



МВД по Республике Бурятия



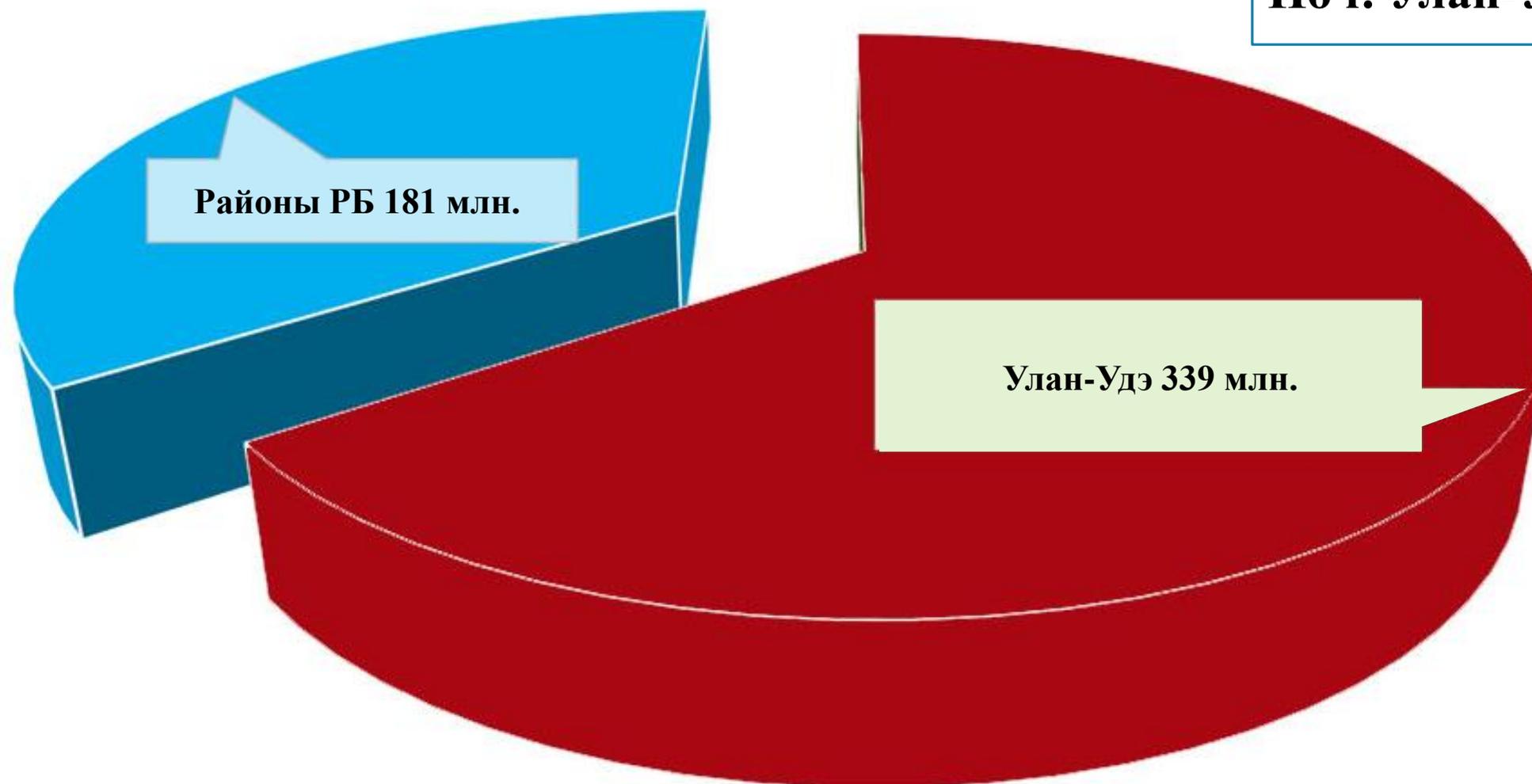
**ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ
ОТ КИБЕРПРЕСТУПЛЕНИЙ**

СТАТИСТИЧЕСКИЕ ДАННЫЕ ЗА 9 МЕСЯЦЕВ 2024 Г.

- **По Республике зарегистрировано:**
- 2135 мошенничеств (рост на 3,9%);
- 776 краж с банковских счетов (снижение на 34,2%);
- 1134 взлома портала «ГОСУСЛУГИ» (РОСТ НА 420,2%).

УЩЕРБ ЗА 9 МЕСЯЦЕВ 2024 года

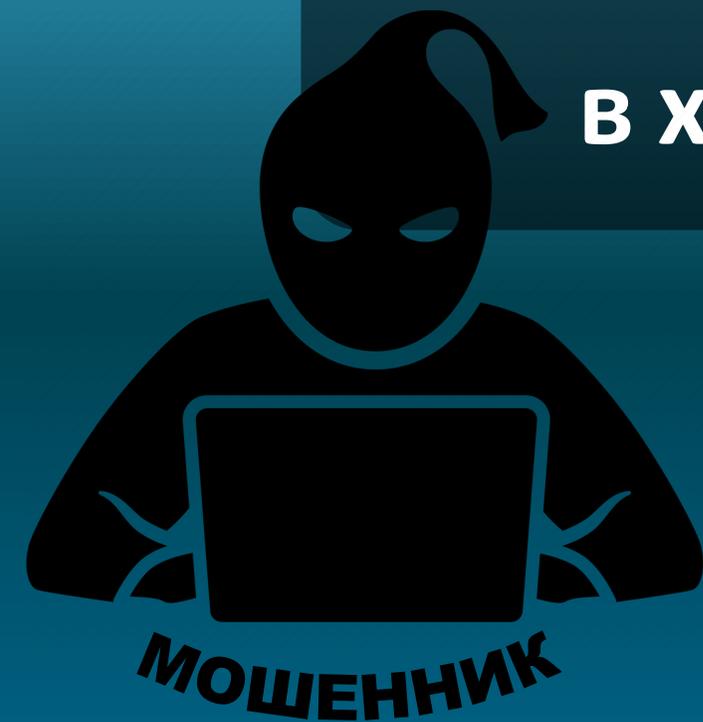
**По Республике 520 млн.
По г. Улан-Удэ 339 млн.**



ГЕОЛОКАЦИЯ МОШЕННИЧЕСКИХ КОЛЛ-ЦЕНТРОВ



Виды обманов в ходе телефонного разговора



1 ВЗЛОМ ПОРТАЛА «ГОСУСЛУГИ»



МОШЕННИК

ЗВОНИТ ЖЕРТВЕ, ПРОСИТ СООБЩИТЬ СМС КОД, ПОД ПРЕДЛОГОМ

Оператора мобильной связи:

- предлагает переоформить, продлить договор связи;
- пугает отключением услуг;
- сообщает о смене тарифного плана;

Сотрудника пенсионного фонда:

- говорит о перерасчете пенсии;
- предлагает получить единовременную выплату;



ЖЕРТВА



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;



ЖЕРТВА

Последствия передачи СМС-кода

8



МОШЕННИК

Входит в Госуслуги

Заполучив доступ

госуслуги

Восстановление пароля

Телефон / Email

89000000000

госуслуги

Изменение номера телефона
+7 924

Новый номер телефона

+7 () - - -

**Получает доступ к персональным данным
Оформляет онлайн-кредит, микро займы
Переводит все ваши деньги!!!**

Пример: Приложение 1

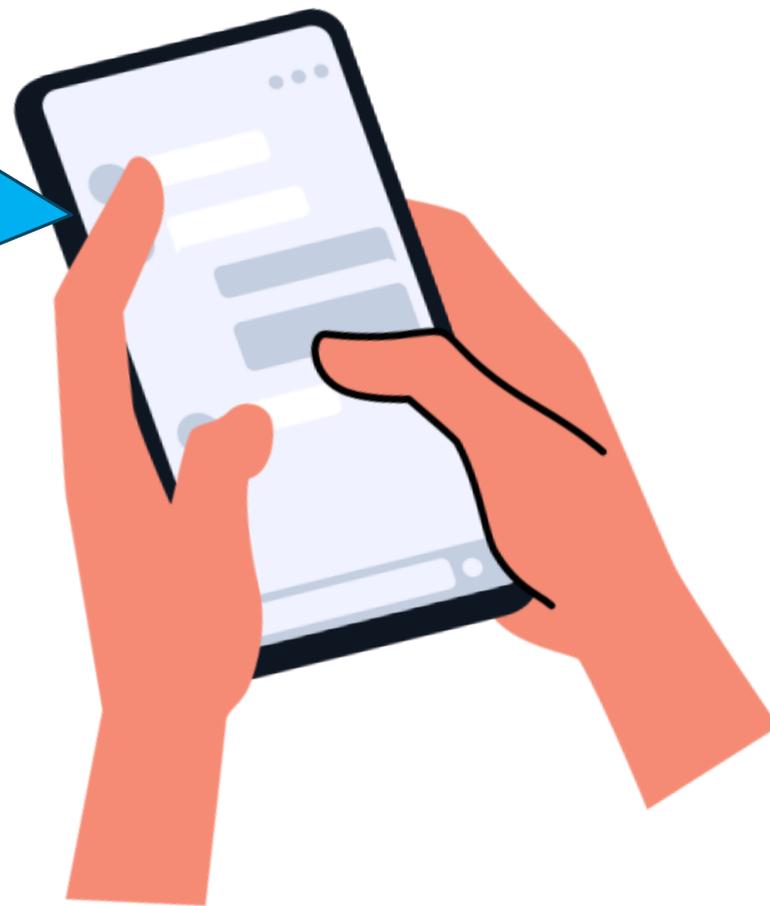


- **НЕ ОТВЕЧАЙ** на звонки с неизвестных номеров;
- **ТОЛЬКО** мошенники звонят в мессенджерах;
- **ЗАПОМНИ**, представители государственных учреждений и операторы сотовой связи **НИКОГДА** не просят СМС-коды!!!

КОД из СМС – это аналог вашей; собственной подписи. Его **НИКОГДА** и **НИКОМУ** нельзя сообщать или пересылать!

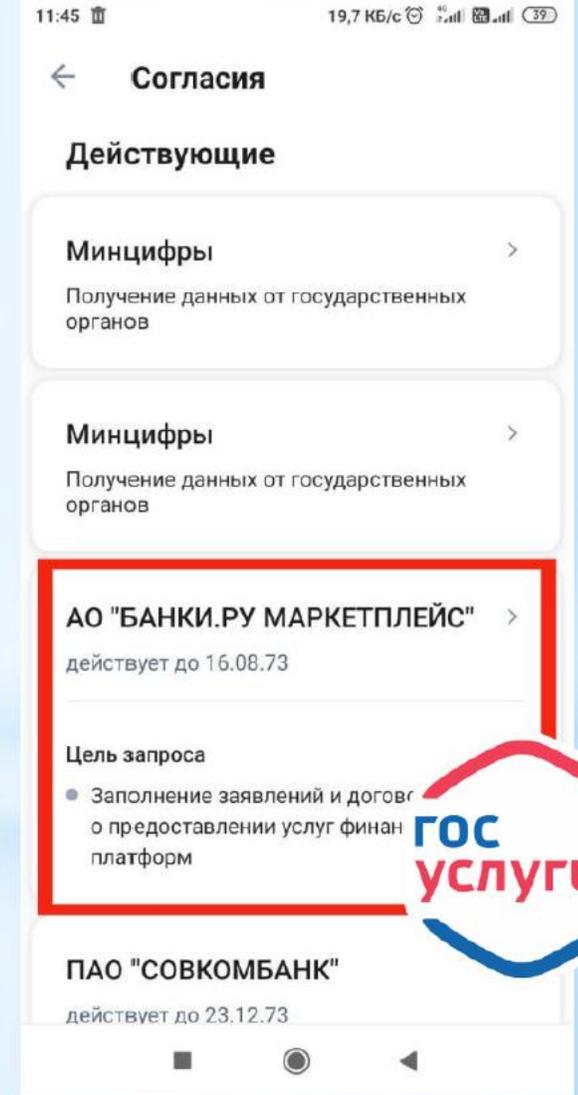
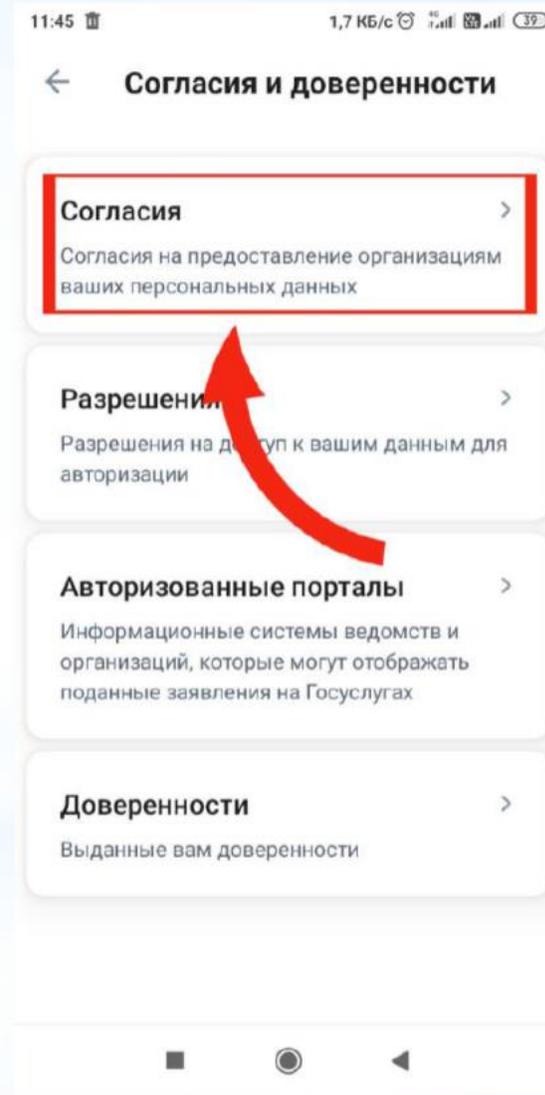
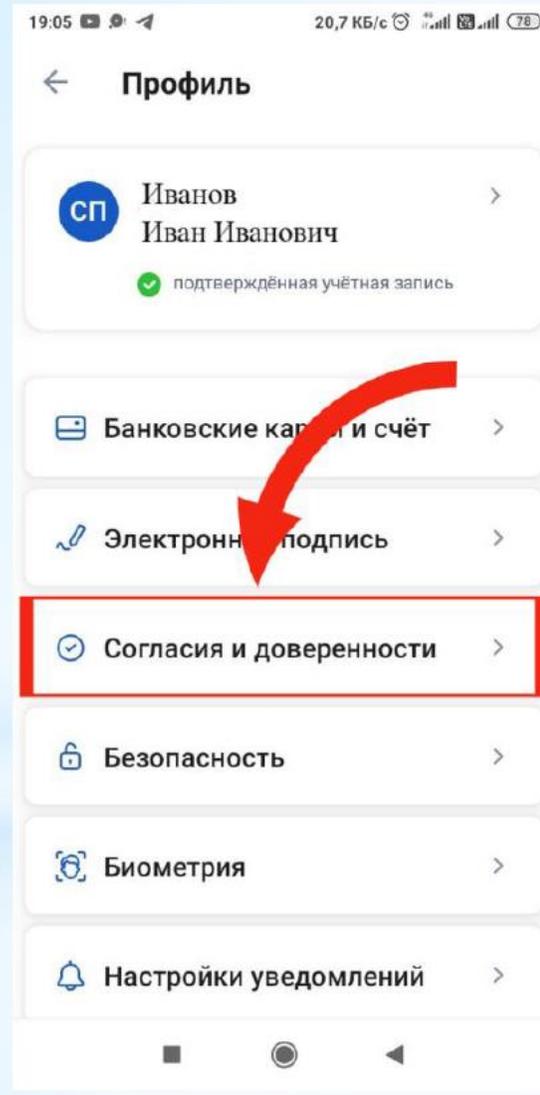
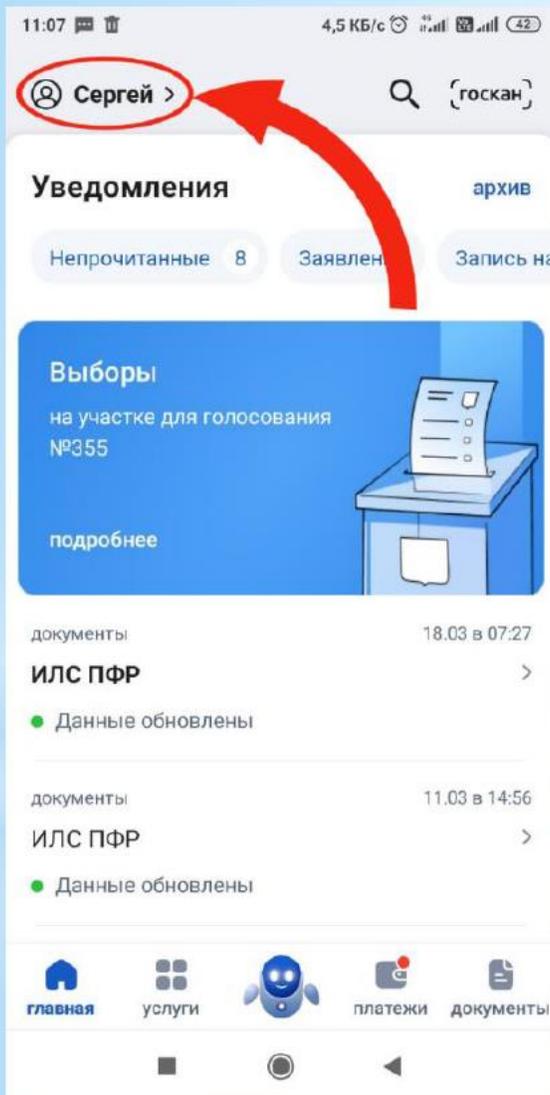
Внимание! Достаем телефоны!

Рекомендуем отозвать согласие на обработку персональных данных с банками, что бы мошенники получив доступ к порталу «Госуслуги», не могли оформить на Вас кредит!!!





Отзыв согласий



Отзыв согласий

← **Согласие**

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Запрашиваемые персональные данные

- Дата рождения, указанная в документе, удостоверяющем личность
- Сведения о водительском удостоверении (страна выдачи, серия, номер, дата выдачи и прекращения действия, орган, выдавший водительское удостоверение, разрешенные категории вождения)
- Сведения о паспорте, удостоверяющем личность гражданина Российской Федерации (серия, номер, дата выдачи и прекращения действия, орган, выдавший паспорт)

Отозвать согласие

← **Согласие**

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Отзыв согласия

АО "БАНКИ.РУ МАРКЕТПЛЕЙС" больше не будет получать ваши данные из личного кабинета на Госуслугах

Организация вправе продолжить обработку уже полученных данных

- Если этого требуют условия действующего договора между вами и организацией
- По основаниям ч. 1 ст. 6 Закона о персональных данных

Отменить **Отозвать**

← **Согласия**

Действующие архив

Минцифры >

Получение данных от государственных органов

Минцифры >

Получение данных от государственных органов

ООО "ХКФ БАНК" >

действует до 11.03.74

Цель запроса

- Предоставление кредита (займа), в том числе кредита с лимитом кредитования и (или) овердрафта, выдачи и обслуживание банковской карты для обслуживания кредита (займа)

Согласие отозвано



2 СПОСОБ МОШЕННИЧЕСТВА. СООБЩЕНИЕ ОТ РУКОВОДИТЕЛЯ



- взламывает аккаунт Вашего руководителя;
- направляет ложное сообщение работнику (например проверка с ФСБ, утечка данных, сейчас свяжутся сотрудники правоохранительных органов);





в схему вступает лже-сотрудник ФСБ, МВД, который грозит блокировкой счета, по которому якобы зафиксированы сомнительные операции, либо, кто-то пытается оформить кредит на имя жертвы, настаивает перевести личные деньги или оформить кредит, затем перевести их на якобы «БЕЗОПАСНЫЙ СЧЕТ»



3 СПОСОБ МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ ЗАРАБОТКА В СЕТИ ИНТЕРНЕТ ¹⁵



- Размещает в сети интернет информацию о заработке на инвестициях;
- Убеждает перейти жертву на ложный сайт;
- Показывает фиктивный заработок (прибыль);



- Видит мнимый доход;
- Вкладывает личные, либо кредитные деньги.

За 9 месяцев текущего года 45 жителей г. Улан-Удэ вложили в инвестиции около 110 млн. рублей

16



- **ПРОВЕРЯТЬ** брокерскую компанию на сайте Банка России на наличие лицензии.
- **НЕ ДОВЕРЯТЬ** рекламе о биржах в социальных сетях;
- **НЕ ВЕРИТЬ** заманчивым и убедительным словам о **ВЫСОКОЙ ДОХОДНОСТИ** при низком риске;
- **Насторожиться** при словах «инвестируйте как можно **БОЛЬШЕ И БЫСТРЕЕ**».
- Если хотите заработать, приобретая инвестиции, проконсультируйтесь в **БАНКЕ!**

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ



МОШЕННИК

**МОШЕННИК НЕ СМОЖЕТ ДО ВАС
ДОЗВОНИТЬСЯ В МЕССЕНДЕРАЖ,
ЕСЛИ ВЫ УСТАНОВИТЕ ЗАЩИТУ ОТ
НЕИЗВЕСТНЫХ ЗВОНКОВ**

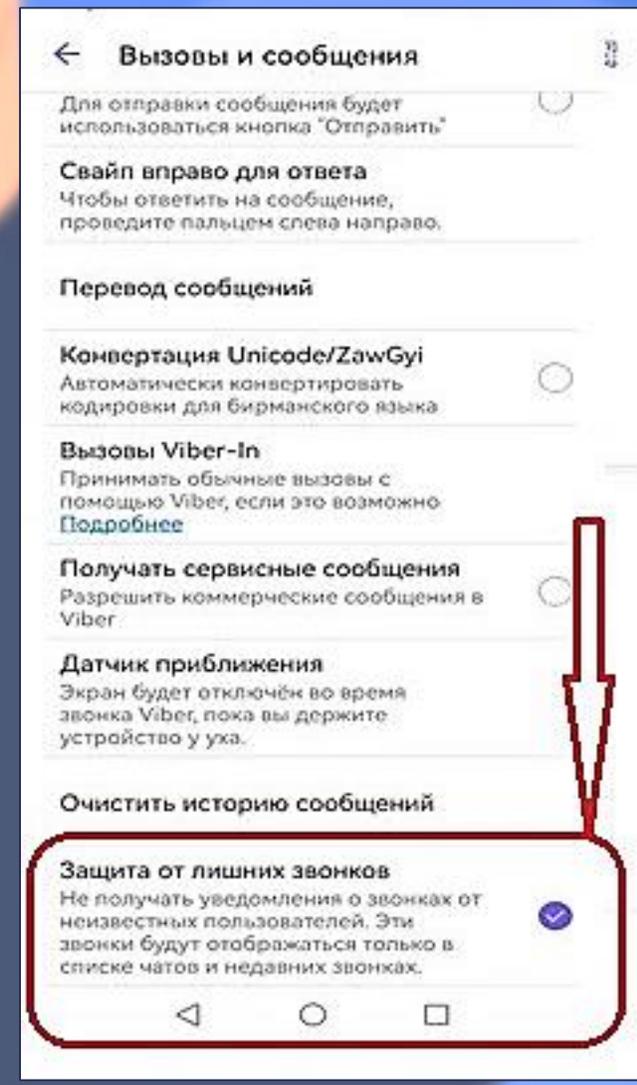
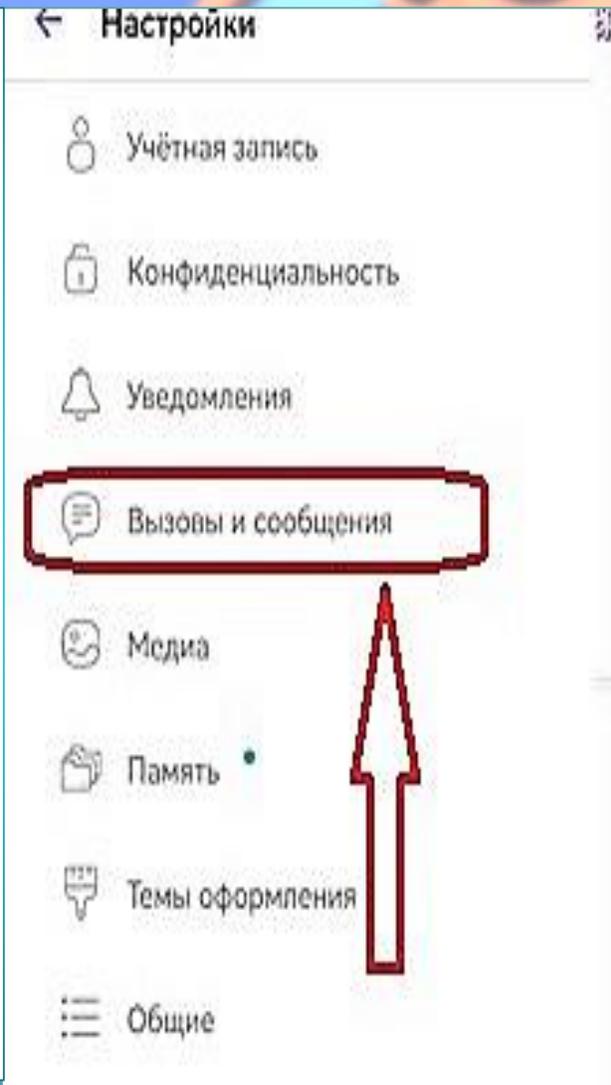
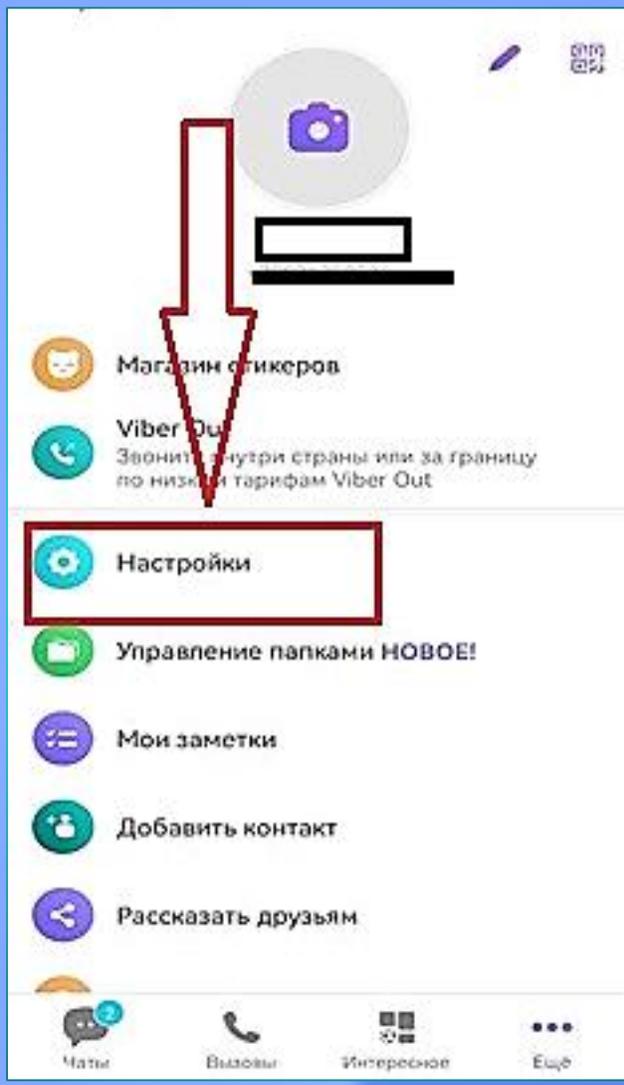
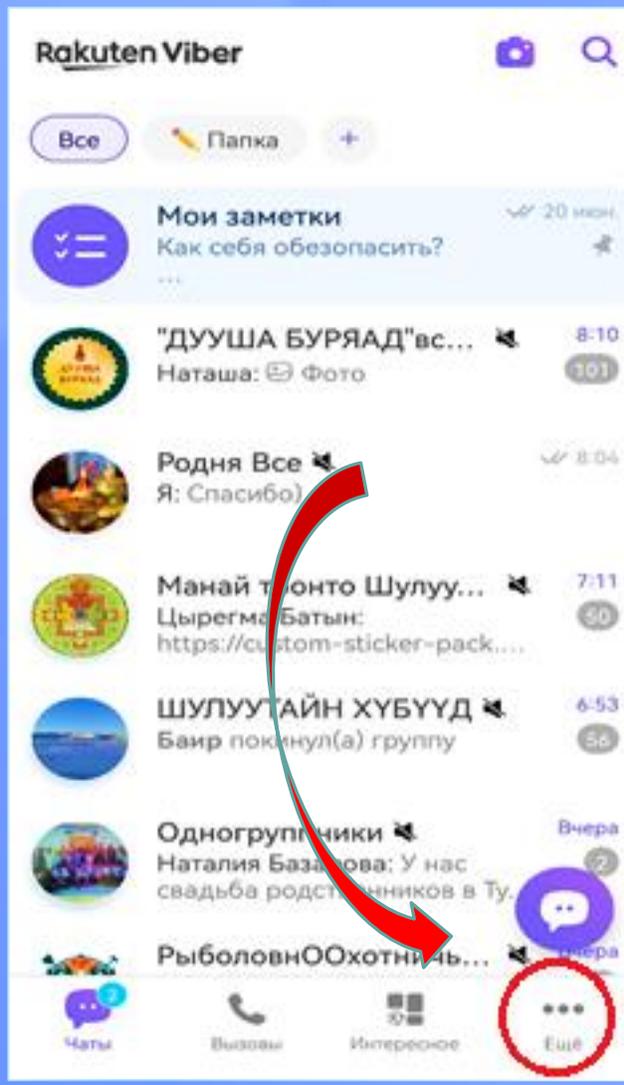
В полицию обратился 65-летний житель г. Улан-Удэ которому позвонили через мессенджер «Viber» и представились сотрудниками ФСБ, пояснили, о необходимости перевода всех его сбережений на «БЕЗОПАСНЫЙ СЧЕТ». Общий ущерб составил 3 млн. рублей.



ЖЕРТВА



Защита от звонков в Viber





Защита от звонков в WhatsApp



WhatsApp

Новая группа
Иван Иванов
Ок
Новая рассылка

Связанные устройства
Александр Але
✓ Жду. С
Избранные сообщения

Настройки

Академическое братство 02:01
~ Андрей: Фото

Мошенники России 01:03
~ Солнечная 🔥🔥🔥: Коллеги ,...

Юлия Дмитрие... Вчера
✓ Сейчас сию статистику в ин...

Степанова МАРИНА Вчера
✓ Аналогичный период прош

Чаты Статус Сообщества Звонки

← Настройки

Иван
Привет! Я использую...

Аккаунт
Уведомления безопасности,
изменение номера

Конфиденциальность
Заблокировать контакты, исчезающие
сообщения

Аватар
Создать, изменить, фото профиля

Чаты
Тема, обои, история чатов

Уведомления
Звуки сообщений, групп и звонков

Данные и хранилище
Использование сети, автозагрузка

Язык приложения
Русский (сначала выберите язык)

← Конфиденциальность

Исчезающие сообщения

Автоматический таймер сооб...
Начинайте новые чаты
с сообщениями, которые будут
исчезать в соответствии с заданным
таймером. Выкл.

Группы
Все

Геоданные
Нет

Звонки
Отключить звук для неизвестных номеров

Заблокированные
5

Блокировка приложения
Отключено

Заккрытие чата

Расширенные
Защитить IP-адрес во время звонков.

← Звонки

Отключить звук
для неизвестных номеров

Звук звонков с неизвестных
номеров будет отключён. Они
будут по-прежнему отображаться
на вкладке Звонки
и в уведомлениях. Подробнее



Защита от звонков в Telegram

3 истории

- Оксана
Все мои знакомые
- Subaru Tribeca fans
Флудилка 🎵 Автозвук,...
Сергей Прокофьев: 👉
- Отряд
Доброй ночи, стран: ❤️... 120
- Прямое попадание рос... 357
- «Спецоперация Z» | Юр... 04:59
"Даже не думайте о мире..." 32
- Прямой Эфир • Новости 04:18
Тренера молодёжной с... 547
- Очередной под... 03:38
680
- antiterror_lpr1 канал 03:01
Всём нашим тихой ночи! Б... 18
- Лещ Фандорина 2

- Мой профиль
- Создать группу
- Контакты
- Звонки
- Люди рядом
- Избранное
- Настройки** !
- Пригласить друзей
- Возможности Telegram

Чтобы Вы всегда могли зайти в Telegram, важно указать актуальный номер телефона. Подробнее

Да Нет

Настройки

- Настройки чатов
- Конфиденциальность**
- Уведомления и звуки
- Данные и память
- Энергосбережение
- Папки с чатами
- Устройства
- Язык Русский

Telegram Premium

Конфиденциальность

Устройства 1

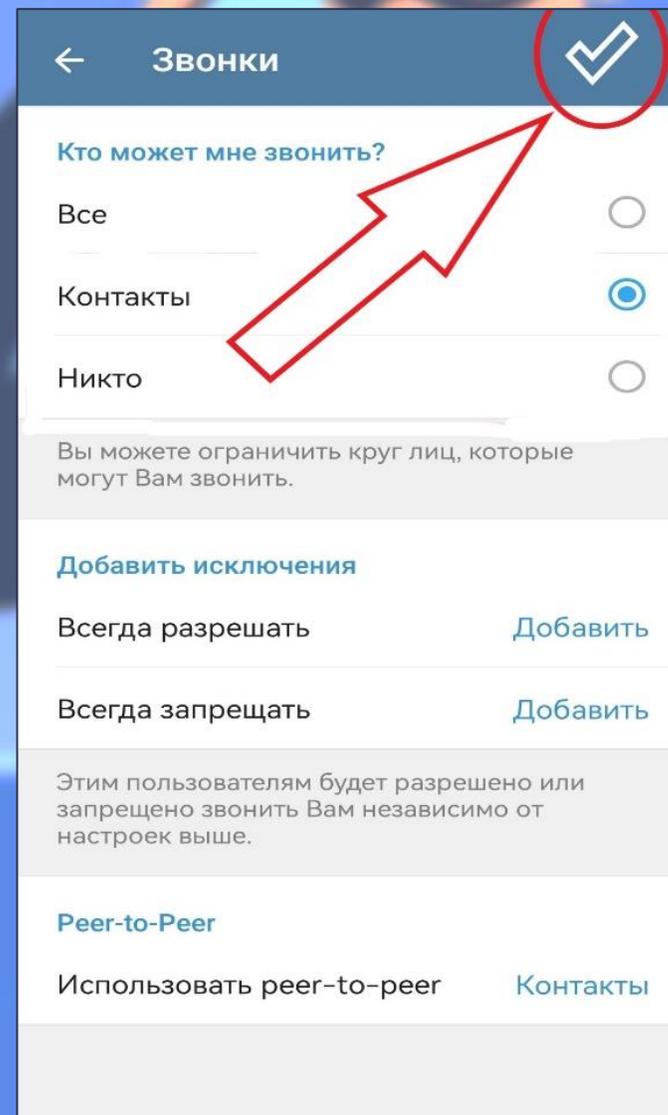
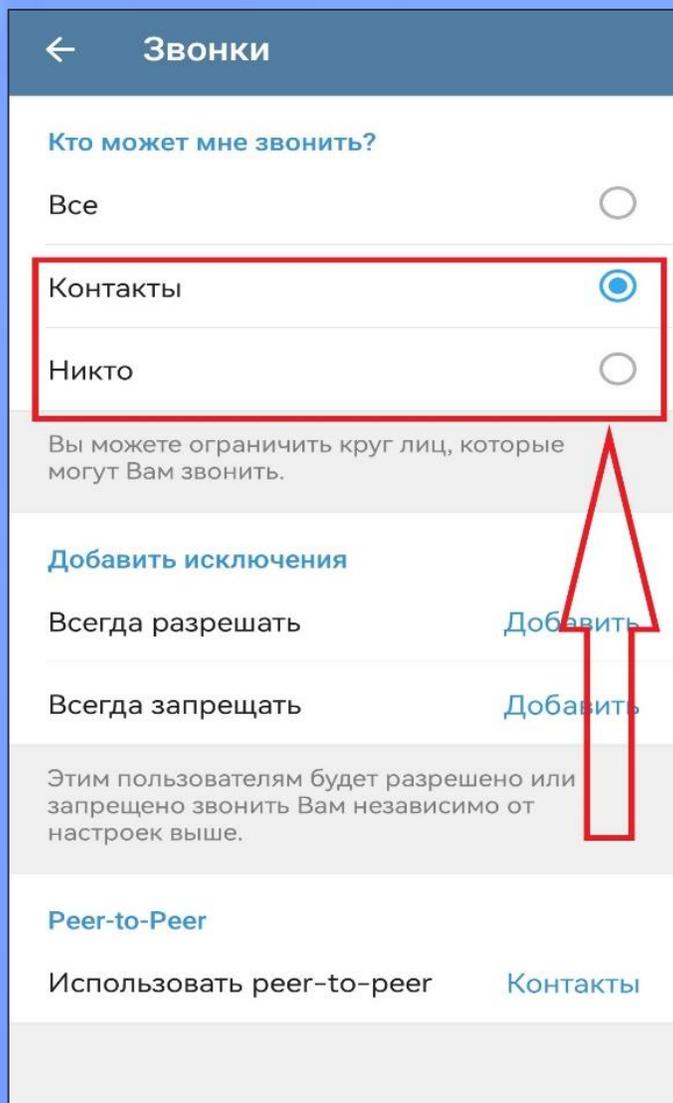
Просмотреть список устройств, на которых Ваш аккаунт авторизован в приложении Telegram.

Конфиденциальность

- Номер телефона Контакты
- Время захода Никто
- Фотографии профиля Контакты
- Пересылка сообщений Контакты
- Звонки** Контакты
- Голосовые сообщения ☆ Все
- Сообщения Все
- Дата рождения Контакты
- О себе Все



Защита от звонков в *Telegram*



СИМ-КАРТА – ЭТО ВАШ ВТОРОЙ ПАСПОРТ;



**Абонентский номер привязан к аккаунтам, к личным кабинетам банков, к порталу «Госуслуги»;
Если вы сменили номер, то открепите старый абонентский номер от банков и госуслуг;
Установите дополнительную защиту личного кабинета;**



4 СПОСОБ ИСПОЛЬЗОВАНИЕ СТАРОЙ СИМ-КАРТЫ

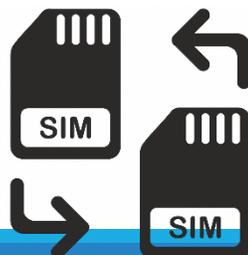


**ЧЕРЕЗ 2-6 МЕС СТАРАЯ СИМКАРТА ВНОВЬ
ОФОРМЛЯЕТСЯ НА НОВОГО АБОНЕНТА,
МОШЕННИК:**

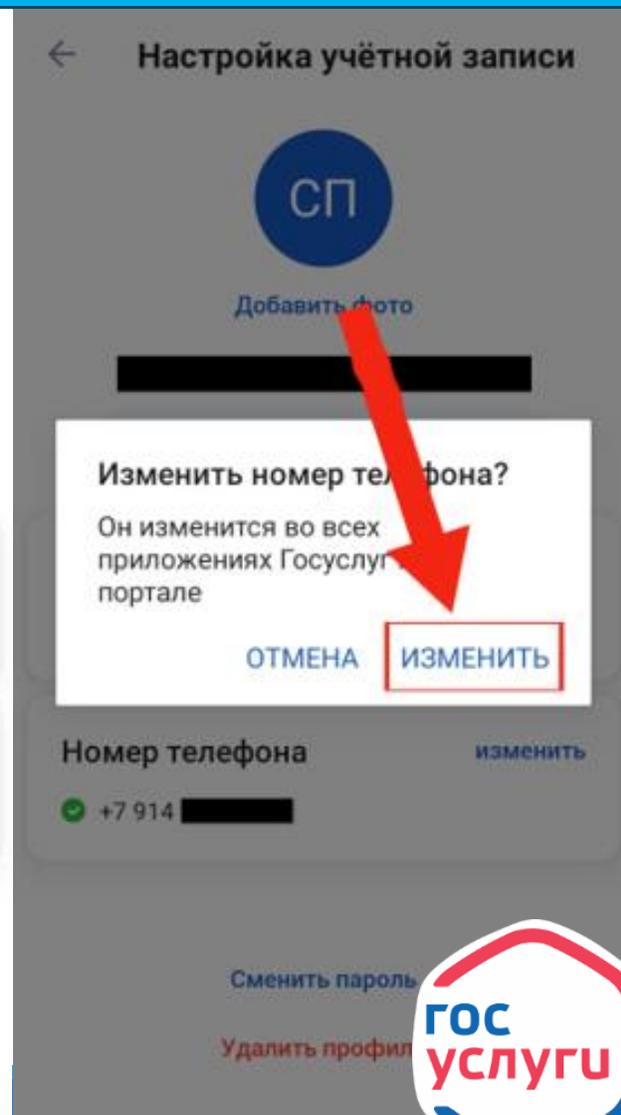
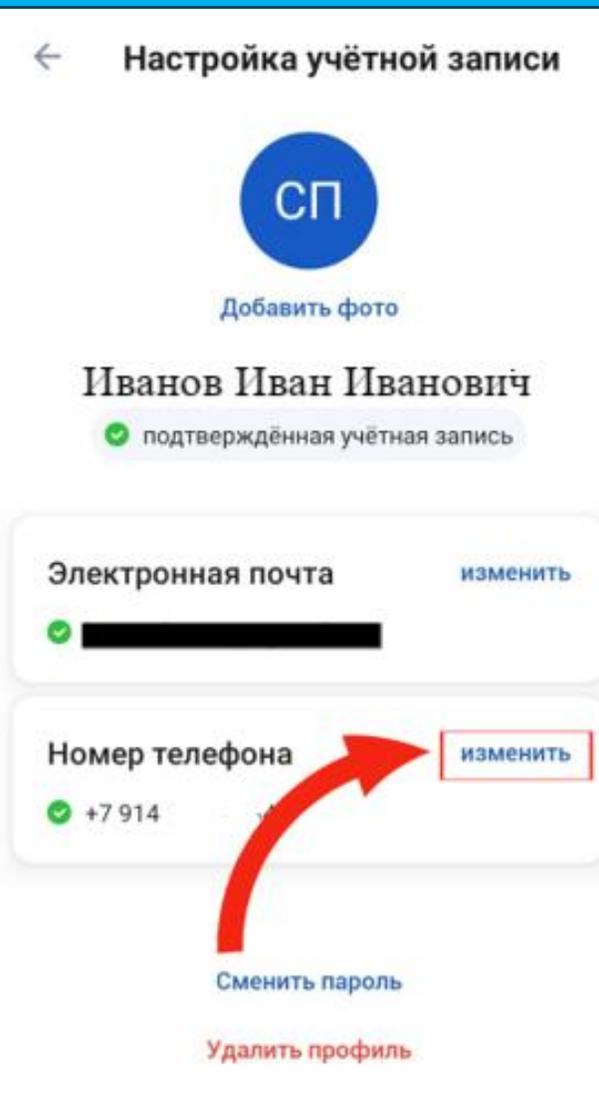
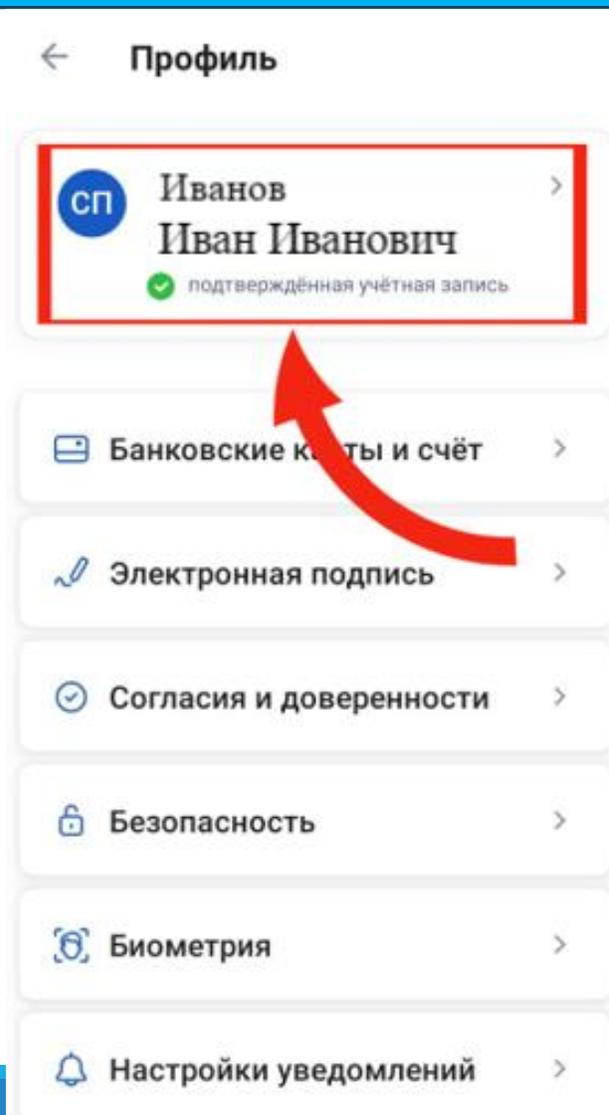
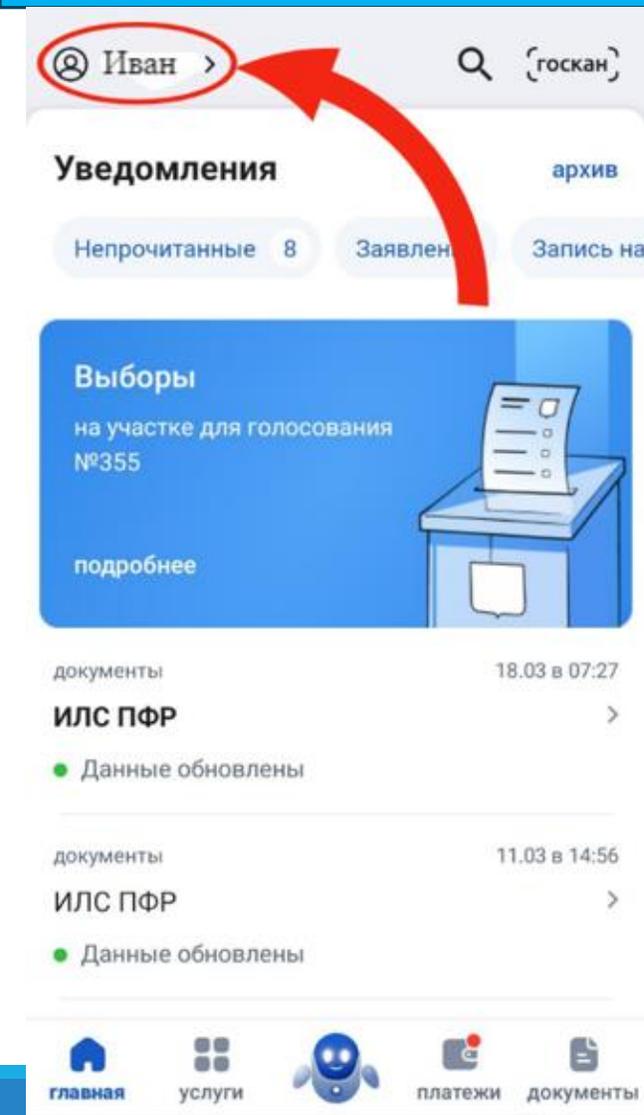
- **ПРИБРЕТАЕТ СИМ-КАРТУ;**
- **ПРОВЕРЯЕТ НА НАЛИЧИЕ ПРИВЯЗАННЫХ
ЛИЧНЫХ КАБИНЕТОВ «ГОСУСЛУГ», БАНКОВ,
КРЕДИТНЫХ ОРГАНИЗАЦИЙ;**
- **ОФОРМЛЯЕТ КРЕДИТ, МИКРОЗАЙМЫ;**
- **ПЕРЕВОДИТ ВСЕ ВАШИ ДЕНЬГИ.**



ЖЕРТВА



Наглядный пример открепления старого номера телефона





Наглядный пример открепления старого номера телефона

← Изменение телефона

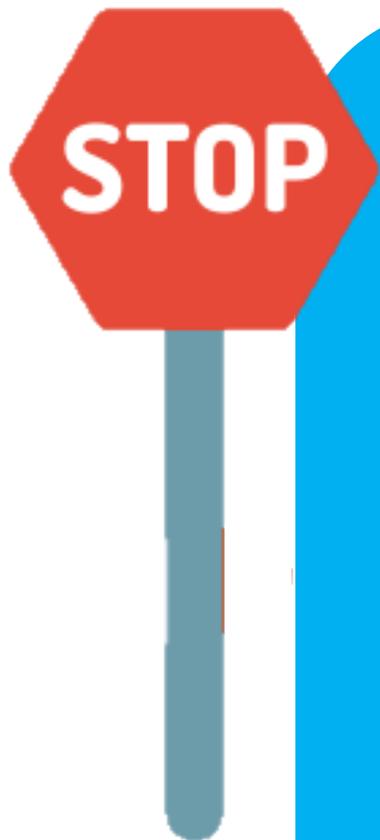
Есть доступ к старому номеру
+7 914 [REDACTED]

Да >

Нет >

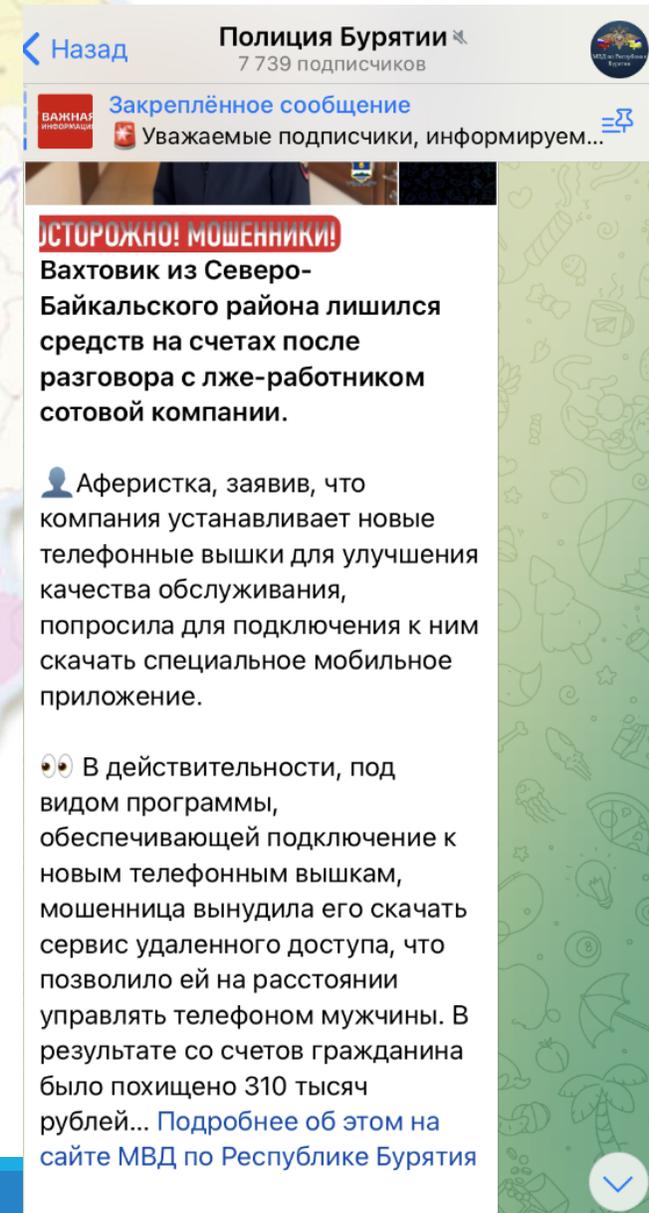
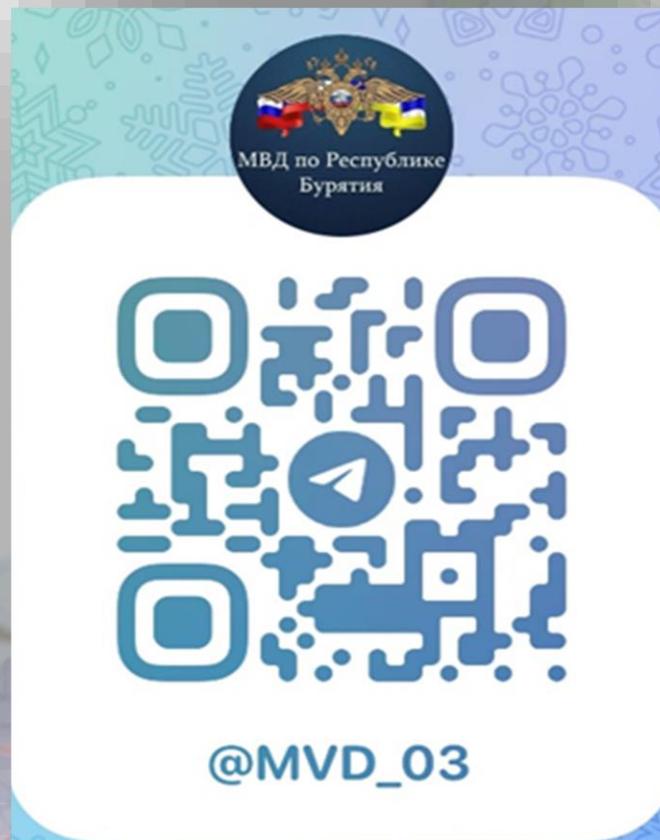
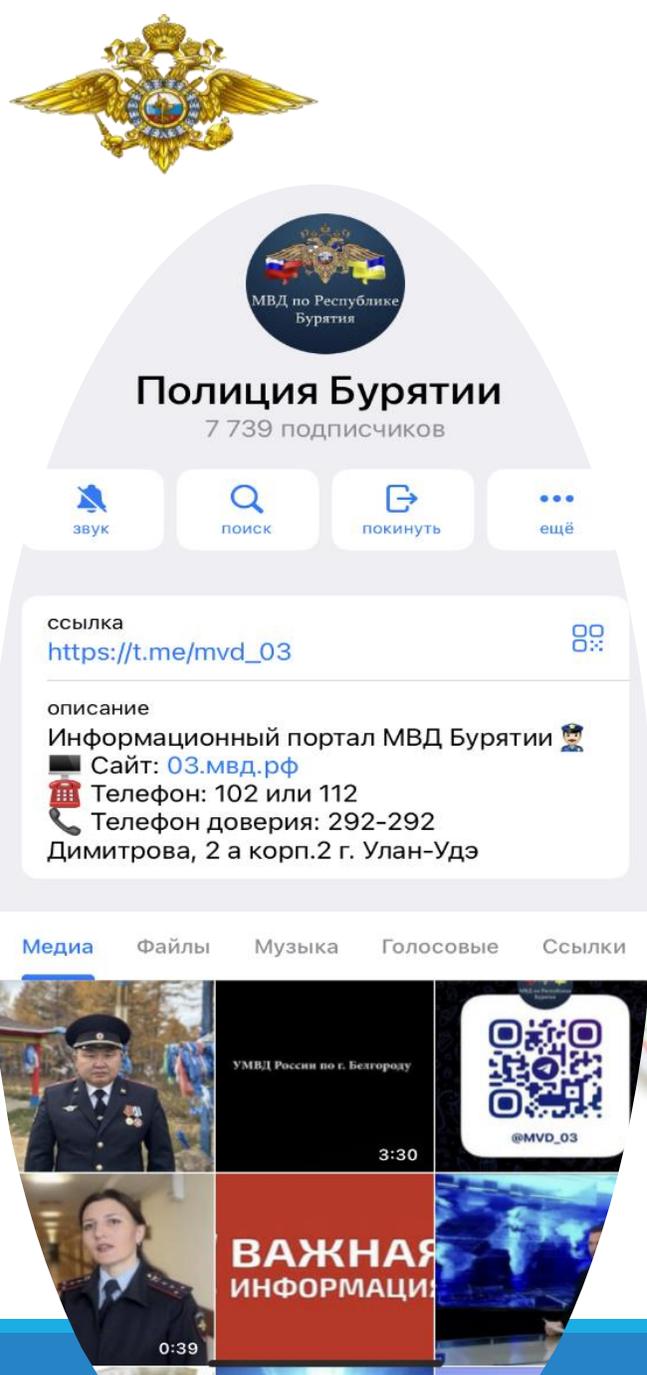


5 ОСНОВНЫХ ПРАВИЛ БЕЗОПАСНОСТИ ОТ КИБЕРПРЕСТУПЛЕНИЙ



- **НИКОГДА** не скачивать приложения или обновления через ссылки, которые приходят по смс, в мессенджерах или по почте (доверяйте только проверенным магазинам для Iphone- App Store, для Android – Google Play Store).
 - **НЕ** называть код из СМС;
 - **НЕ** отвечать на звонки с неизвестных номеров, **ПРЕРВИТЕ** разговор, если он касается финансовых вопросов;
 - **НЕ** переводить деньги на неизвестные, «безопасные» счета;
- НЕ ТОРОПИСЬ** принимать решение, самостоятельно позвоните близкому человек, в банк, в полицию!

МВД по Республике Бурятия в «Telegram» (актуальная информация по профилактике ИТТ-преступлений)



ПРИМЕР:

В апреле 2024 года в полицию обратился 46-летний житель г. Улан-Удэ, который в ходе телефонного разговора с лже-сотрудником сотовой компании сообщил коды от Госуслуг поступившие на его телефон.

Далее с ним связался якобы работник портала Госуслуг, который сообщил, что мошенники взломали его личный кабинет, а так же предупредил, что с потерпевшим свяжутся сотрудники ФСБ.

Через несколько минут с ним связался лже-сотрудник ФСБ, который сообщил, что мошенники используя анкетные данные заявителя подали в банк заявку на оформление кредита, в целях пресечения действий мошенников необходимо опередить мошенников и оформить кредит самостоятельно. После чего потерпевший в одном из банков г. Улан-Удэ оформляет кредит на сумму 1 миллион рублей, при этом по указанию лже-сотрудника ФСБ сообщил банковскому менеджеру, что оформляет кредит на покупку автомашины.

После получения кредитных денежных средств он их переводит на якобы специальный «безопасный счет».



ПРИМЕР:

В октябре 2024 года в полицию обратился 65-летний житель г. Улан-Удэ, который работает преподавателем в одном из учебных заведений г. Улан-Удэ, которому в мессенджере «Ватсап» поступило сообщение от якобы заместителя директора, который сообщил, что по вине их бухгалтерии произошла утечка персональных данных сотрудников учебного заведения и по этому поводу будет проводиться проверка со стороны сотрудников «ФСБ». Далее лже-замдиретора сообщил о том, что персональные данные потерпевшей и её коллег подверглись разглашению неизвестными лицами и сообщил о скором звонке сотрудника «ФСБ». Спустя некоторое время так же в мессенджере «Ватсап» позвонил мужчина, который представился сотрудником «ФСБ» Антроповым и сообщил, что в их учебном заведении произошла утечка персональных данных сотрудников, и что с банковского счета потерпевшей мошенники хотят похитить денежные средства в сумме 750 тыс. рублей, после чего лже-сотрудник «ФСБ» Антропов сообщил, что для сохранности денежных средств, ей необходимо перевести все свои накопления на «БЕЗОПАСНЫЙ СЧЕТ», в чем потерпевшая окажет помощь сотруднику финансового отдела ФСБ Икоркину. Далее по указанию лже-сотрудника «ФСБ» потерпевший последовал в отделение банка и со своего накопительного счета перевел денежные средства в размере 500 тыс. руб., далее так же по указанию лже-сотрудника «ФСБ» потерпевший аналогичным способом перевел на якобы «БЕЗОПАСНЫЙ СЧЕТ» денежные средства в общей сумме 2 360 000 рублей. Кроме того, по указанию лже-сотрудника «ФСБ», потерпевший приобрел новый сотовый телефон, для якобы конфиденциальной беседы. О том, что это были мошенники осознал после того, как сверил абонентский номер лже-директора в мессенджере «Ватсап».

В марте 2024 года в полицию обратился 63-летний мужчина о том, что в сети интернет он увидел рекламу компании «Тинькофф Инвестиции» и зарегистрировался на их сайте. Далее на его сотовый телефон позвонил лже-сотрудник «Тинькофф банка» и предложил заработать на инвестициях. Мужчина решив попробовать установил приложение «БайБит» для обмена денежных средств на криптовалюту и приложение «ТЕРМИНАЛ» для совершения сделок и отслеживания баланса «инвестиционного счета».

После установки приложений заявитель перевел денежные средства в размере 10 000 рублей на свой «инвестиционный счет» и под руководством приставленного консультанта потерпевший за несколько дней якобы заработал 100 долларов США.

Для получения еще большей прибыли, заявитель в течении недели внес на «инвестиционный счет» денежные средства в размере 1 миллиона 280 тысяч рублей.

Далее когда баланс на виртуальном счете составлял более 2 миллионов рублей он самостоятельно попытался вывести денежные средства с «инвестиционного счета», но в процессе пришло уведомление о том, что приложение «ТЕРМИНАЛ» заблокировано в виду подозрительной активности.

Сотрудник технической поддержки сообщил, что в результате самовольных действий потерпевшего якобы были заблокированы счета компании, необходимо оплатить штраф в размере 1 000 000 рублей, а для вывода средств необходимо внести страховой взнос и налоговый вычет в сумме 900 тысяч рублей.

После чего потерпевший на имя супруги оформил несколько кредитов на общую сумму 1 986 000 рублей которые перевел на счета злоумышленников, полагая, что получит свои якобы заработанные денежные средства.

ПРИМЕР:

В августе 2024 года в полицию поступило заявление 35-летнего жителя г. Улан-Удэ, о том, что в одном из банков на его имя оформлен кредит на сумму 1 млн. рублей, который он сам не оформлял.

В ходе проверки установлено, что кредит оформлен мошенником с использованием старого абонентского номера потерпевшего, которым последний перестал пользоваться и не открепил от личного кабинета банка.

Кроме того в сентябре 2024 года в полицию обратилась студентка одного из учебных заведений г. Улан-Удэ, о том, что по ее старому абонентскому номеру, который она не отвязала от личного кабинета портала Госуслуги, был осуществлён вход в ее личный кабинет данного портала, с помощью которого были оформлены несколько микрозаймов на общую сумму 250 000 рублей.