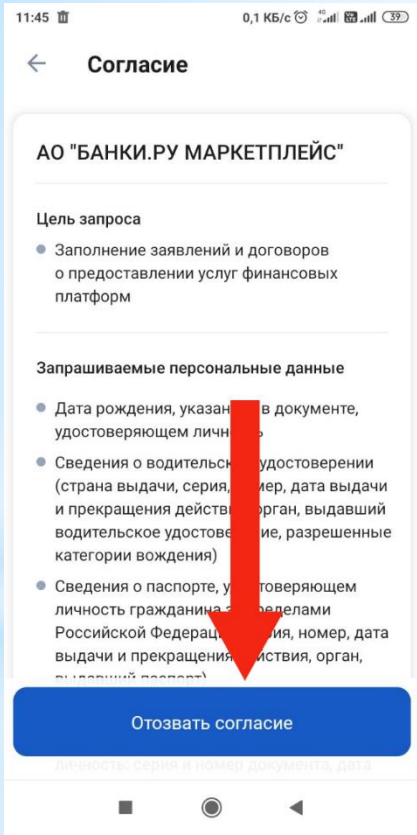


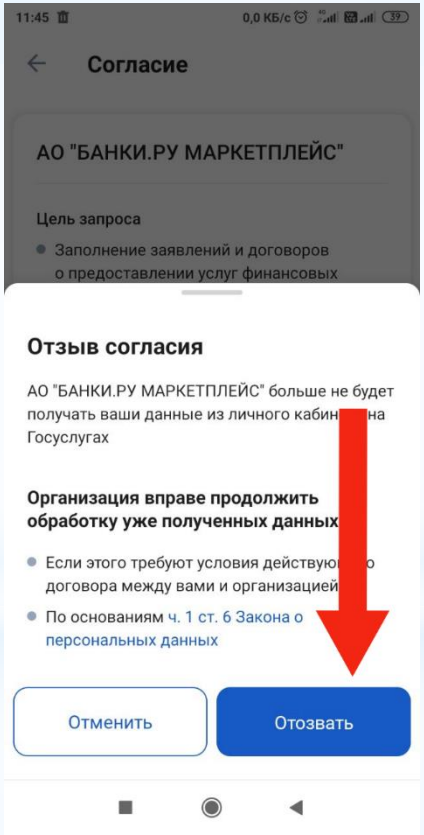


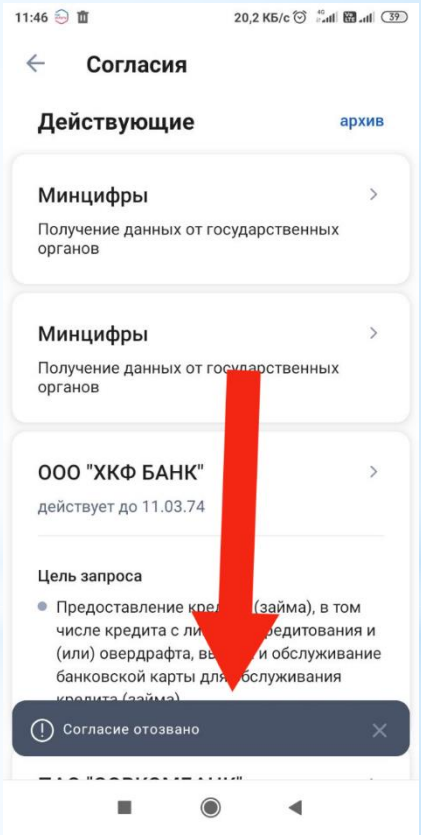




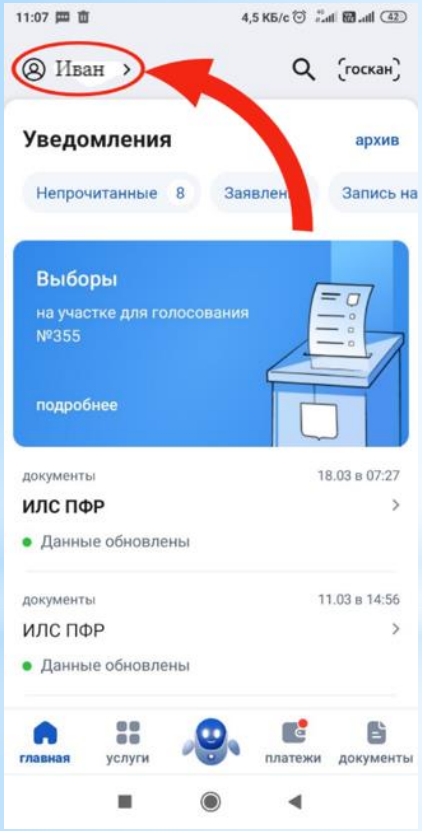
Отзыв согласий

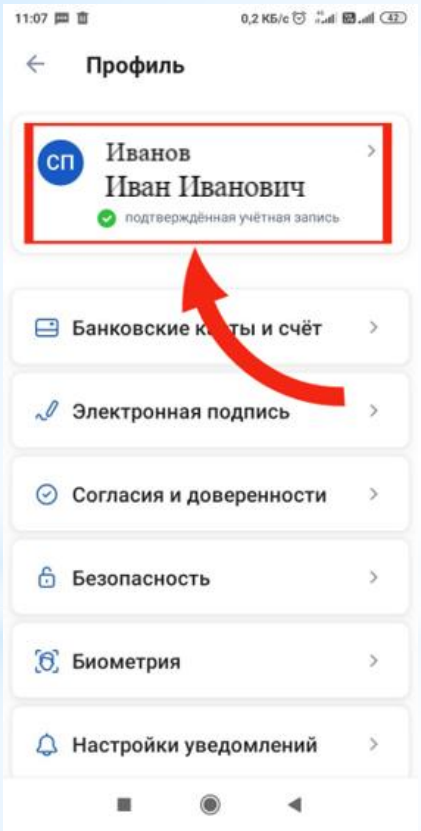


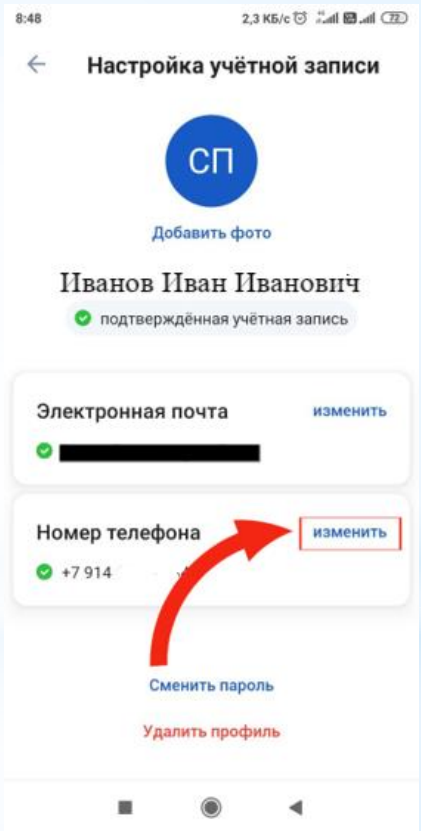


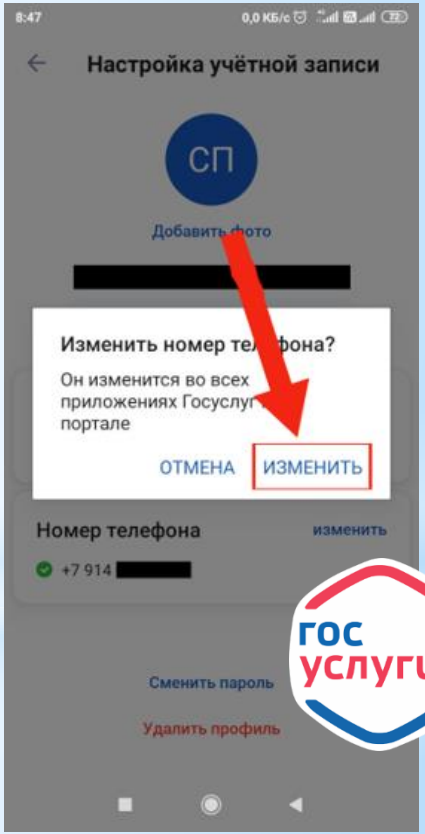


Способ открепления номера телефона





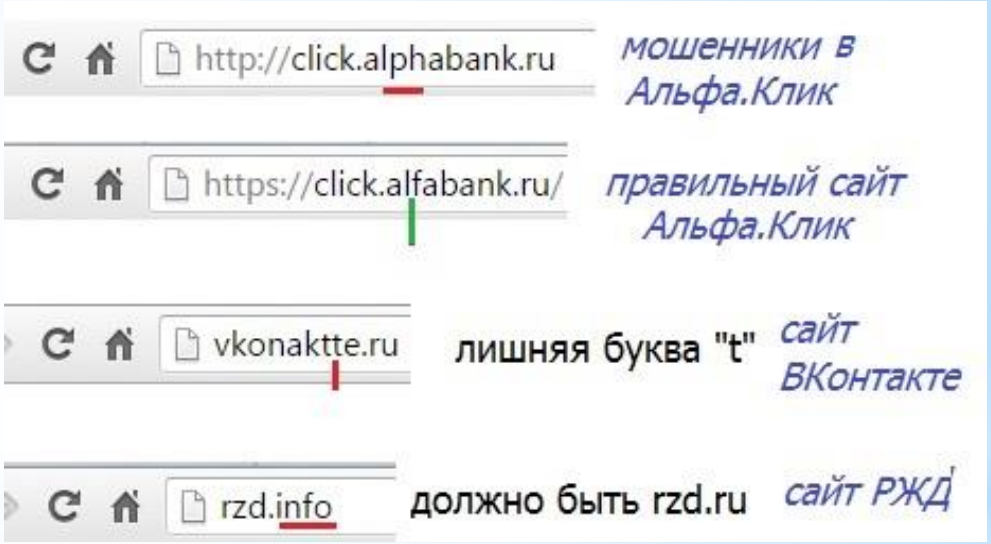




Способ открепления номера телефона

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**



УМВД России по Хабаровскому краю