



ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ



УМВД России по Хабаровскому краю



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



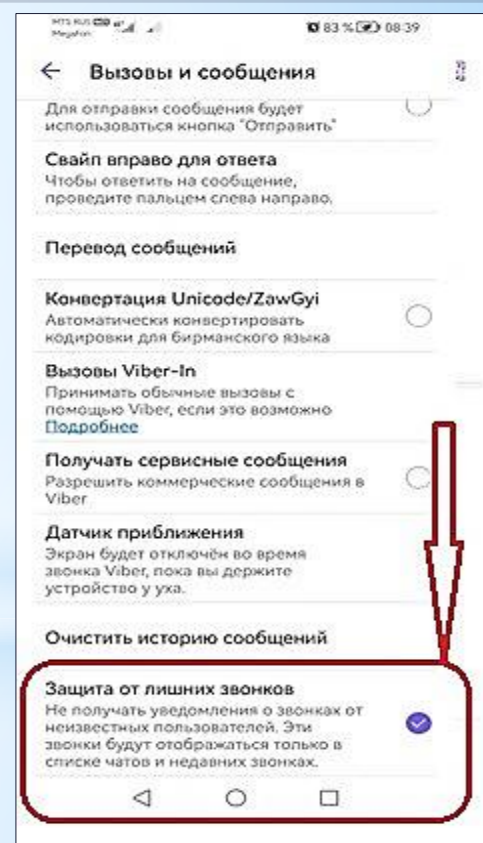
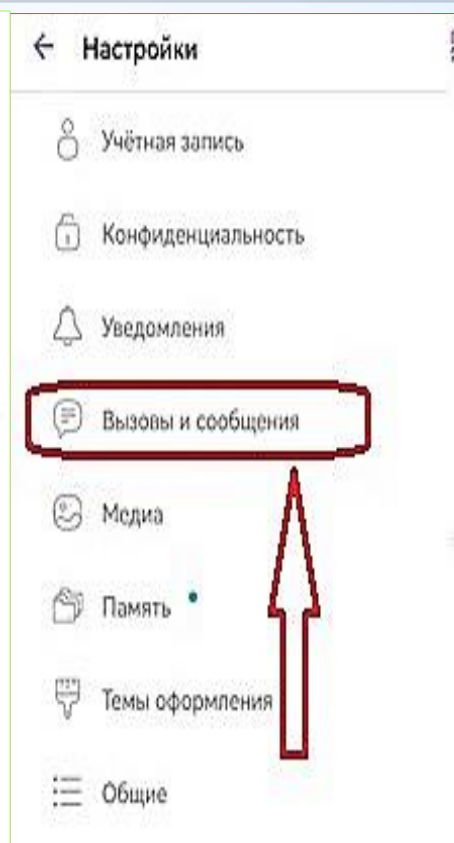
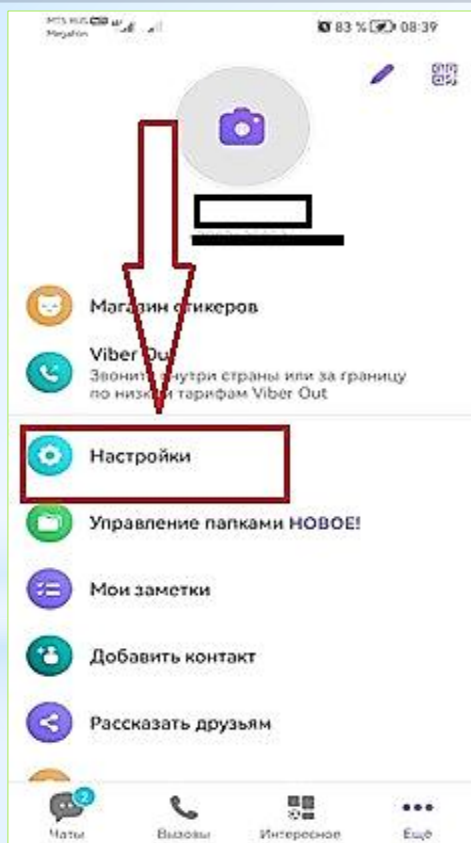
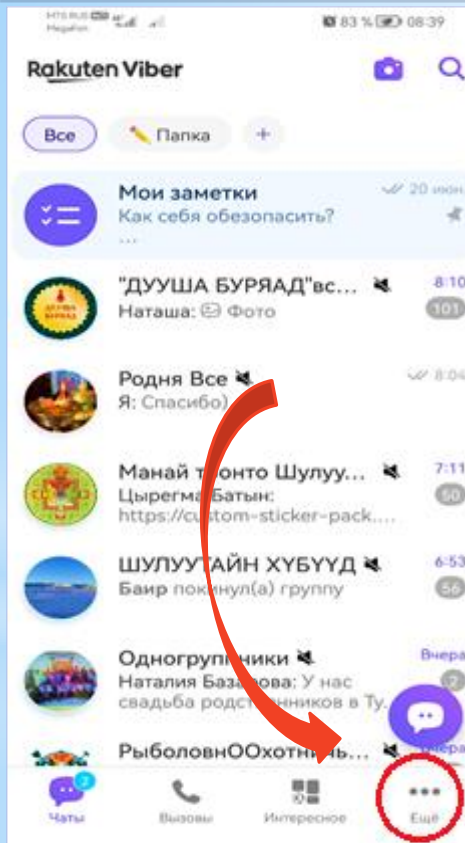
- 5** Не перезванивайте по незнакомым номерам
- 6** Самостоятельно позвоните близкому человеку / в банк / в организацию
- 7** Не сообщайте CVV/CVC и иные данные банковских карт



**Возьмите паузу
и спросите совета
у родных и друзей!**

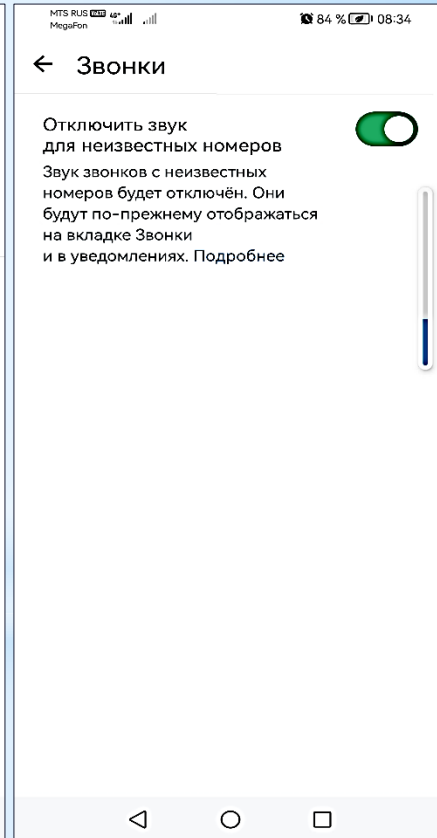
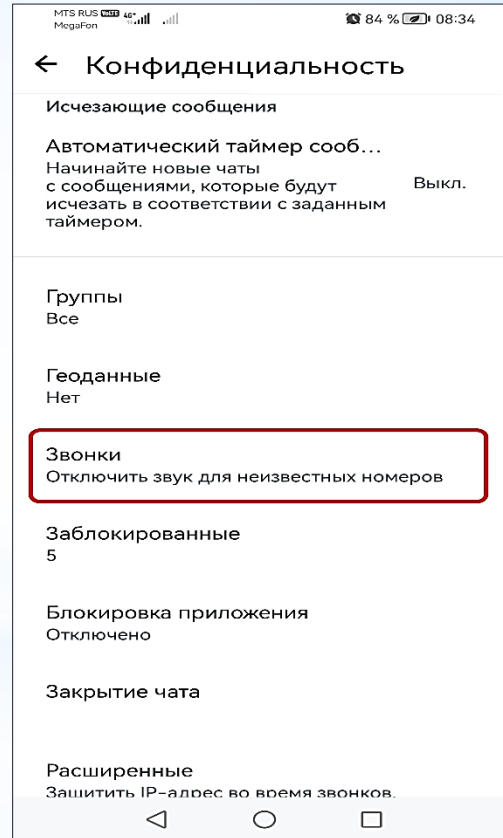
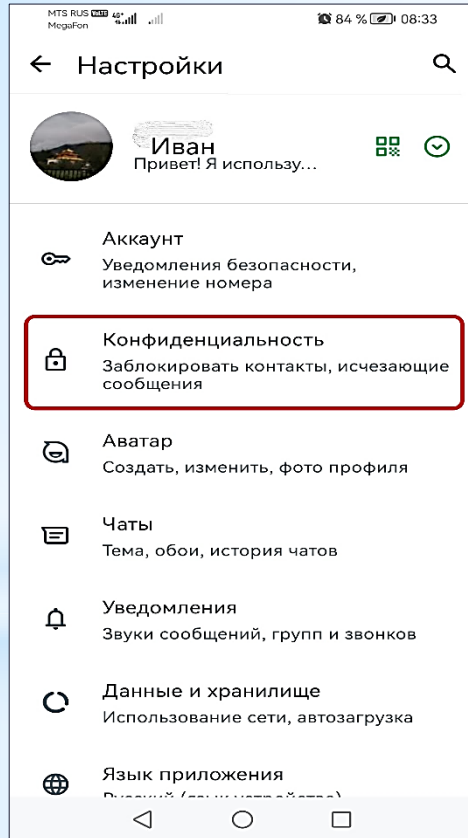
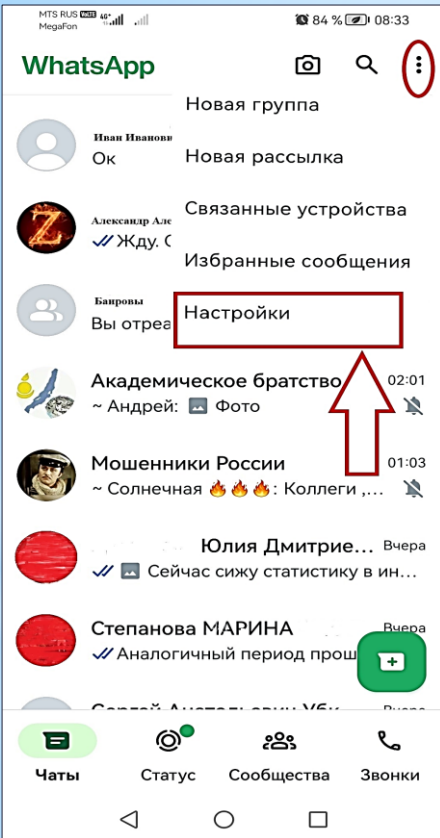


Защита от звонков в Viber





Защита от звонков в WhatsApp





Как сделать общение в MAX безопасным



16:07

MAX

LTE 98



Юрий

госуслуги

Цифровой ID

Войти в Сферум

Пригласить друзей

Уведомления и звук

Приватность

Сообщения

Избранное

16:07

MAX

LTE 98

Приватность

Пароль для входа
Отключён

Безопасный режим

Позвонить могут контакты

Найти меня по номеру могут все

Показывать контент безопасный

Пригласить в чат могут контакты

ИНФОРМАЦИЯ

Статус «в сети» НИКТО

Чёрный список
Список тех, кто не может вам писать, звонить и добавлять в чаты

СЕССИИ

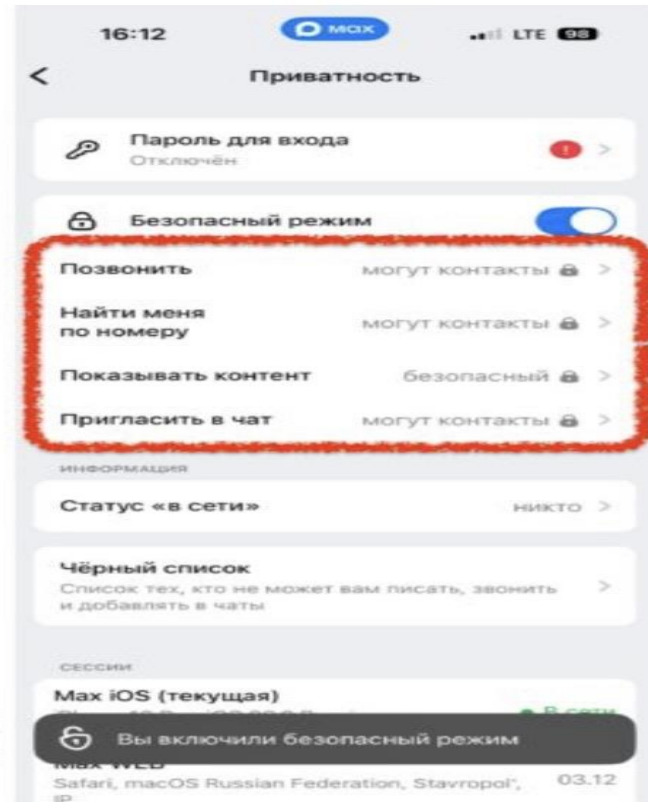
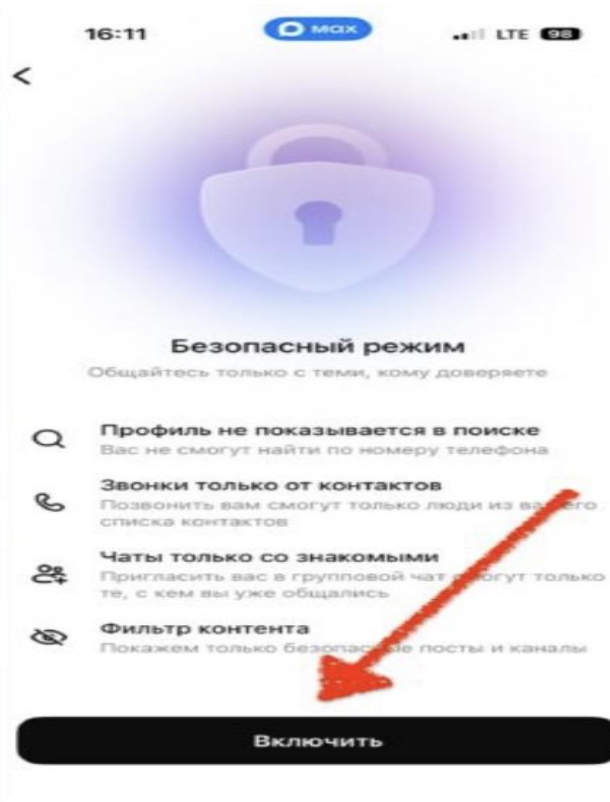
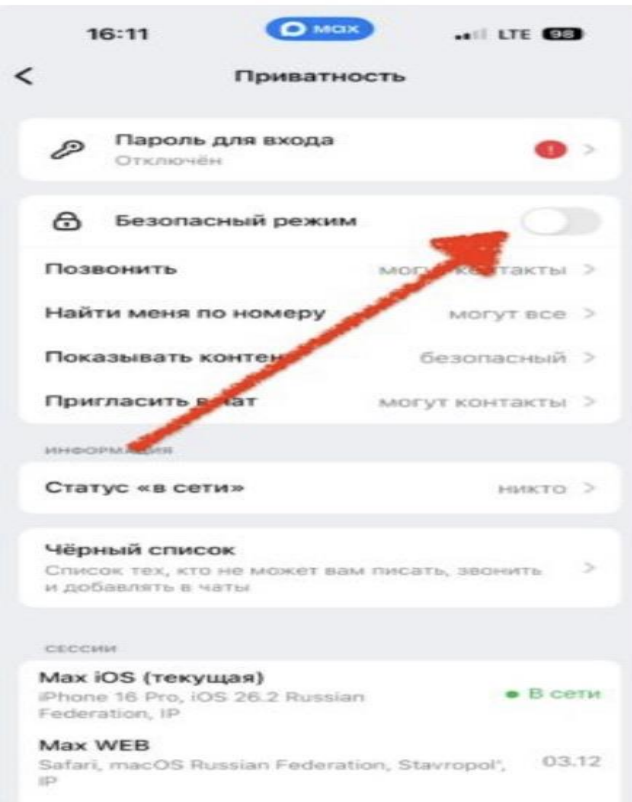
Max iOS (текущая)

iPhone16 Pro iOS 26.2 Russian

В сети

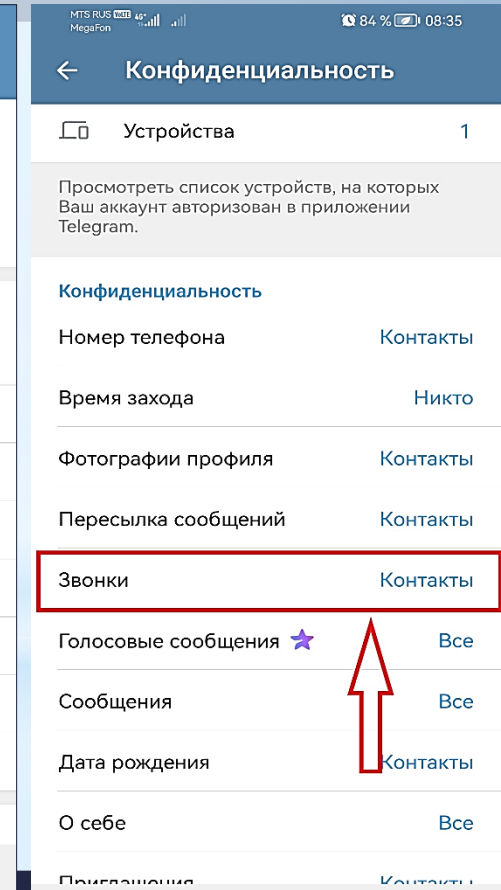
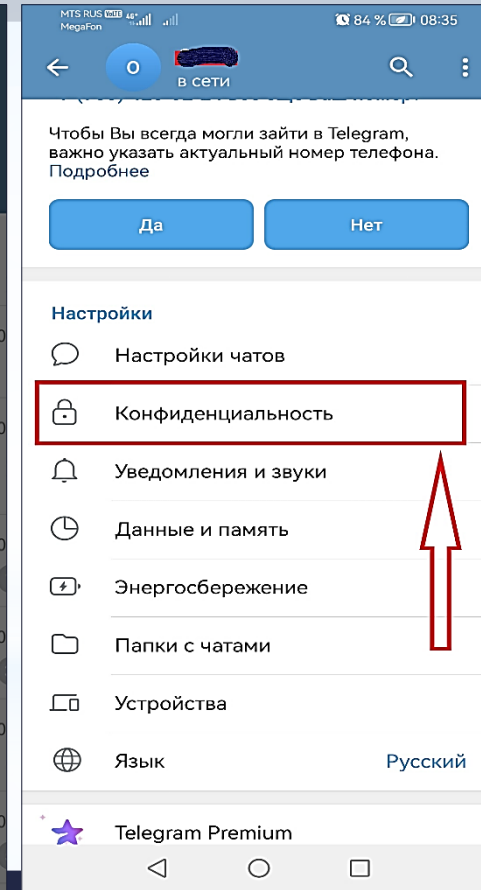
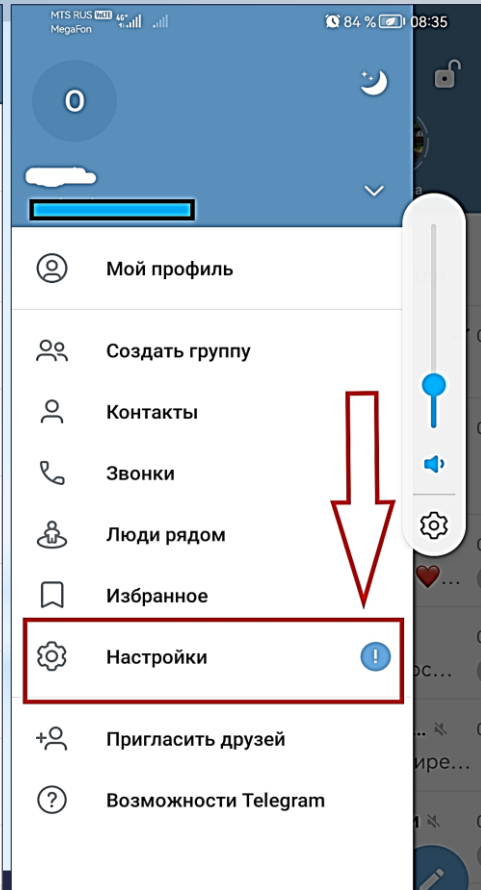
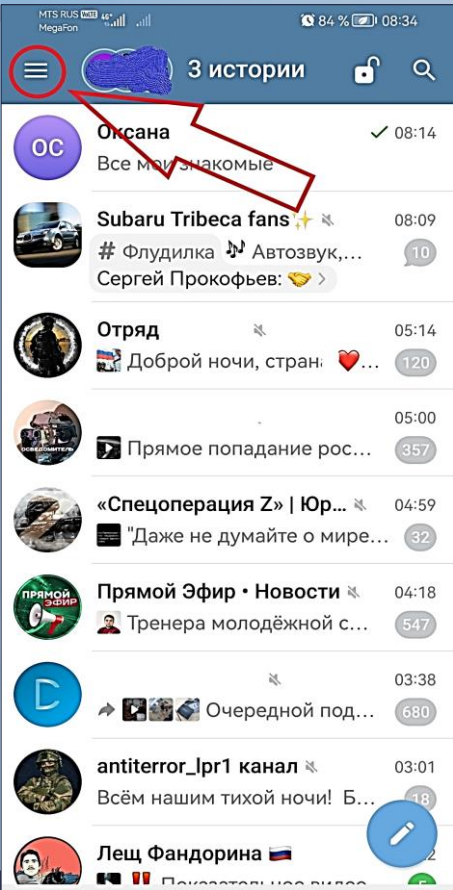


Как сделать общение в MAX безопасным



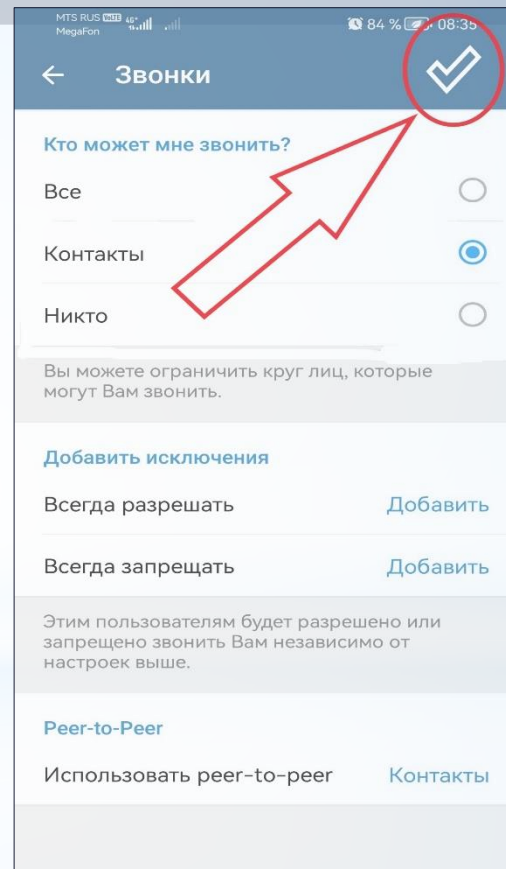
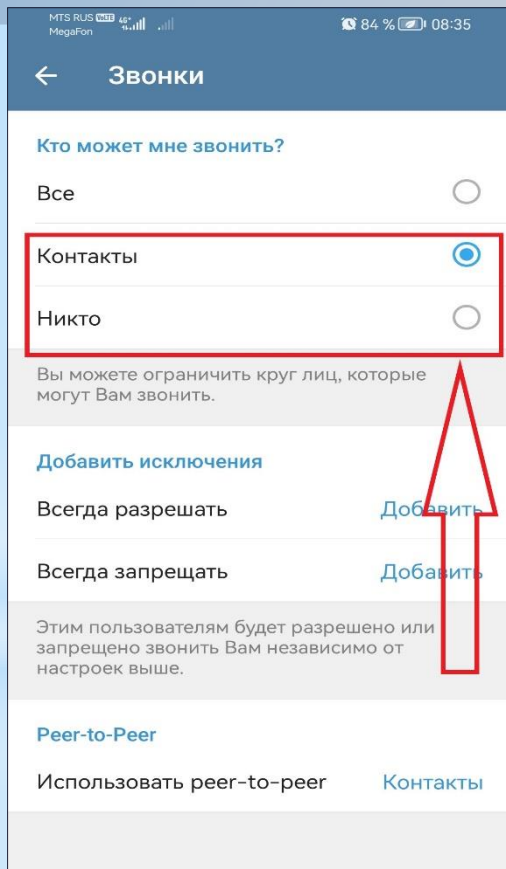


Защита от звонков в Telegram



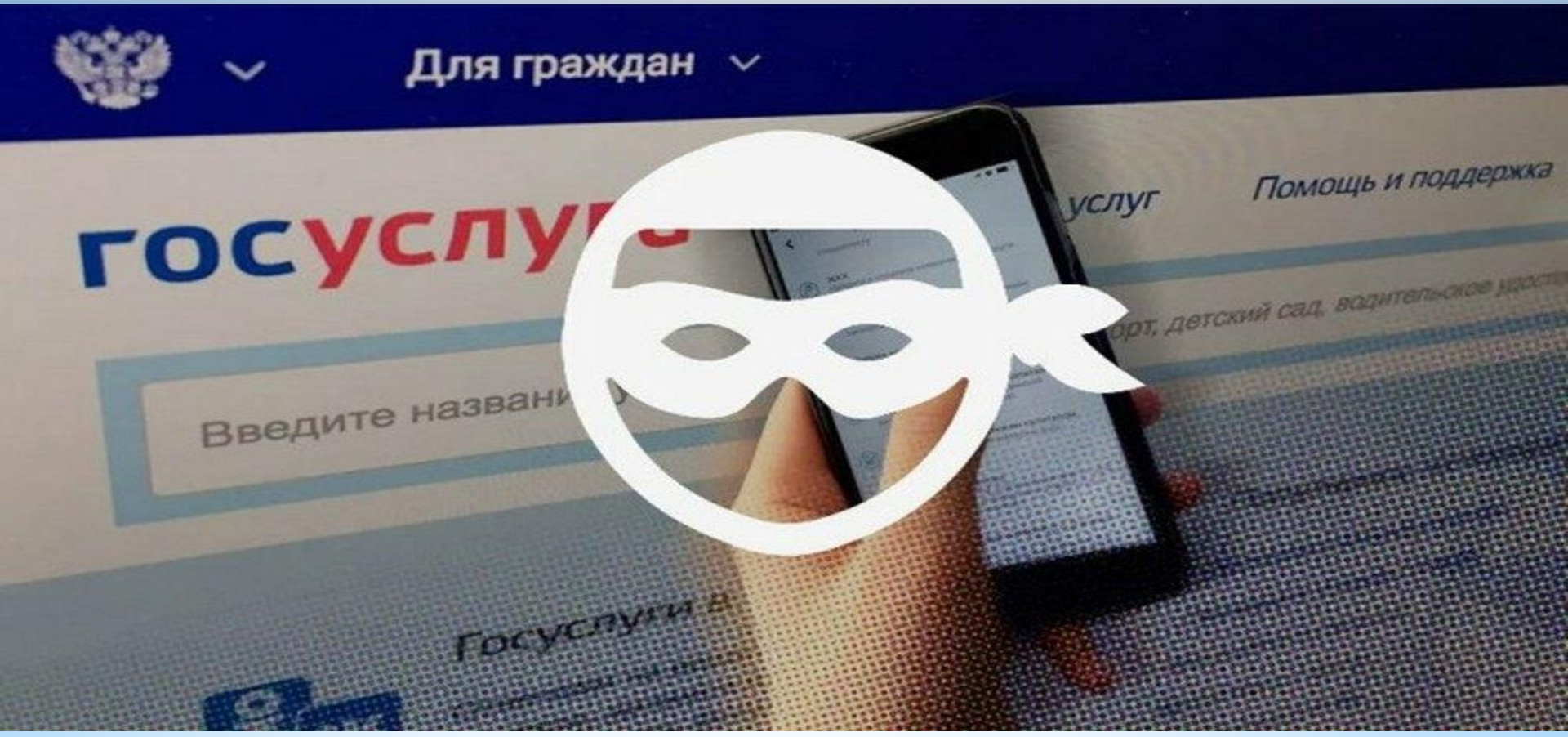


Защита от звонков в Telegram





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.
 - 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».

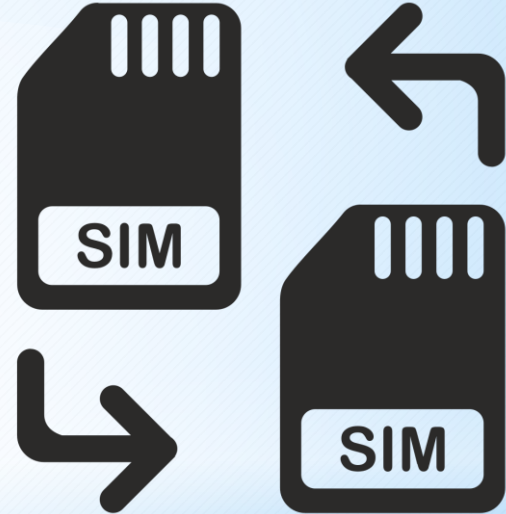
Скриншот интерфейса «Госуслуги» для изменения номера телефона. Вверху логотип «госуслуги». Заголовок: «Изменение номера телефона +7 924». Поле ввода: «Новый номер телефона» с форматом «+7 () - - -».



2. Переоформление SIM-карты

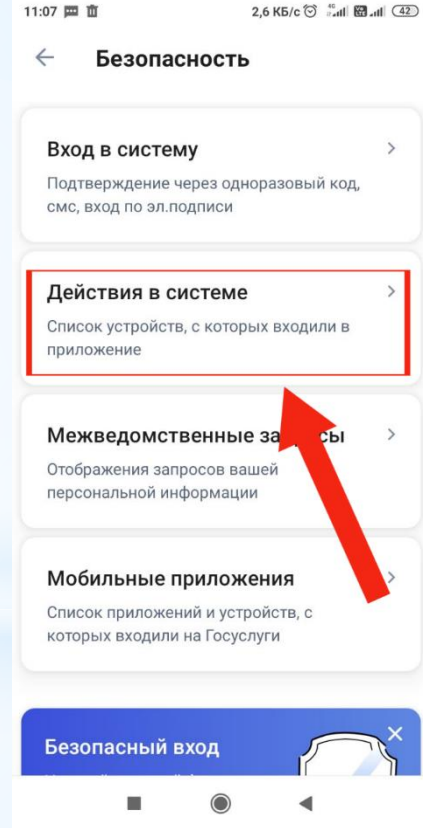
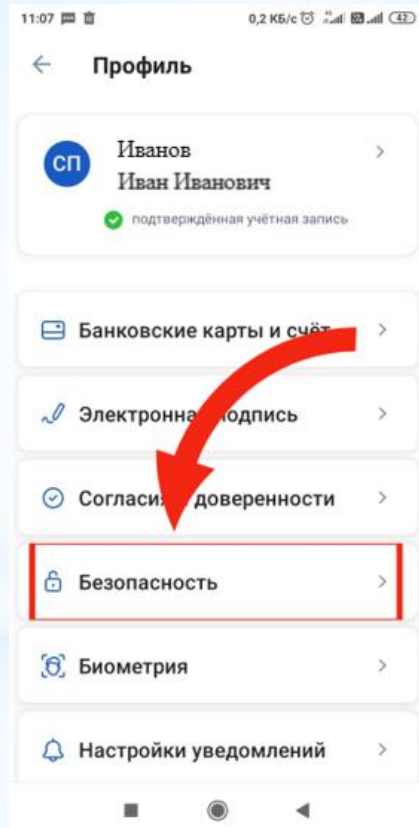
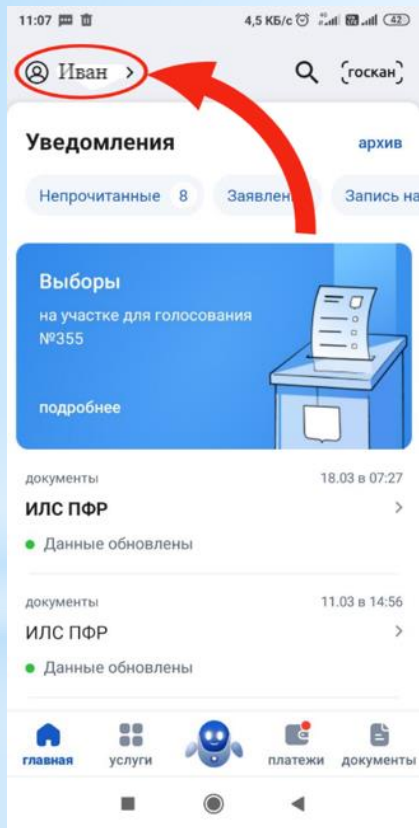
- SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

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.





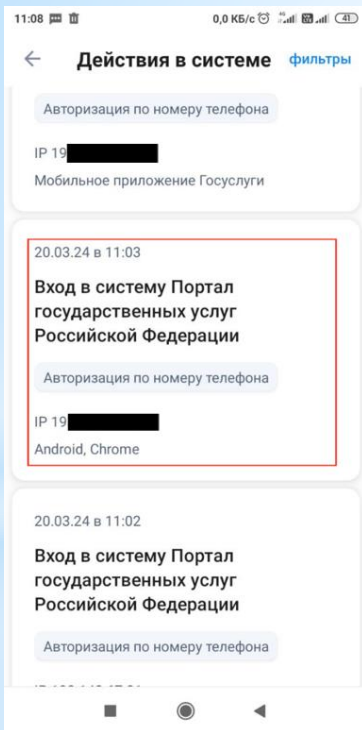
Признаки взлома личного кабинета портала «Госуслуги»





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





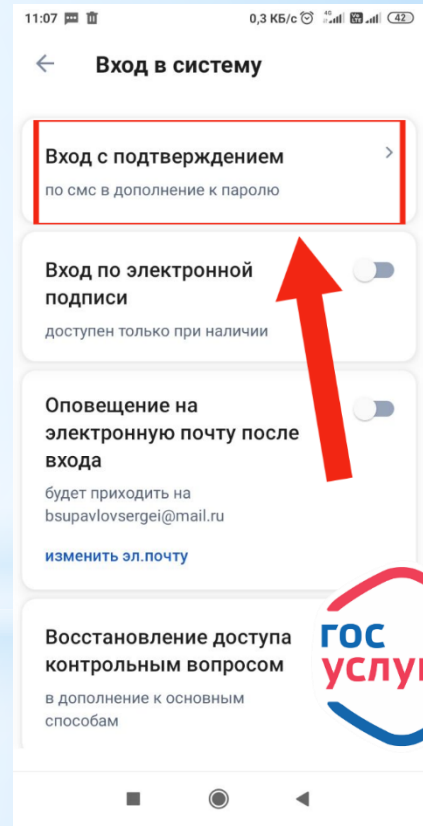
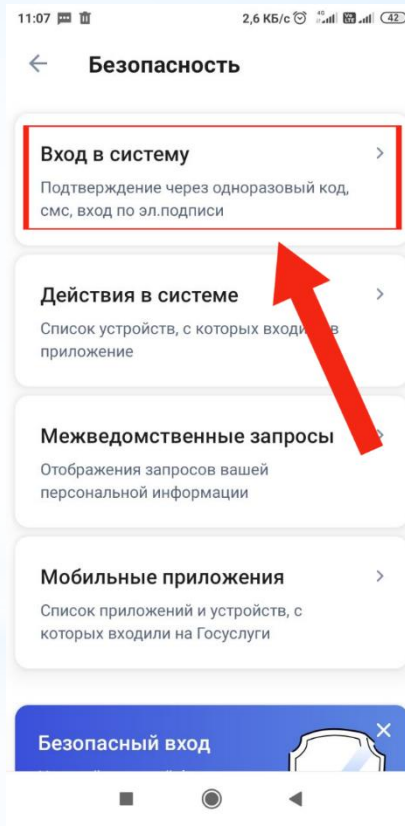
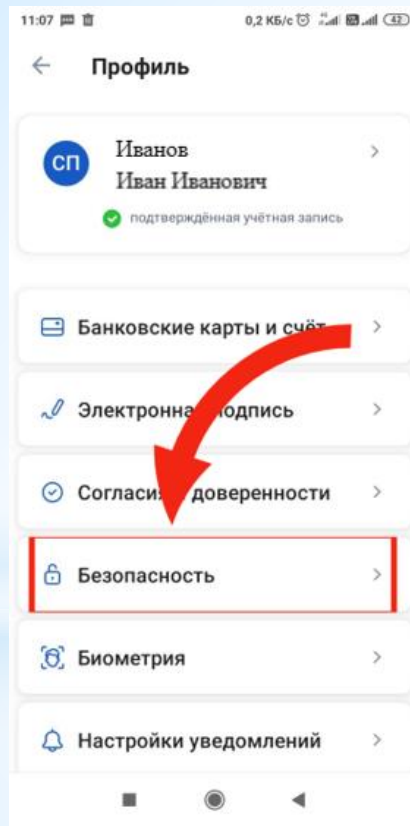
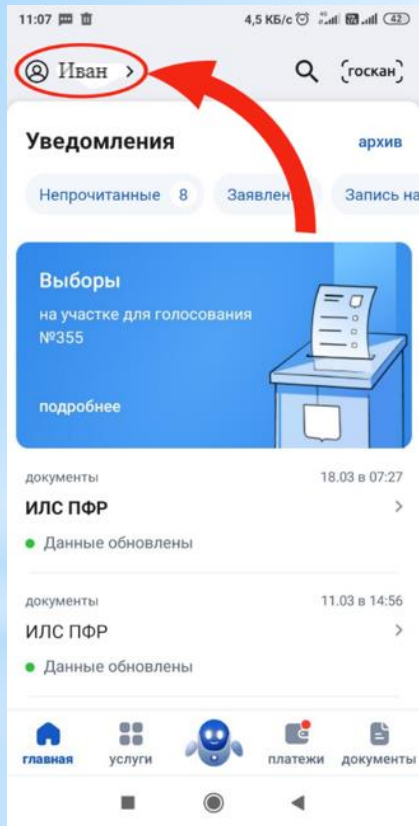
Как обезопасить личный кабинет от взлома?

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.



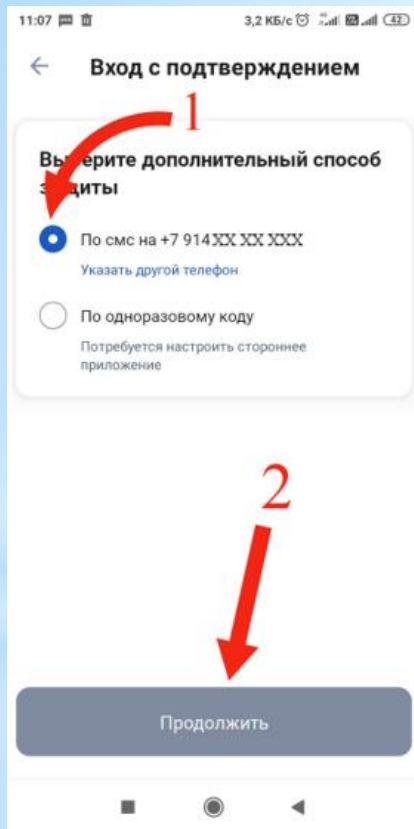


Дополнительная защита личного кабинета





Дополнительная защита личного кабинета



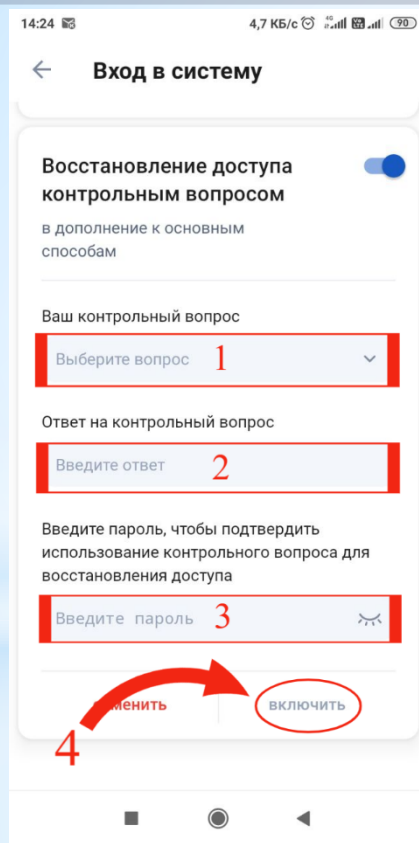
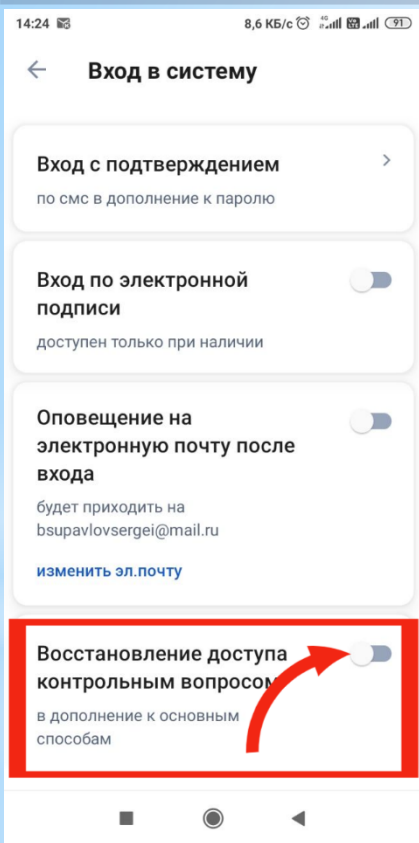
Функция входа с двухэтапной аутентификацией.

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



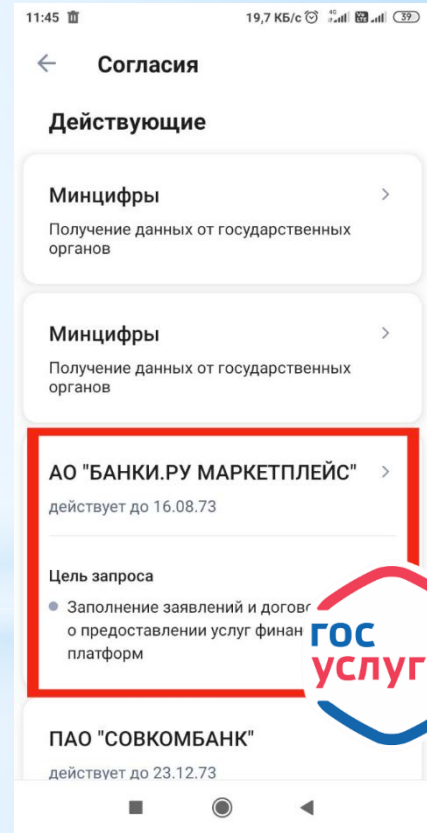
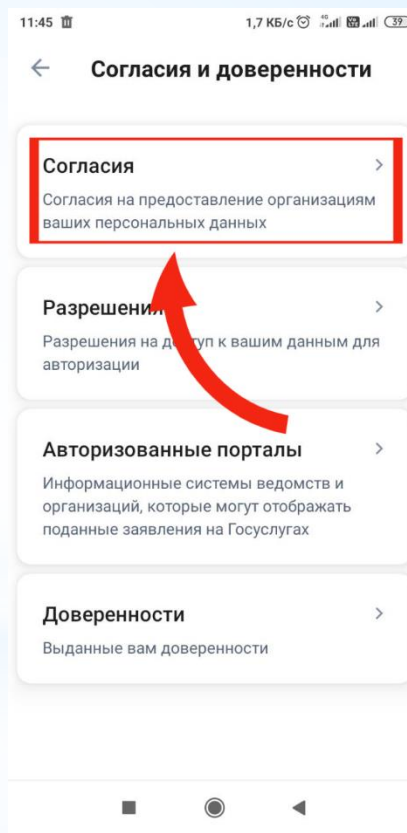
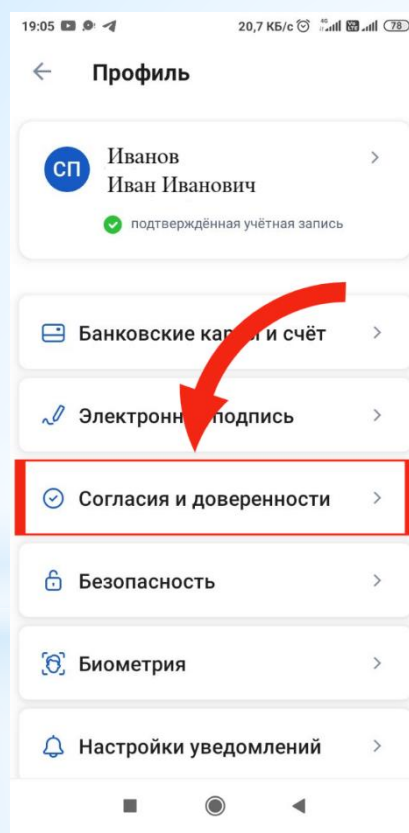
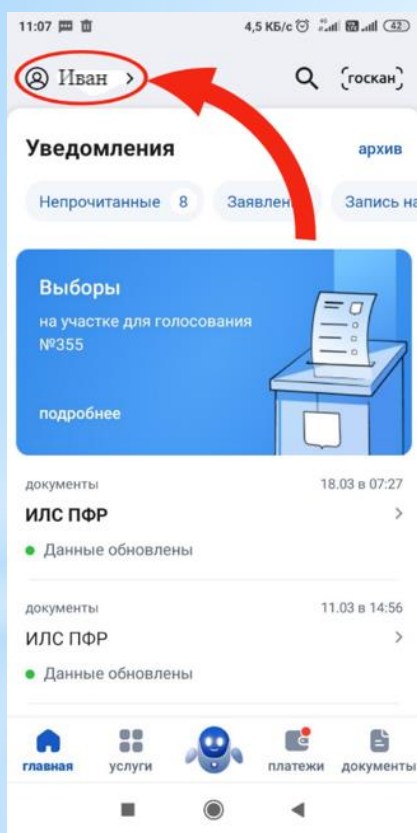
Функция восстановления доступа контрольным вопросом.

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



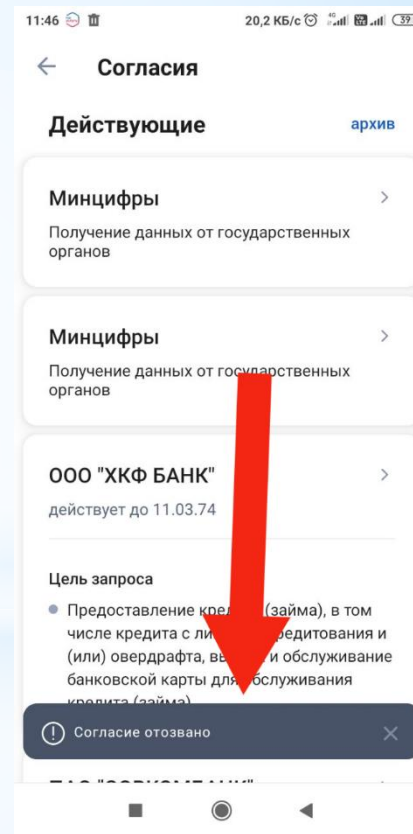
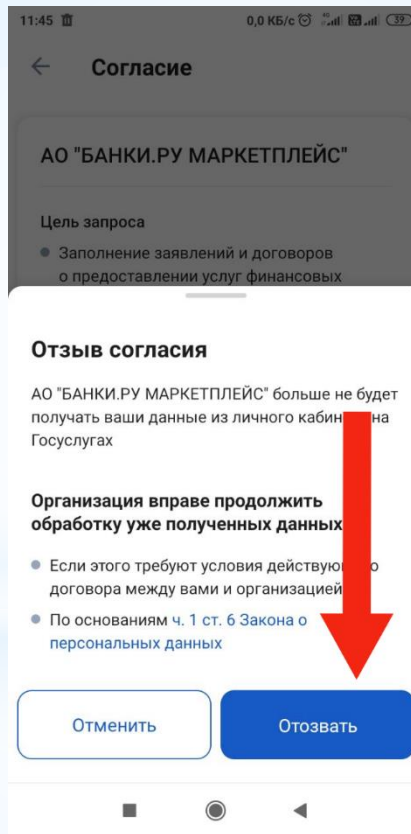
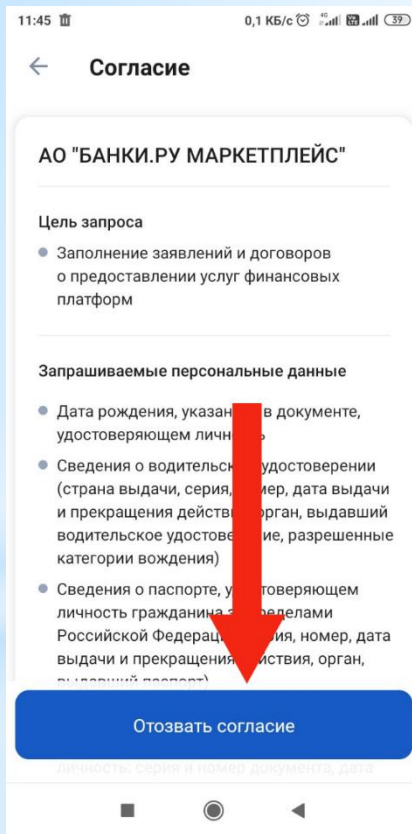


Отзыв согласий



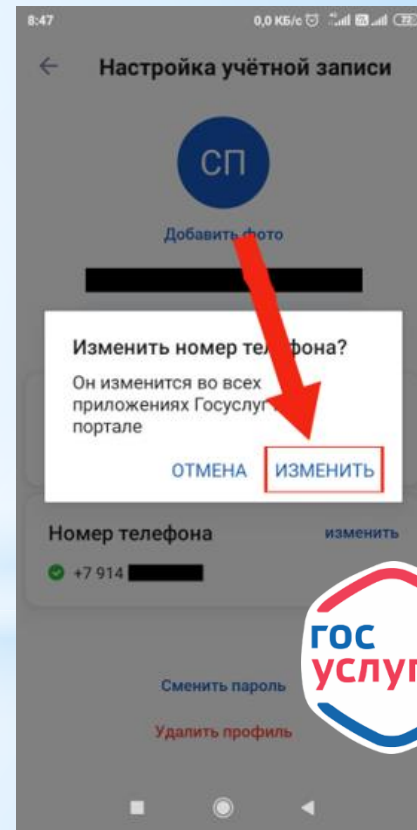
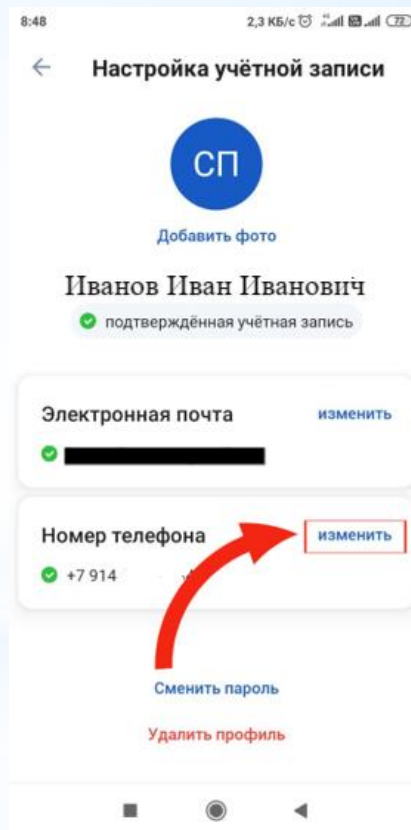
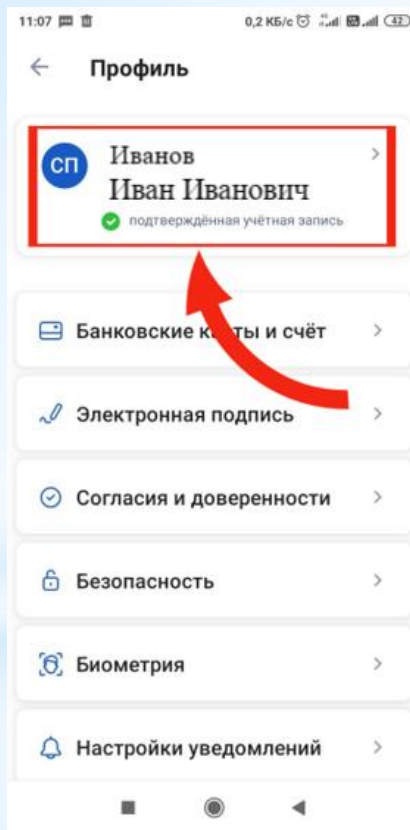
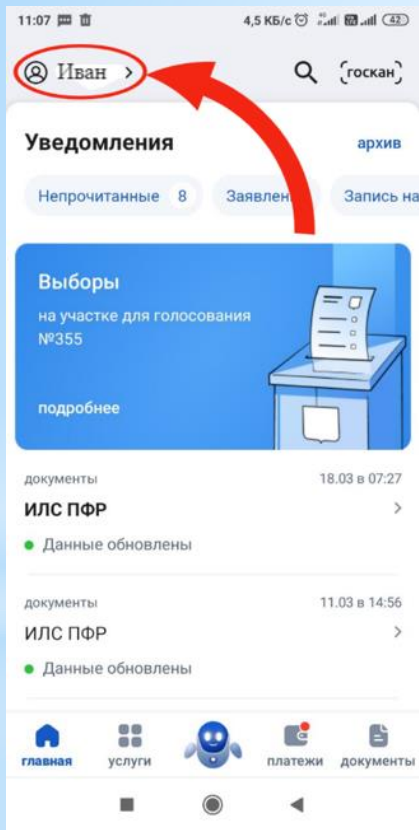


Отзыв согласий





Способ открепления номера телефона





Способ открепления номера телефона





Как распознать сайт двойник?

- ▶ ПРИБЛИЖИТЕСЬ К ПРОБЛЕМЕ
▶ 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 nature:

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

**БУДЬТЕ
ВНИМАТЕЛЬНЫ!**



**НЕ ДАЙТЕ
СЕБЯ ОБМАНУТЬ!**



УМВД России по Хабаровскому краю