# ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ

полковник полиции
Базаржапов Бато Баторович

МВД по Республике Бурятия

# 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!**

# Советы по безопасности

Покупайте и продавайте в вашем городе, из рук в руки

Называйте только номер карты - этого достаточно для перевода денег

Оформите отдельную карту для оплаты в интернете

Не отправляйте деньги наперед

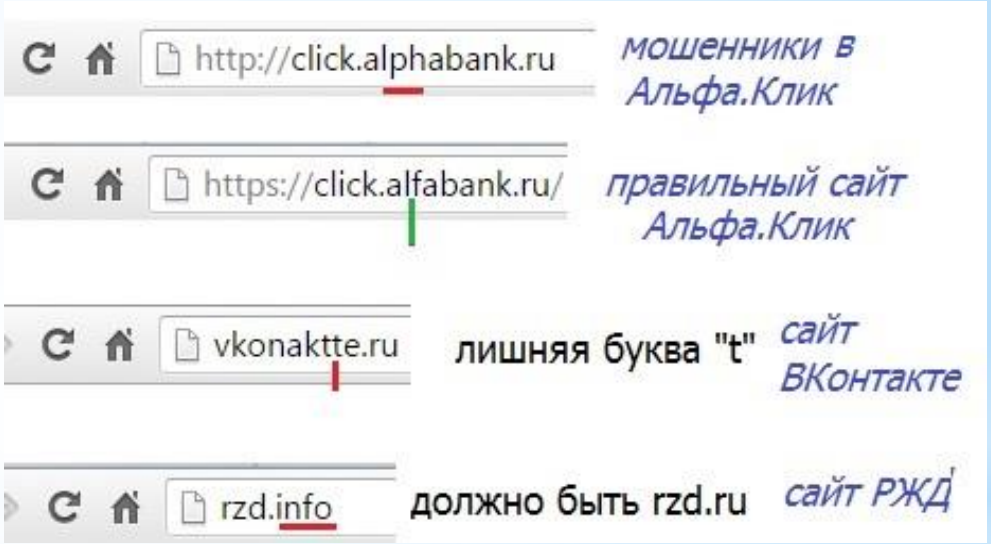
Настаивайте на наложенном платеже без предоплаты

Проверяйте данные продавца/покупателя в интернете

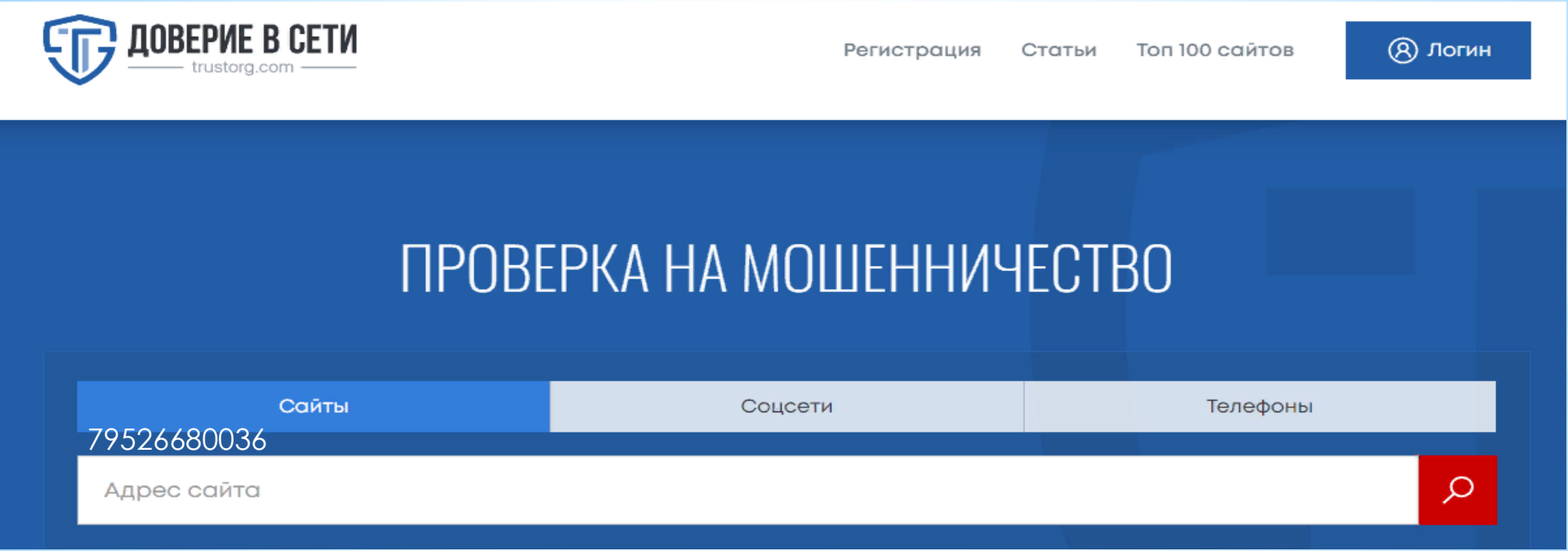
- ***Не переходите по неизвестным ссылкам, для совершения безопасной сделки сформируйте ссылку самостоятельно.**

# 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**



# Проверьте продавца / покупателя при помощи различных сервисов. Например на сайте «Доверие в сети»



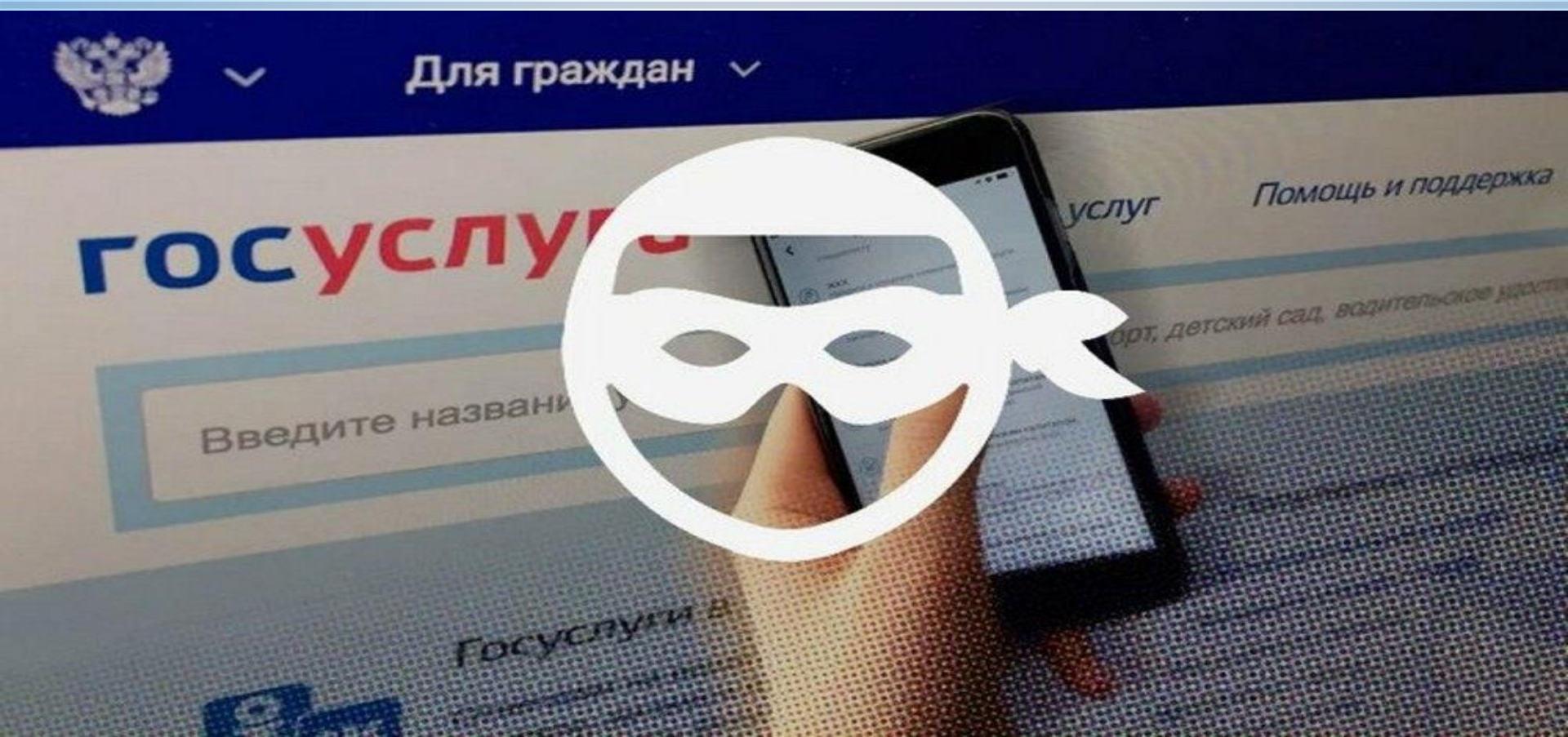
# Признаки финансовой пирамиды

1. Обещание слишком высоких доходов
2. Прибыль за счет привлечения новых вкладчиков
3. Ограниченный доступ к учредительным документам и финансовой отчетности компании
4. Сомнительные договоры
5. Агрессивная реклама

# Как себя обезопасить?

- **Проверять брокерскую компанию на сайте Банка России на наличие лицензии (https://cbr.ru/finorg/);**
- **Не доверять рекламе о биржах в социальных сетях;**
- **Не верить заманчивым и убедительным обещаниям о высокой доходности и отсутствии риска.**

# Взлом личного кабинета Госуслуг

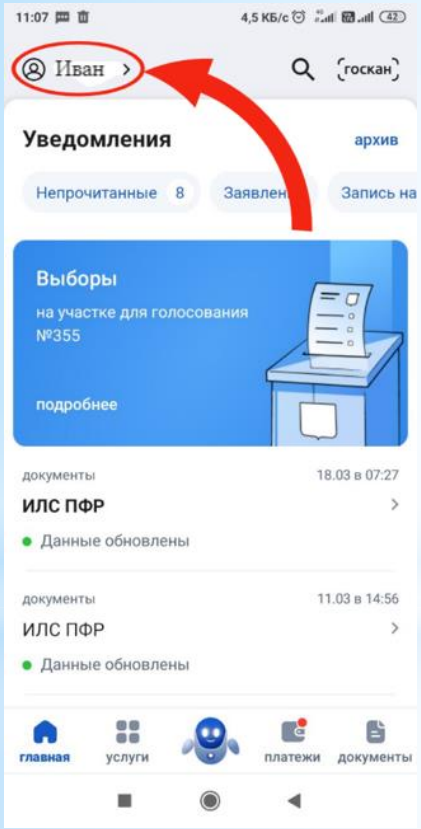


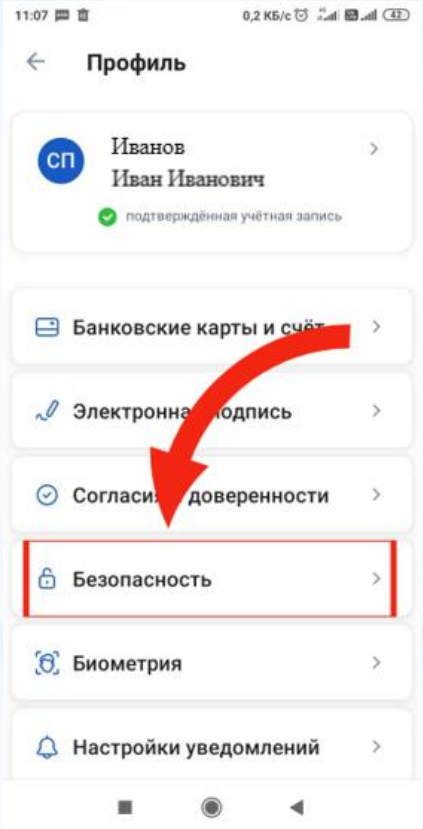
# Основные схемы взлома портала «Госуслуги»:

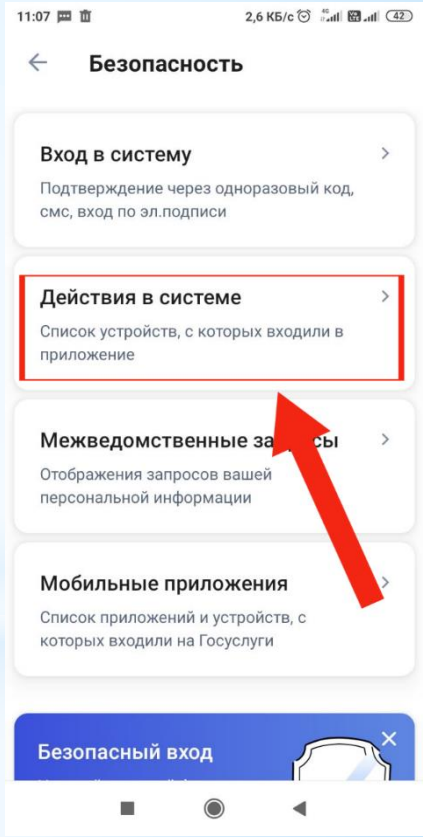
1. Звонок от работника сотового оператора

2. Переоформление SIM-карты

# Признаки взлома личного кабинета портала «Госуслуги»

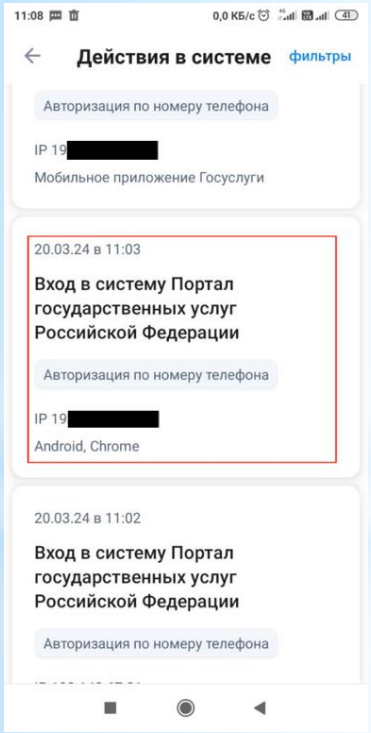


# Признаки взлома личного кабинета портала «Госуслуги»

## 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?

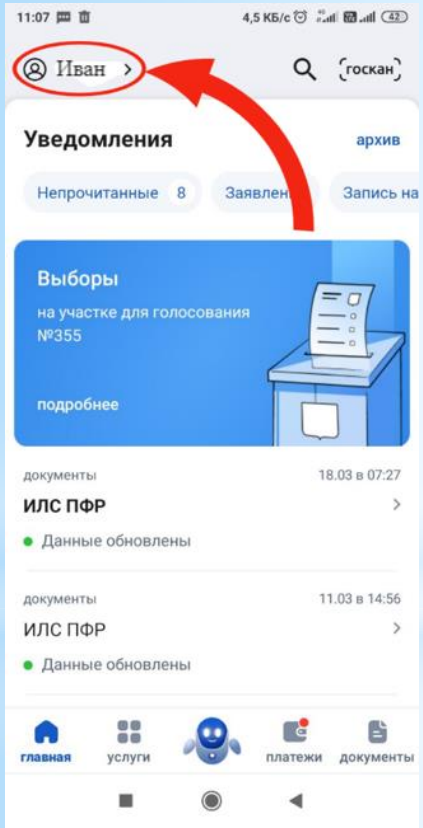
1. Никому не сообщайте код из SMS-сообщения, поступившего с портала «Госуслуги»;

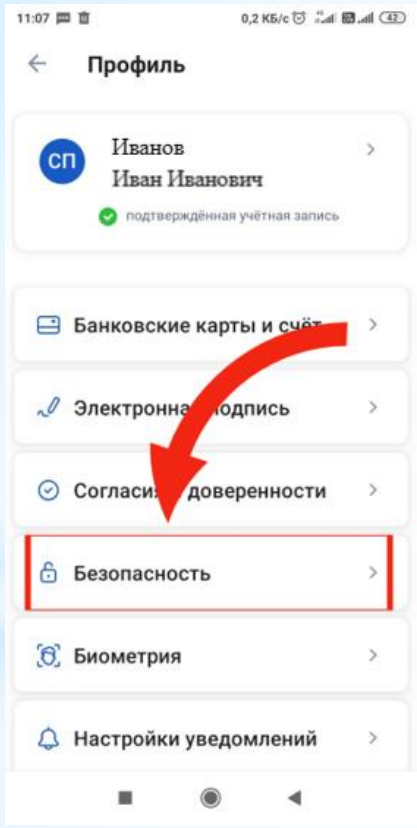
2. Настроить двухэтапную аутентификацию;

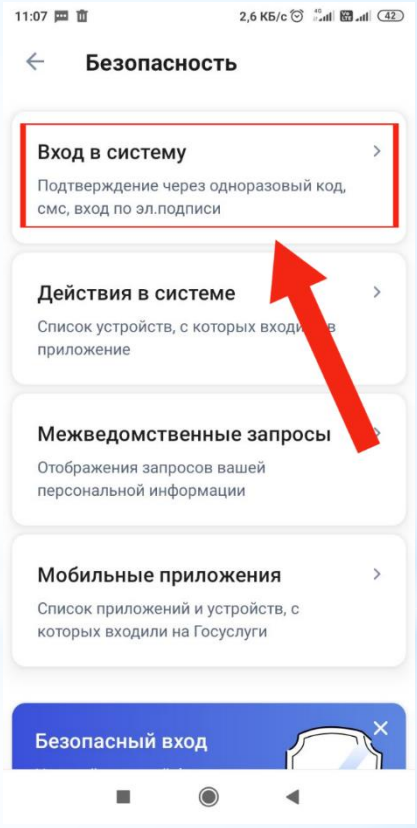
3. Отозвать неизвестные для вас согласия в личном кабинете;

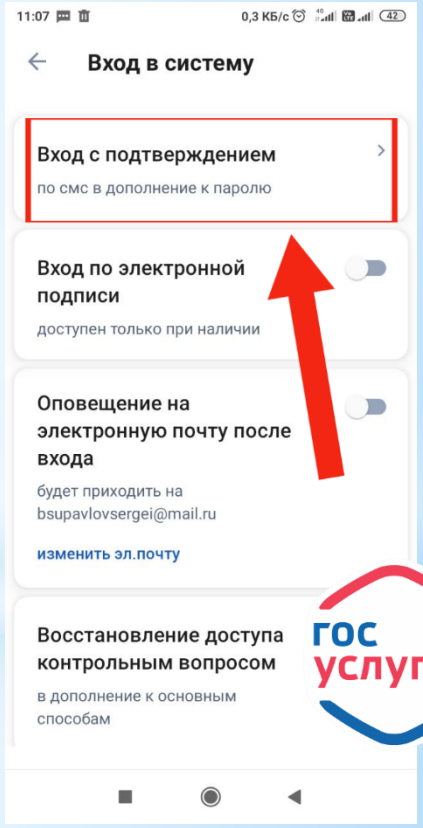
4. Регулярно, раз в полгода необходимо менять пароли доступа.

# Дополнительная защита личного кабинета

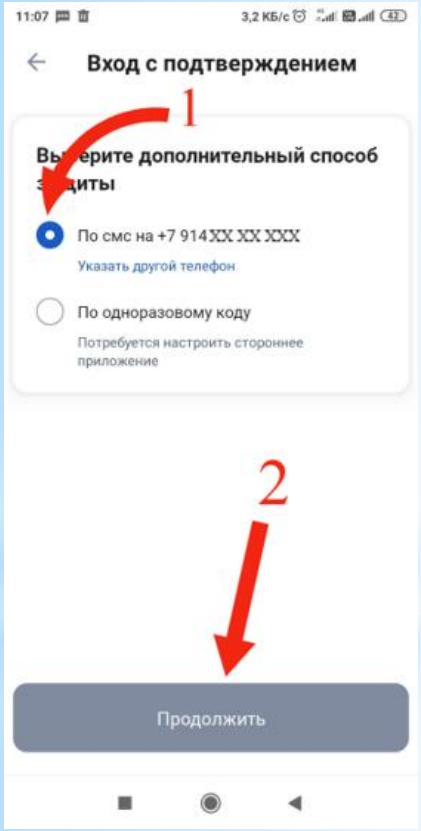


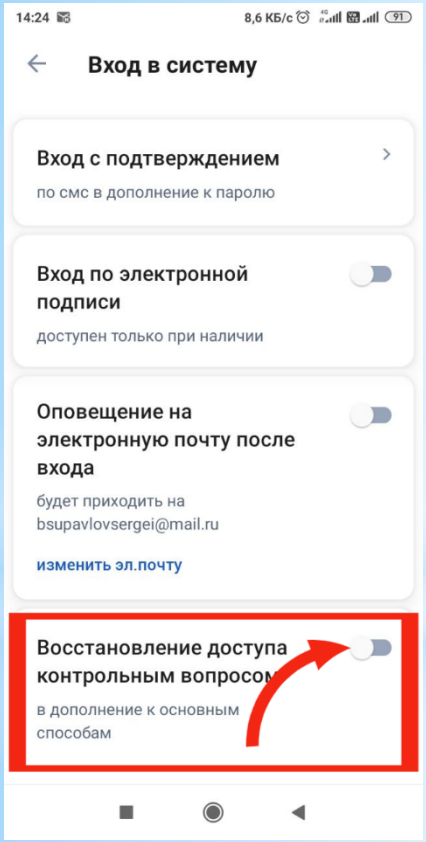
# Дополнительная защита личного кабинета

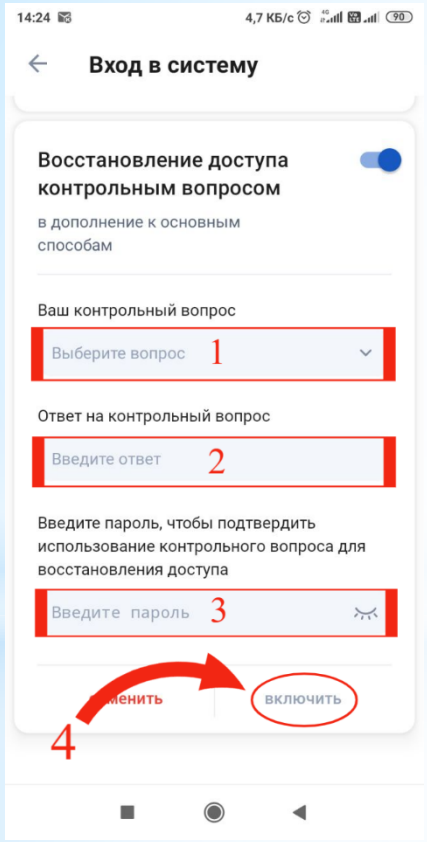



Функция входа с двухэтапной аутентификацией.

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

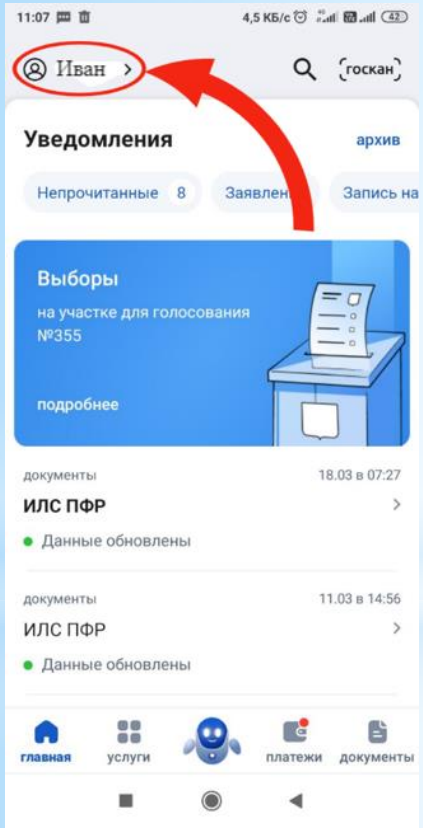


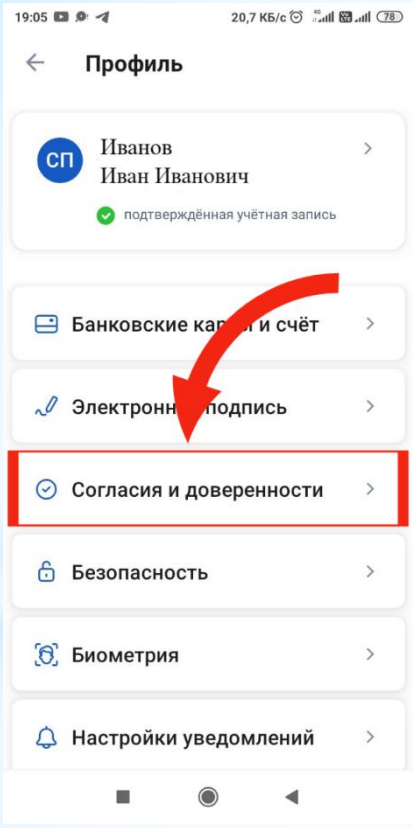



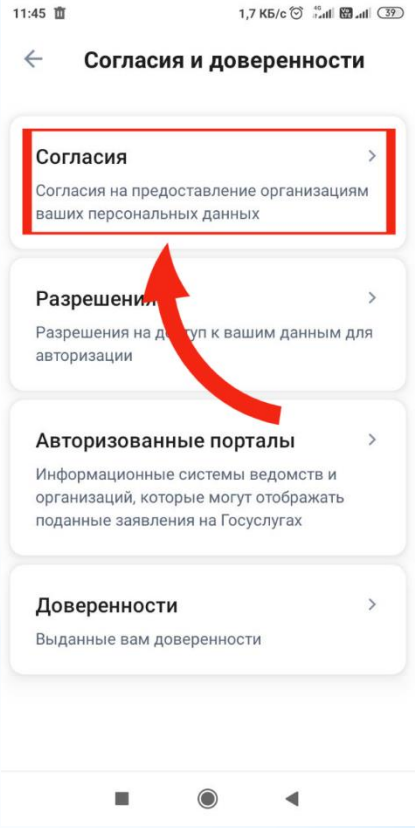

Функция восстановления доступа контрольным вопросом.

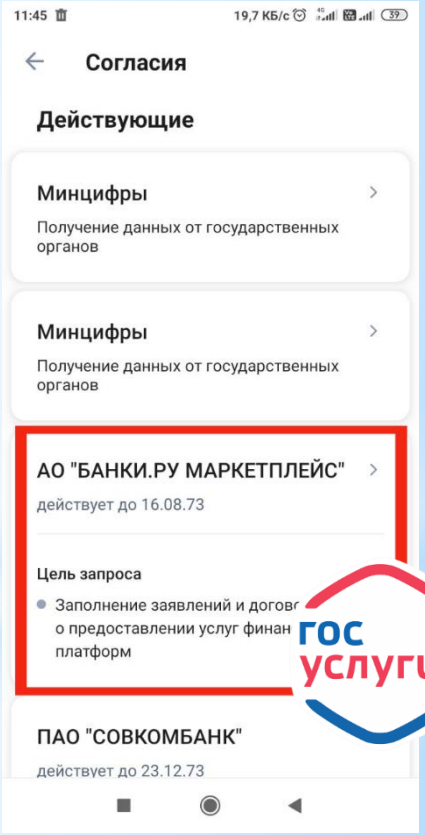
После переоформления SIM-карты, мошенники не смогут восстановить доступ к личному кабинету, так как они не знают ответ на контрольный вопрос.

# Отзыв согласий

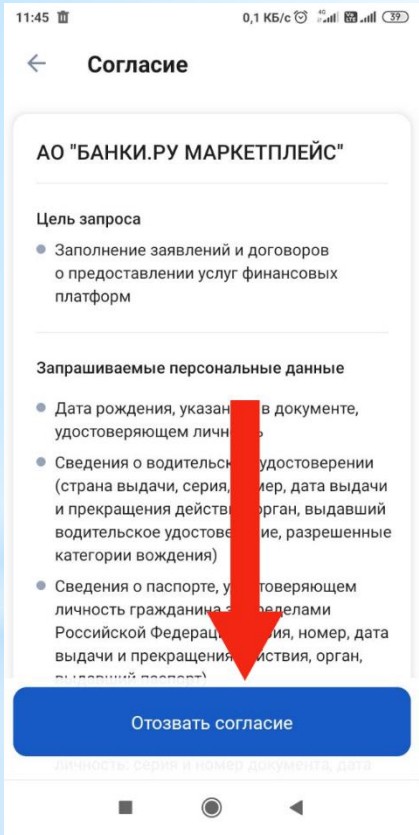


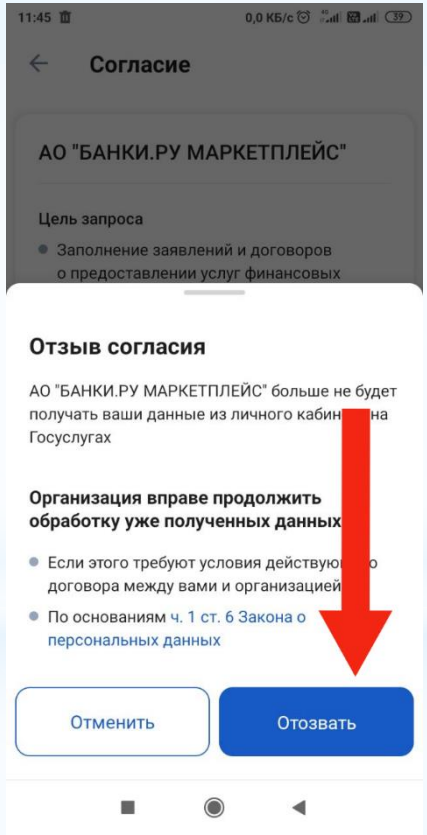



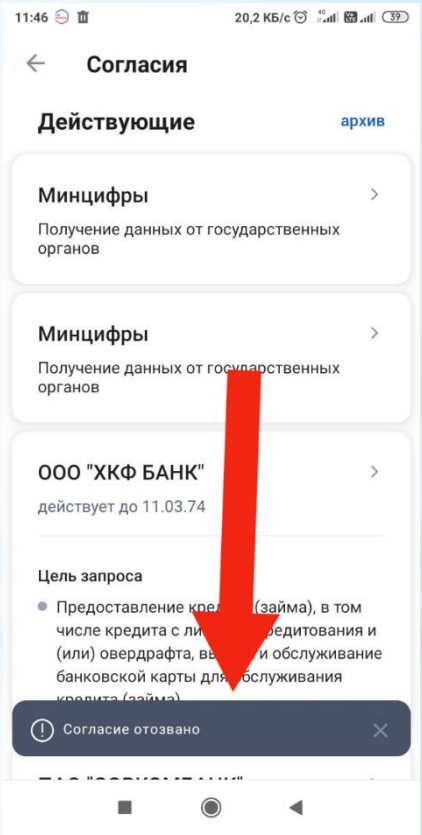



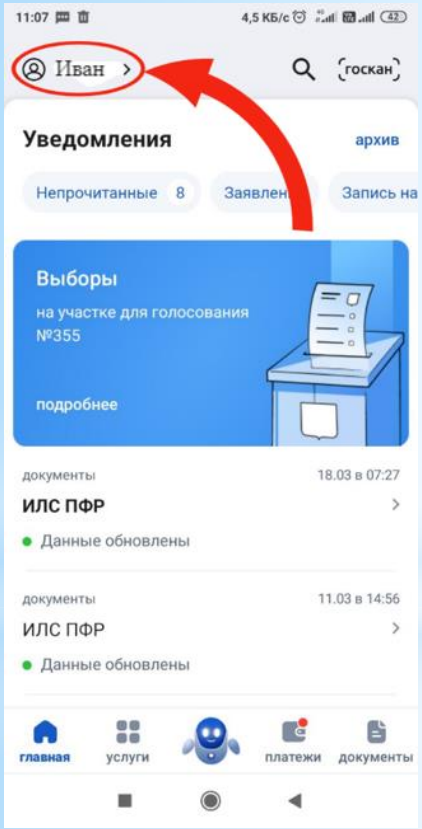
# Отзыв согласий

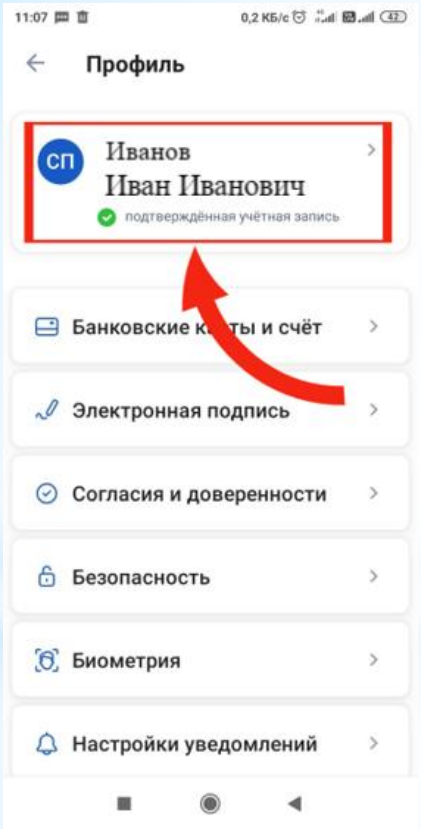


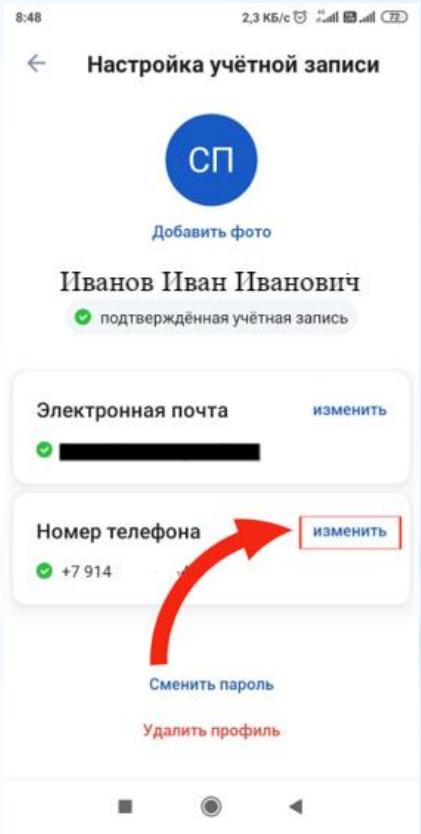



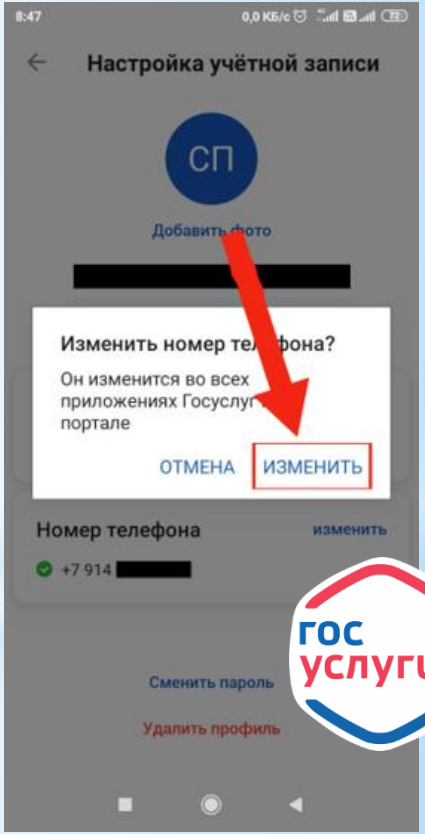



# Способ открепления номера телефона



# Способ открепления номера телефона

# ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА И ЗАЩИТА ОТ НИХ

полковник полиции
Базаржапов Бато Баторович

МВД по Республике Бурятия