Управление МВД России по г. Улан-Удэ

ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ ОТ КИБЕРПРЕСТУПЛЕНИЙ

СТАТИСТИЧЕСКИЕ ДАННЫЕ ЗА 2024 год

- **По Республике зарегистрировано:**
- 2847 мошенничеств (рост на 3,4%);
- 972 краж с банковских счетов (снижение на 34,0%);
- 1856 взлома портала «ГОСУСЛУГИ» (РОСТ НА 336,7%).

- **По г. Улан-Удэ зарегистрировано:**
- 1722 мошенничества (снижение на 6,0%);
- 581 краж с банковских счетов (снижение на 36,4%);
- 1045 взлома портала «ГОСУСЛУГИ» (РОСТ НА 262,8%).

Профилактическая работа

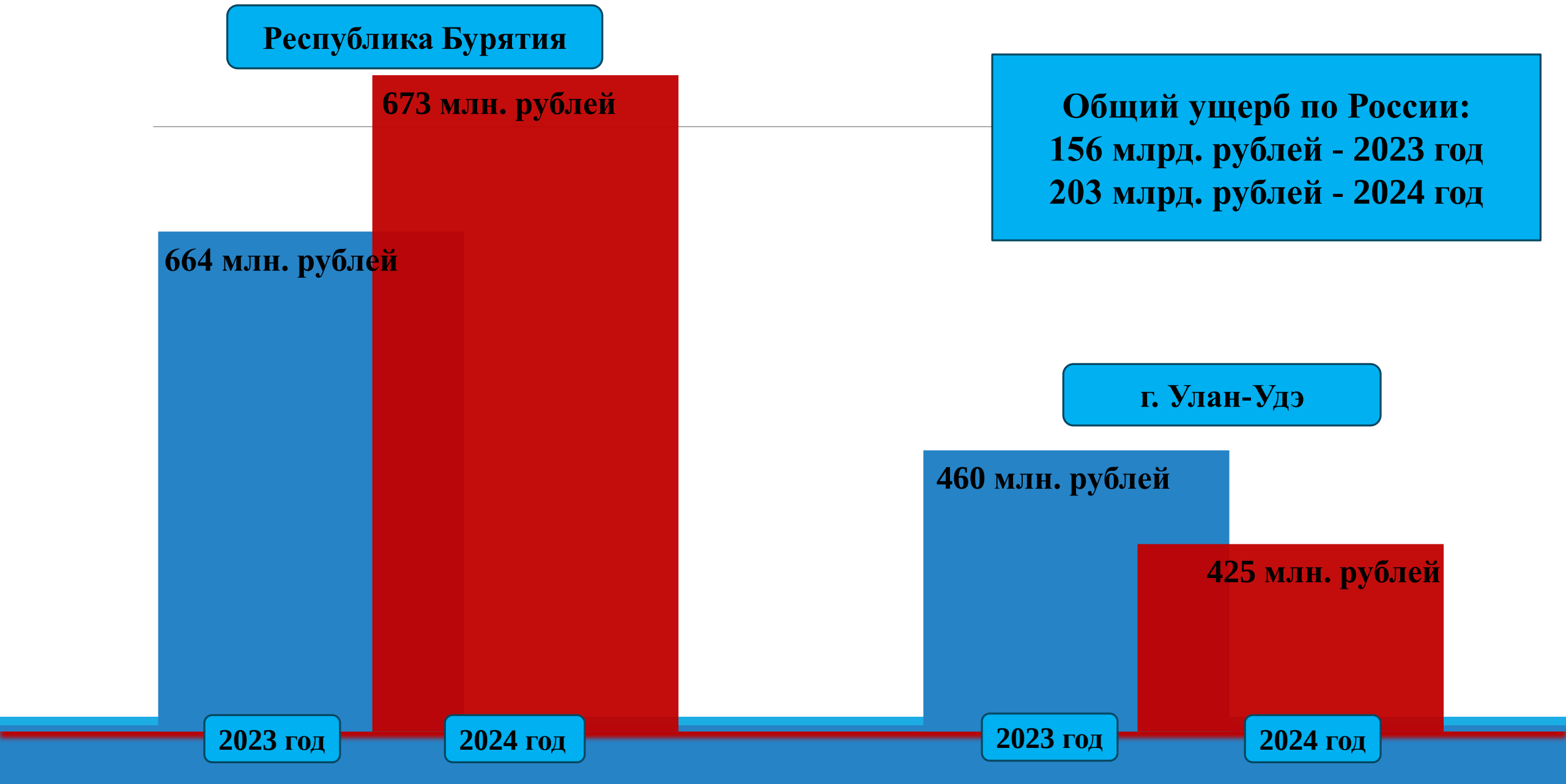
Ежедневно сотрудниками полиции проводится не менее 20 встреч. Всего в 2024 году на территории Республики Бурятия проведено 19 978 встреч с населением, охват составил 477 547 человек; по г. Улан-Удэ проведено 7369 встреч с населением, охват составил 216 077 человек.

Руководством МВД России проводимая МВД по Республике Бурятия работа признана передовым опытом и направлена в регионы с указанием о практическом внедрении.

Совместная работа с банками по разработанному алгоритму

Всего в 2024 году, сотрудниками полиции во взаимодействии с сотрудниками банков удалось предотвратить материальный ущерб
общую сумму 65 986 000 рублей!

Ущерб за 2023-2024 год



ГЕОЛОКАЦИЯ МОШЕННИЧЕСКИХ КОЛЛ-ЦЕНТРОВ

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 и т.д.;

Сотрудника пенсионного фонда:
- говорит о перерасчете пенсии;
- предлагает получить единовременную выплату и т.д.;

ЖЕРТВА

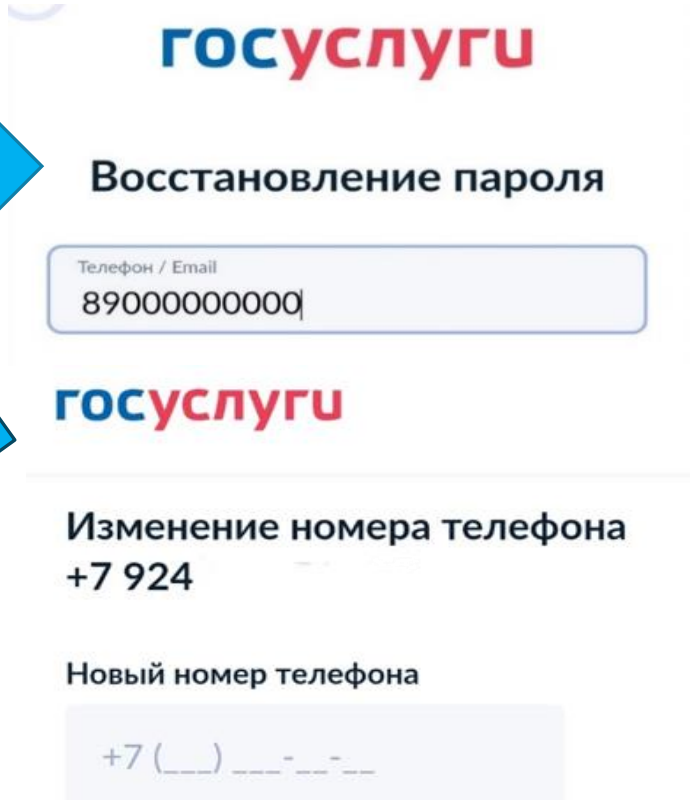
ЗВОНИТ ЖЕРТВЕ, ПРОСИТ СООБЩИТЬ СМС КОД, ПОД ПРЕДЛОГОМ

Сотрудника здравоохранения:
-Предлагает продлить срок действия страхового полиса;
-Запись по электронной очереди и т.д.;
Сотрудника коммунальных служб:
-Предлагает замену электросчетчиков
-Скачать приложение;
Сотрудника Госуслуг
-Сообщает о взломе личного кабинета и т.д.;

Последствия передачи СМС-кода

Входит в Госуслуги

Заполучив доступ



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

МЕРЫ БЕЗОПАСНОСТИ

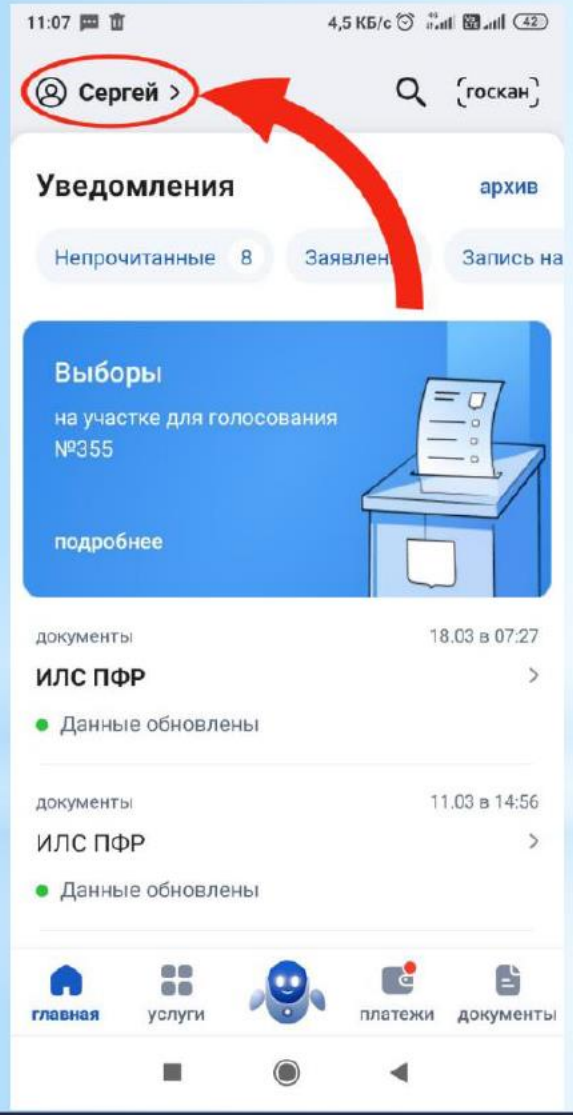
- **НЕ ОТВЕЧАЙ** на звонки с неизвестных номеров;
- **ТОЛЬКО** мошенники звонят в мессенджерах;
- **ЗАПОМНИ,** представители государственных учреждений и операторы сотовой связи **НИКОГДА** не просят СМС-коды!!!

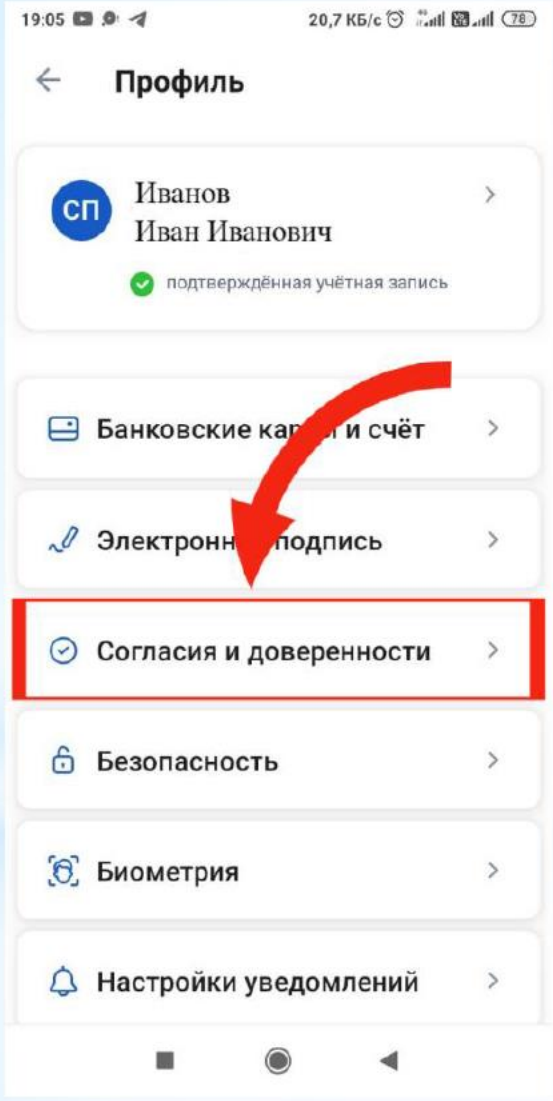
КОД из **СМС** – это аналог вашей; собственной подписи. Его **НИКОГДА** и **НИКОМУ** нельзя сообщать или пересылать!

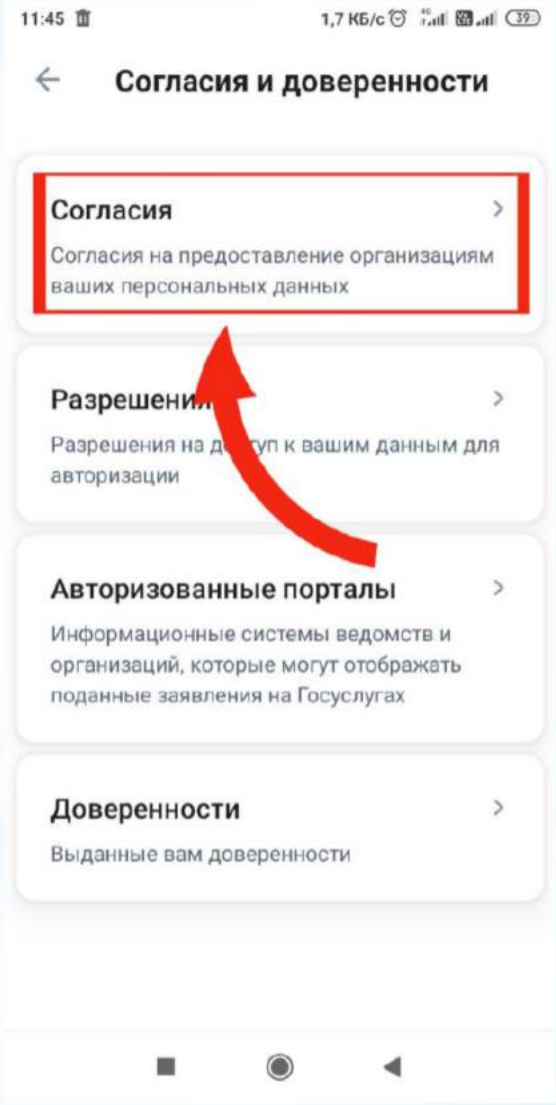
Внимание! Достаем телефоны!

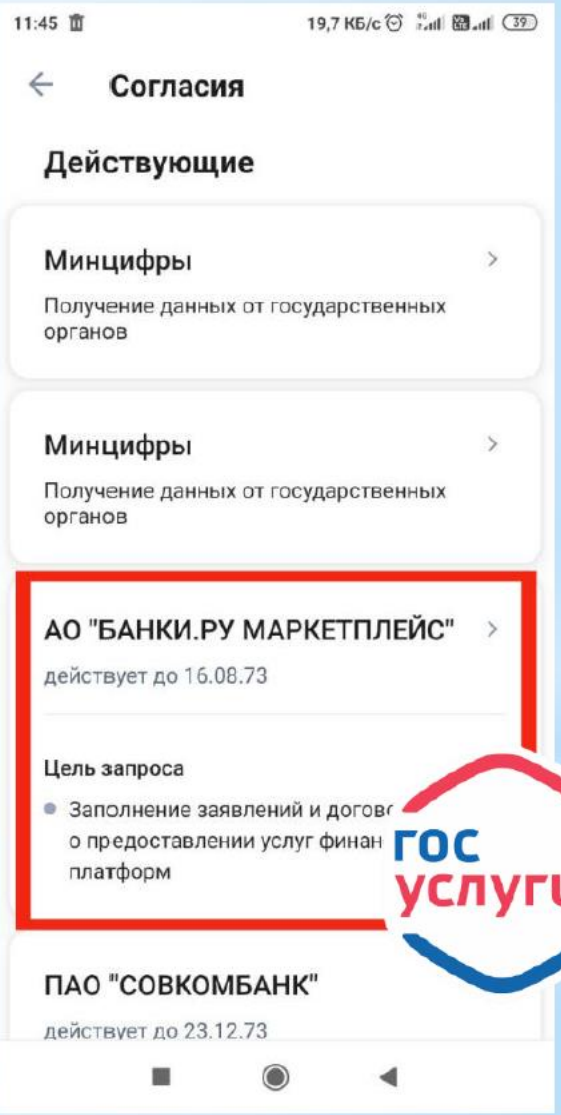
Рекомендуем отозвать согласие на обработку персональных данных с банками, что бы мошенники получив доступ к порталу «Госуслуги», не могли оформить на Вас кредит!!!

Отзыв согласий

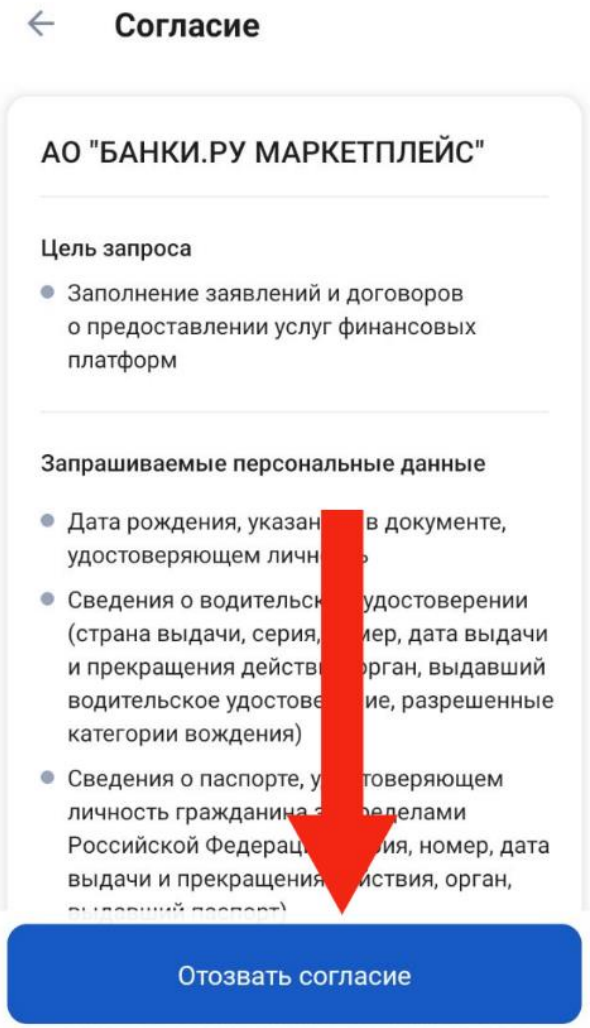


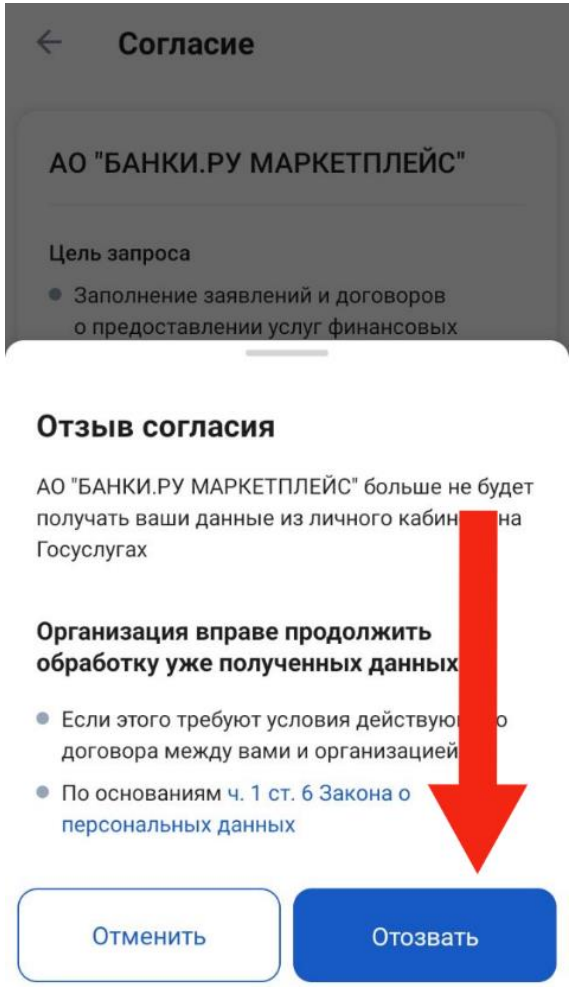


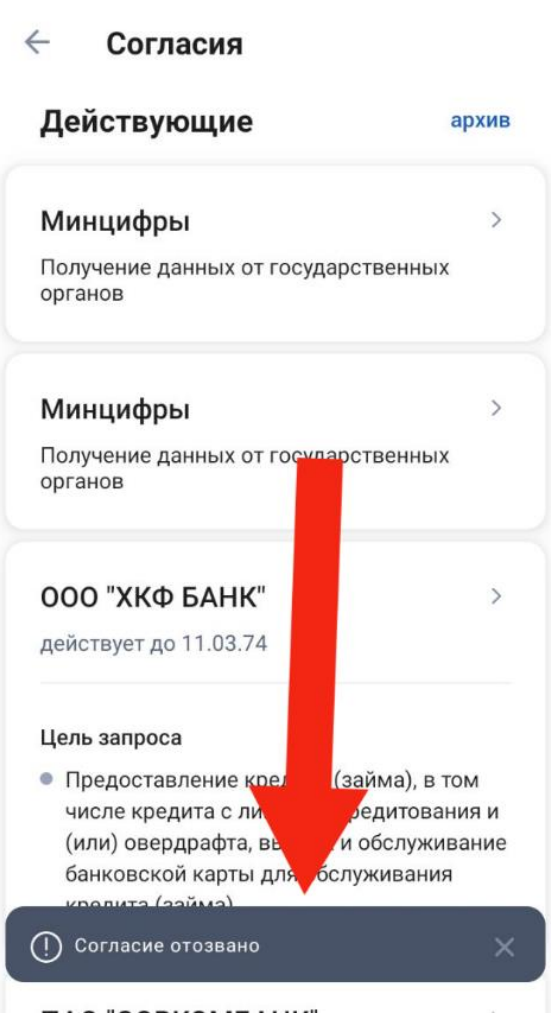




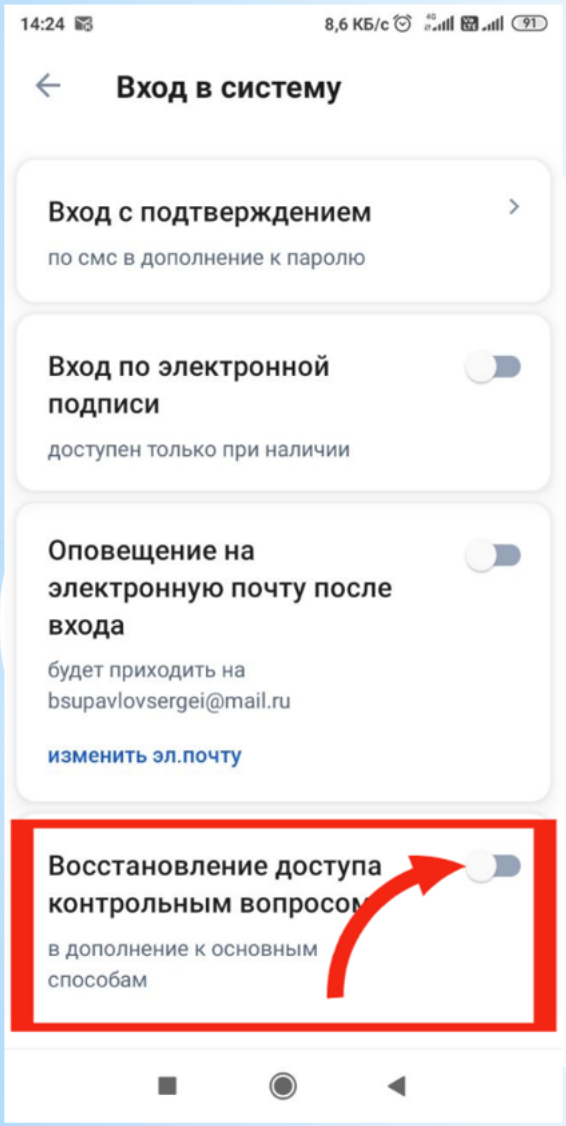
Отзыв согласий

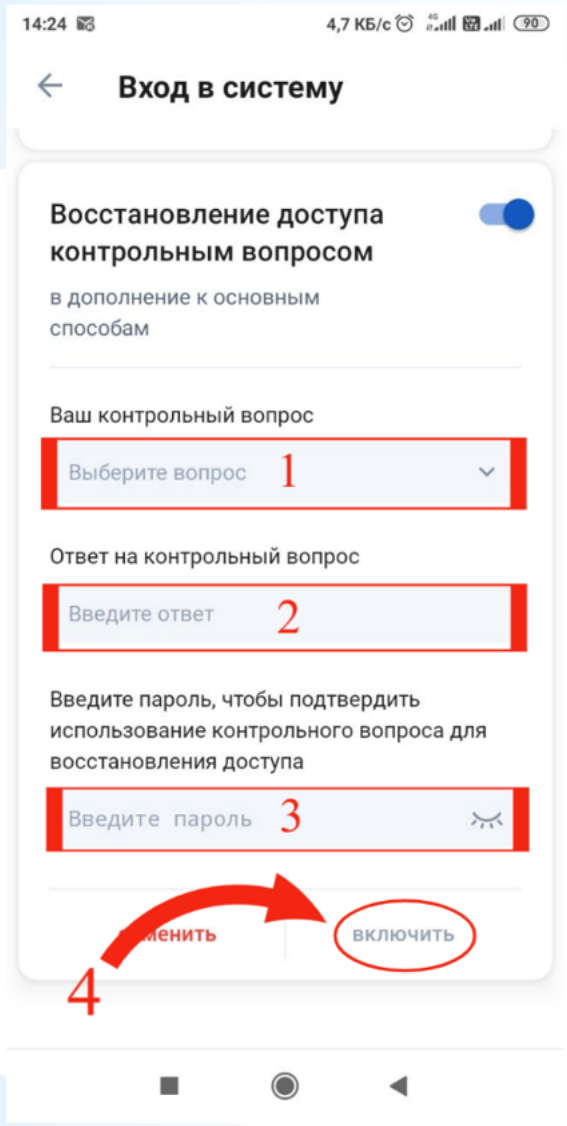






Дополнительная защита личного кабинета





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.

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 и т.д.);**

ЖЕРТВА

СООБЩЕНИЕ ОТ РУКОВОДИТЕЛЯ

МОШЕННИК

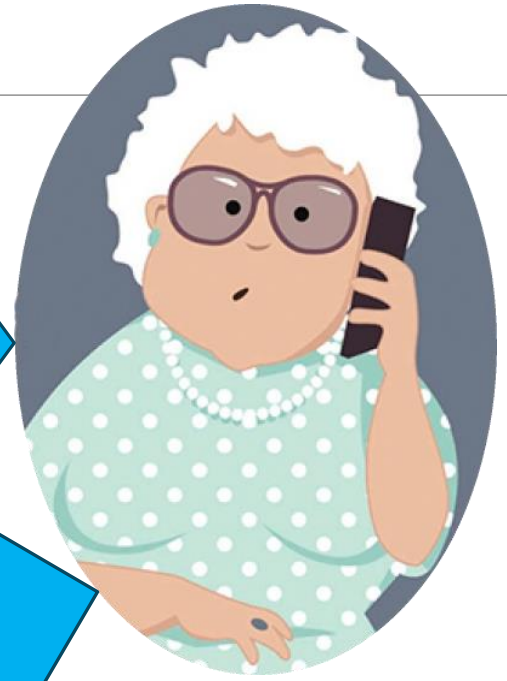
в схему вступает лже-сотрудник ФСБ, МВД, который грозит блокировкой счета, по которому якобы зафиксированы сомнительные операции, либо, кто-то пытается оформить кредит на имя жертвы, настаивает перевести личные деньги или оформить кредит, затем перевести их на якобы «БЕЗОПАСНЫЙ СЧЕТ»

ЖЕРТВА

Пример: Приложение 2

3 СПОСОБ МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ ЗАРАБОТКА В СЕТИ ИНТЕРНЕТ

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



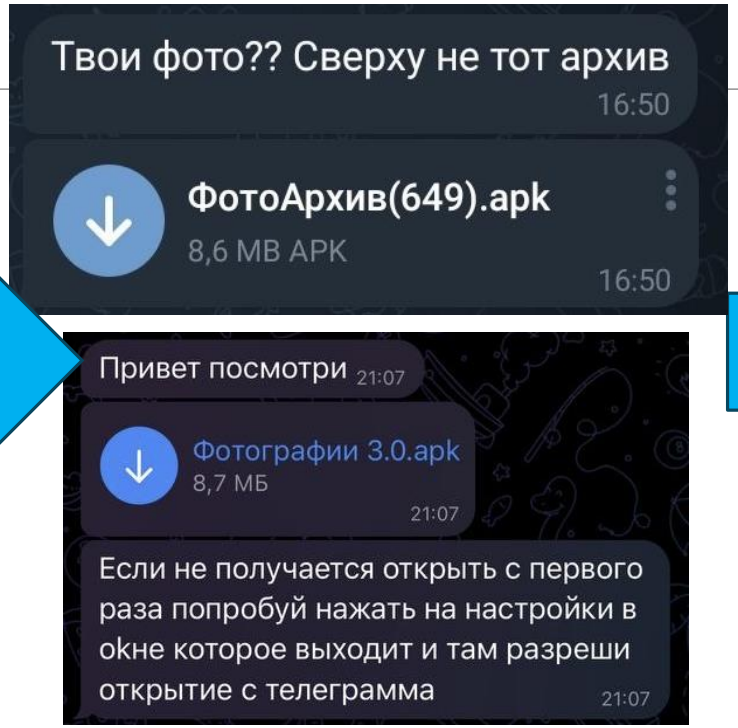
- Видит мнимый доход;
- Вкладывает личные, либо кредитные деньги.

За 2024 год 141 жители г. Улан-Удэ вложили в инвестиции более 128 млн. рублей

- **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!**

4 СПОСОБ МОШЕННИЧЕСТВА «ЭТО ТЫ НА ФОТО?»

Мошенник под видом знакомого отправляет фотографию



ЖЕРТВА

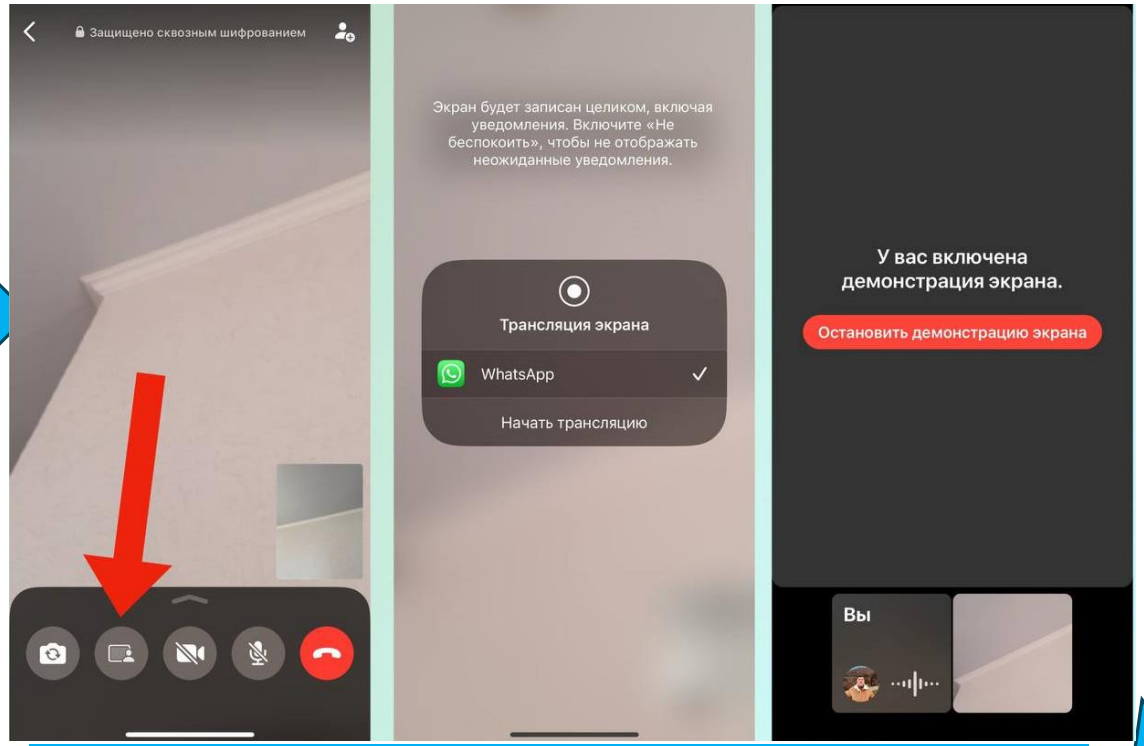
- **переходит по ссылке ➡ в сотовый телефон устанавливается вирусное (невидимое) приложение;**
- **мошенник получает дистанционный доступ к управлению сотового телефона жертвы ➡ оформляет кредит, переводит личные денежные средства, направляет смс-рассылки;**

Пример: Приложение 4

5 ДЕМОНСТРАЦИЯ ЭКРАНА СМАРТФОНА,

звонивший мошенник под разными предлогами просит включить демонстрацию экрана

Звонит жертве



Включает демонстрацию

- Трансляция позволяет мошеннику увидеть номера карт, суммы на счетах, СМС-коды от банка, мошенник получает доступ к личному кабинету жертвы, переводит все денежные средства, оформляет кредит.

КАК ОБЕЗОПАСИТЬ ЧАСТНУЮ ПЕРЕПИСКУ

- НЕ проходите по ссылкам в сообщениях;
- НЕ открывайте вложенные файлы;
- НЕ скачивайте приложения по ссылкам;

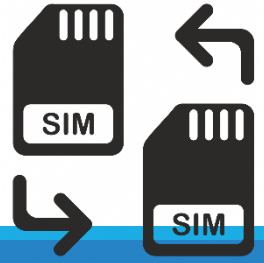
Если пришло сообщение от ЗНАКОМОГО ЧЕЛОВЕКА с просьбой занять денежные средства, свяжитесь с ним другим способом и уточните лично;

6 СПОСОБ
ИСПОЛЬЗОВАНИЕ СТАРОЙ СИМ-КАРТЫ

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

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

ЖЕРТВА

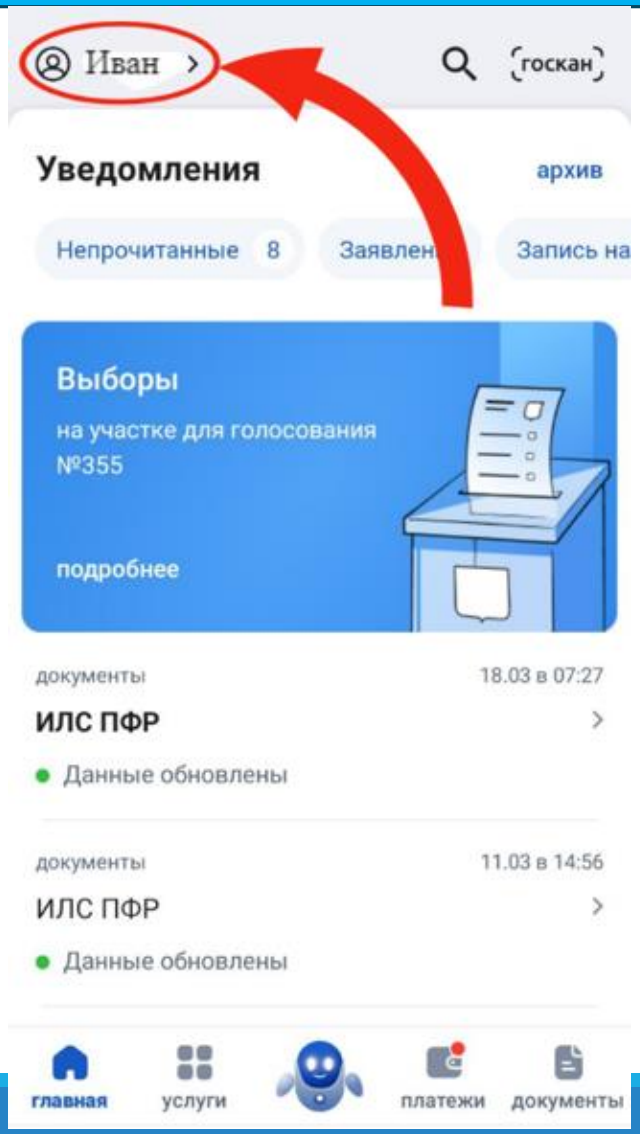


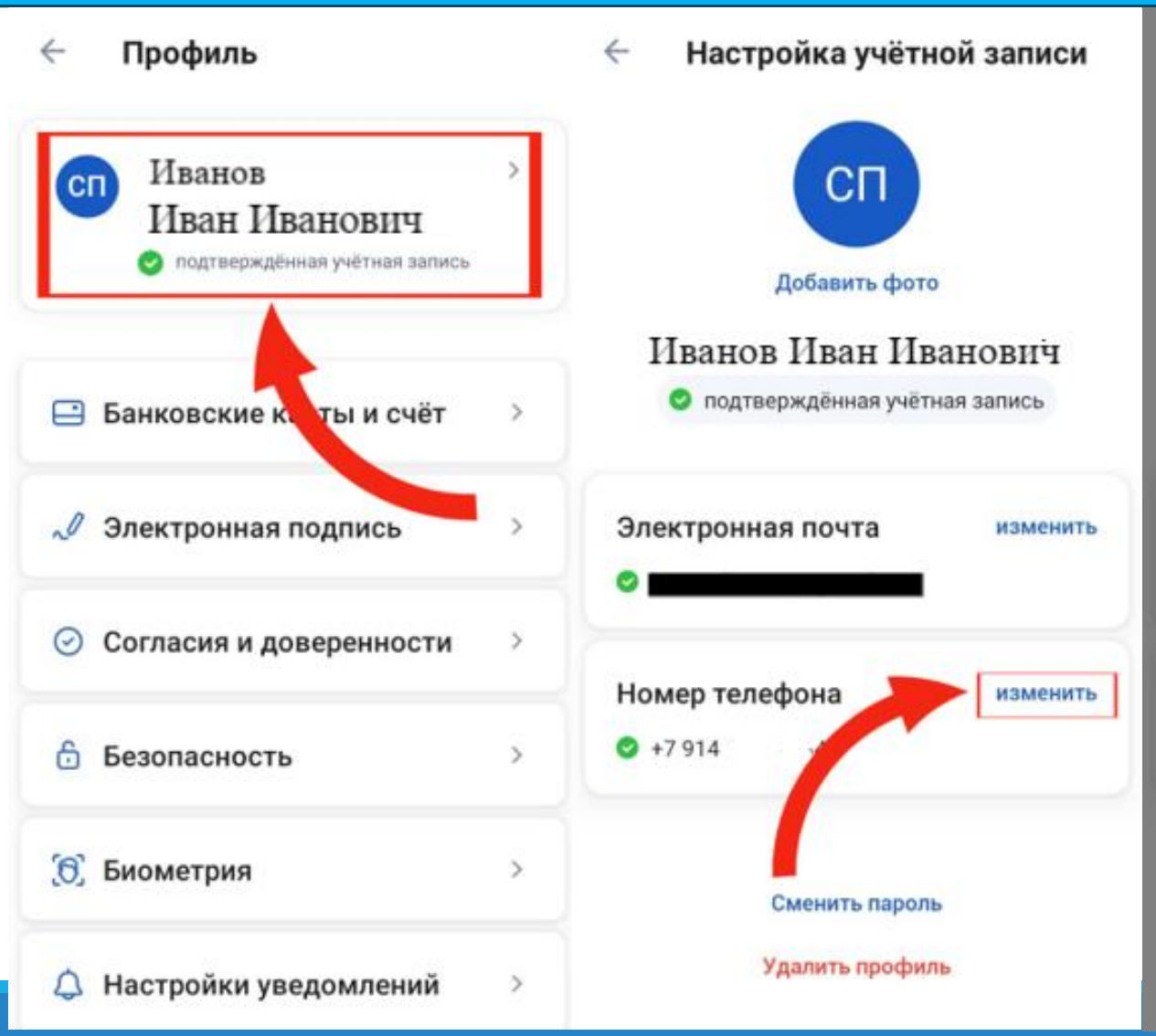
Пример: Приложение 6

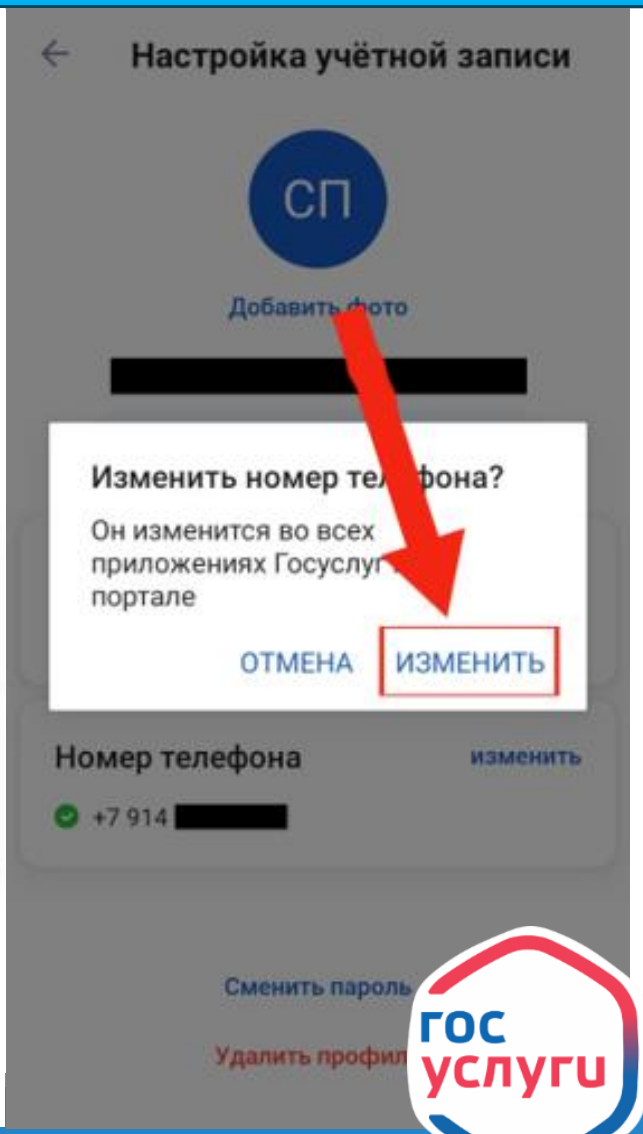
СИМ-КАРТА – ЭТО ВАШ ВТОРОЙ ПАСПОРТ;

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;

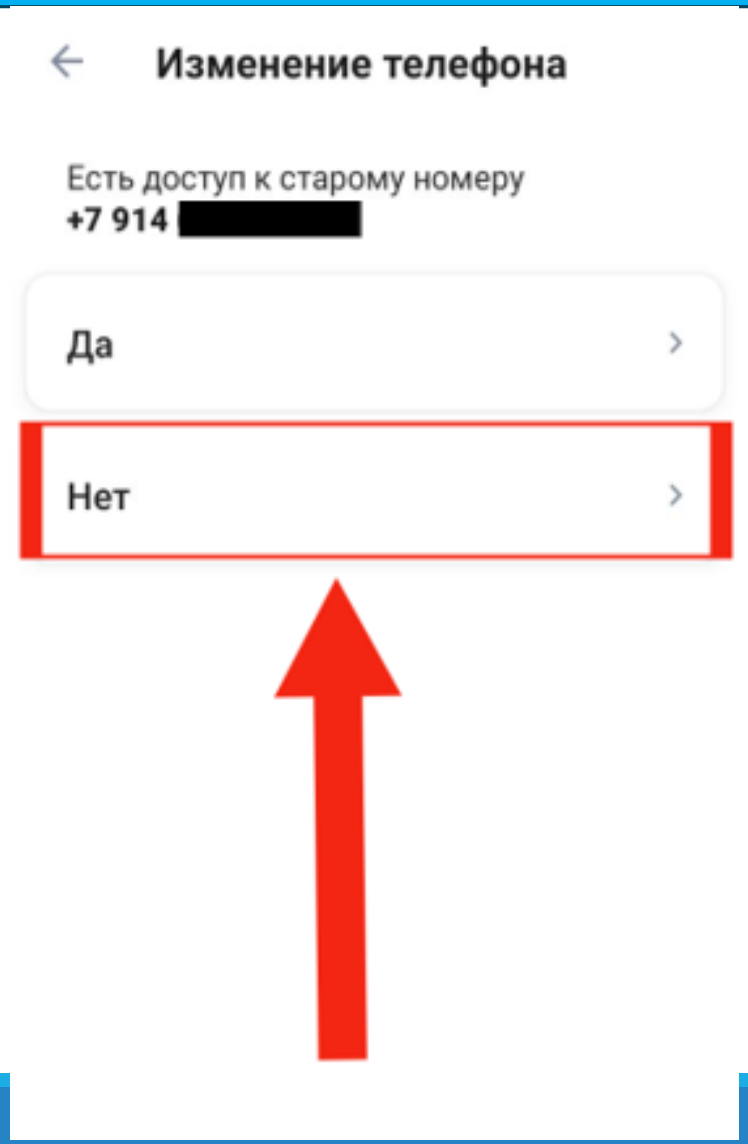
Наглядный пример открепления старого номера телефона







Наглядный пример откреплення старого номера телефона



КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ

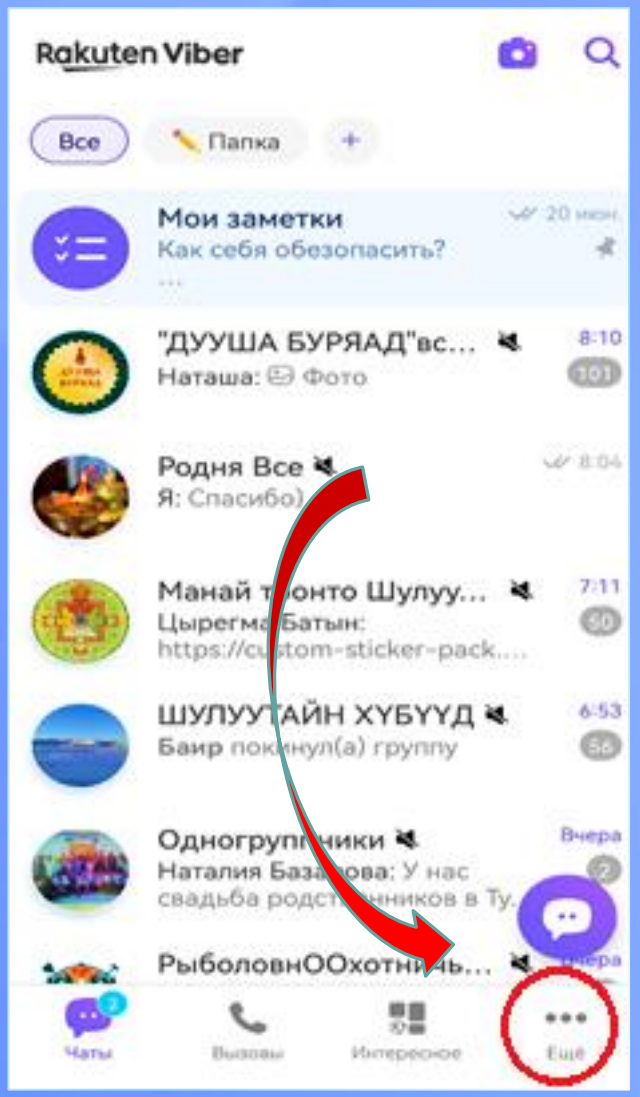
МОШЕННИК

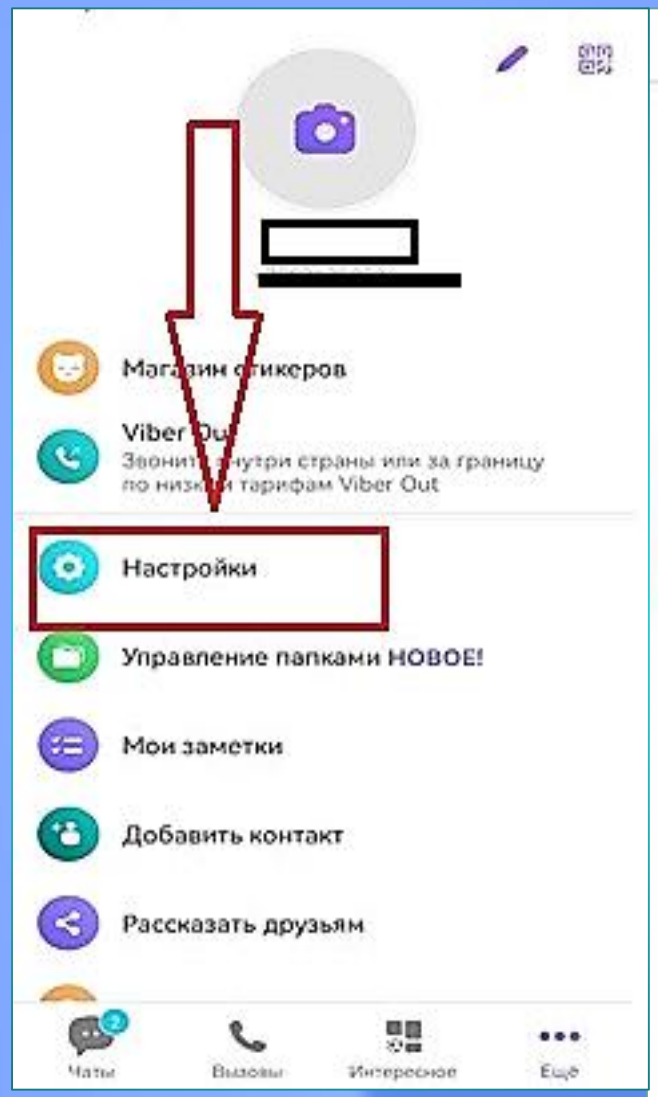
МОШЕННИК НЕ СМОЖЕТ ДО ВАС ДОЗВОНИТЬСЯ В МЕССЕНДЕРАЖ, ЕСЛИ ВЫ УСТАНОВИТЕ ЗАЩИТУ ОТ НЕИЗВЕСТНЫХ ЗВОНКОВ

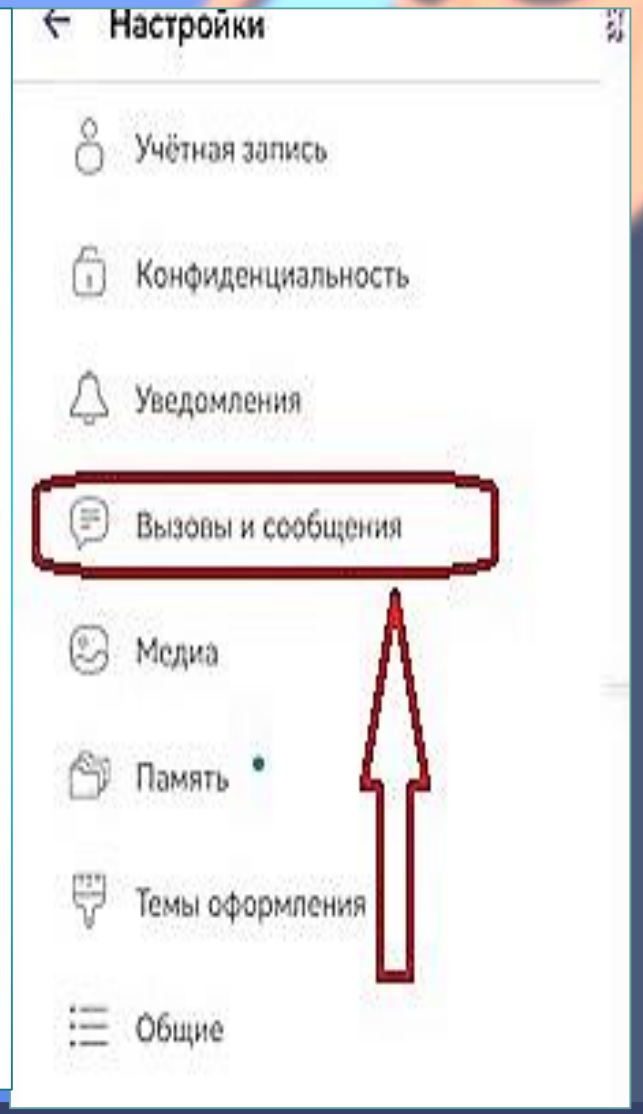
В полицию обратился 65-летний житель г. Улан-Удэ которому позвонили через мессенджер «Viber» и представились сотрудниками ФСБ, пояснили, о необходимости перевода всех его сбережений на «БЕЗОПАСНЫЙ СЧЕТ». Общий ущерб составил 3 млн. рублей.

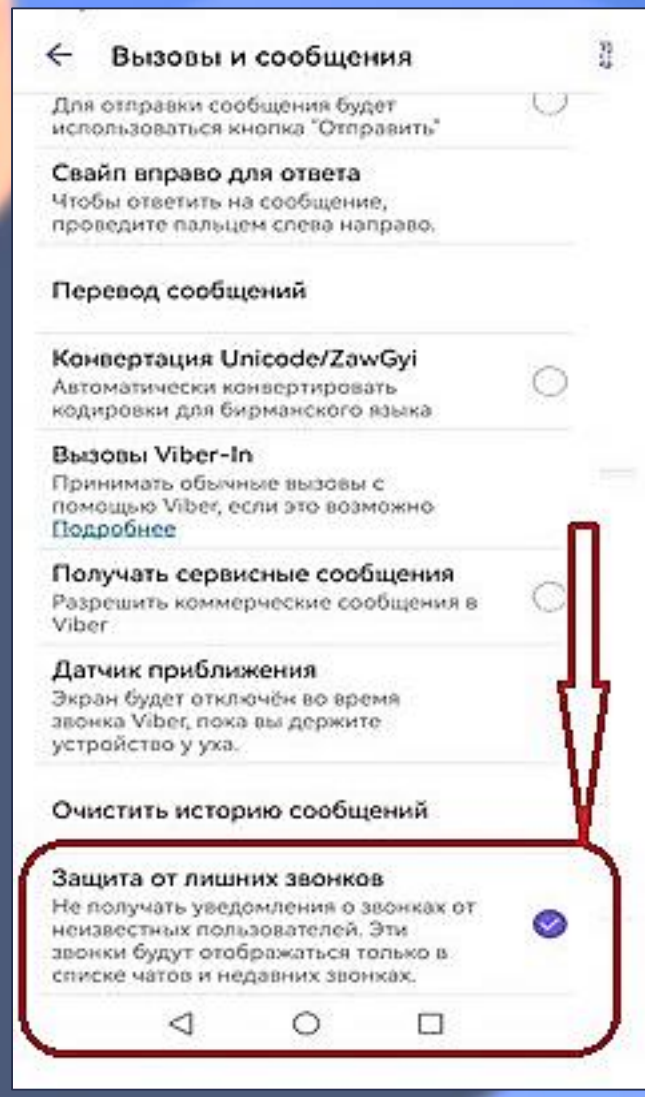
ЖЕРТВА

Защита от звонков в *Viber*

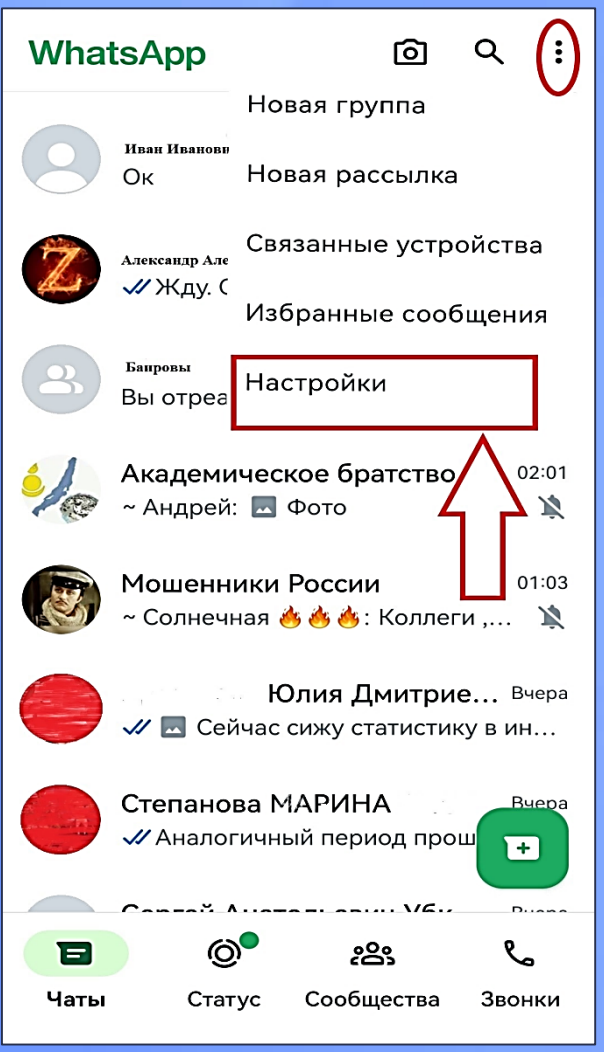


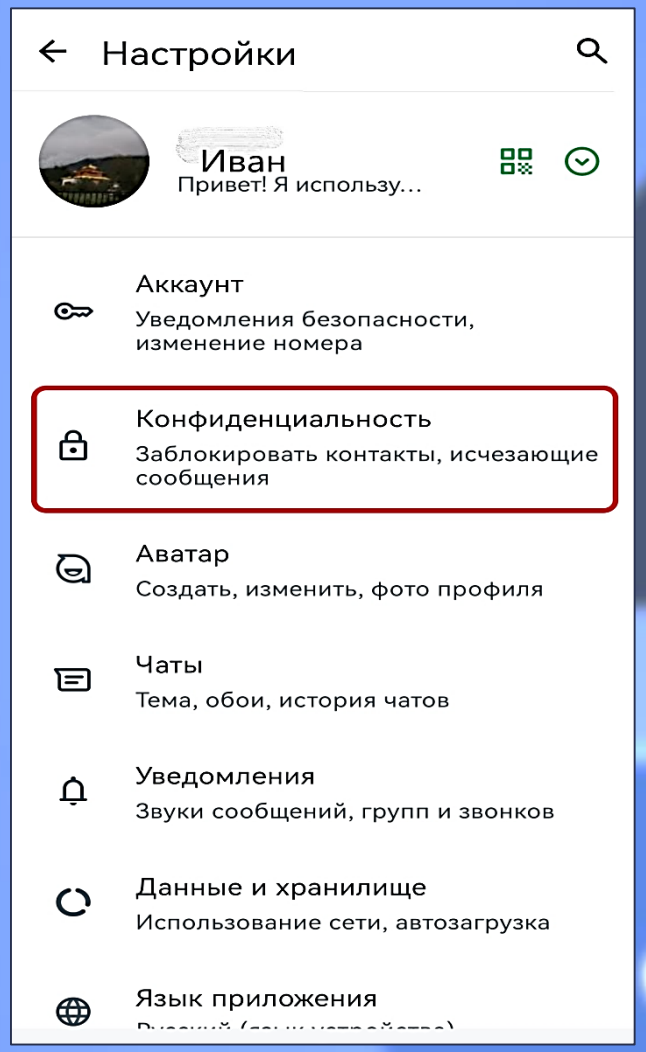


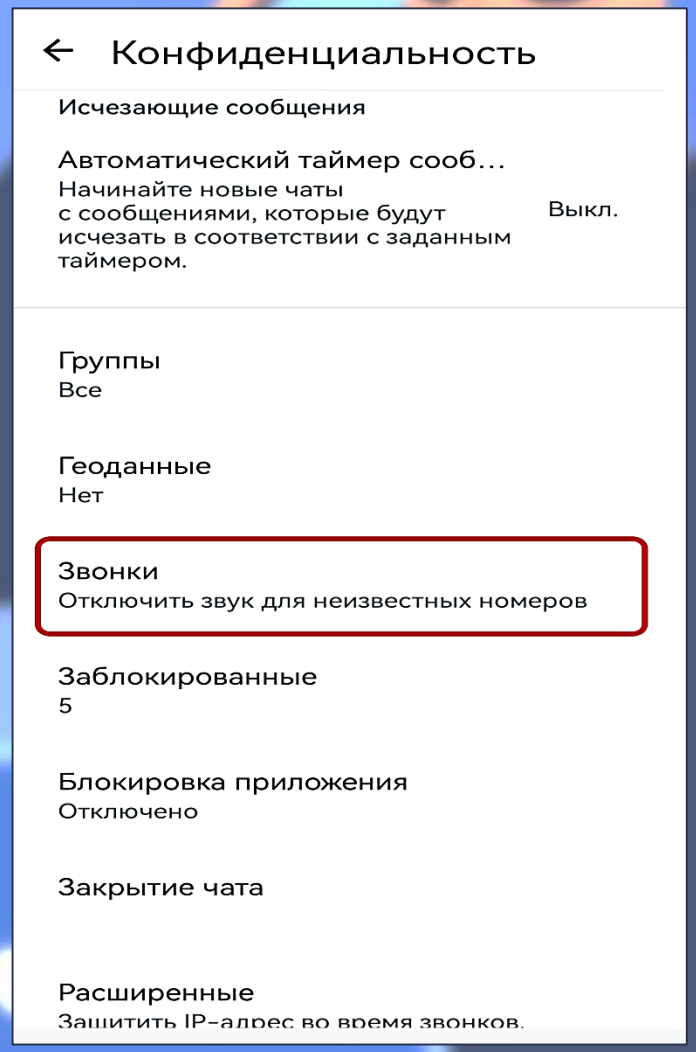


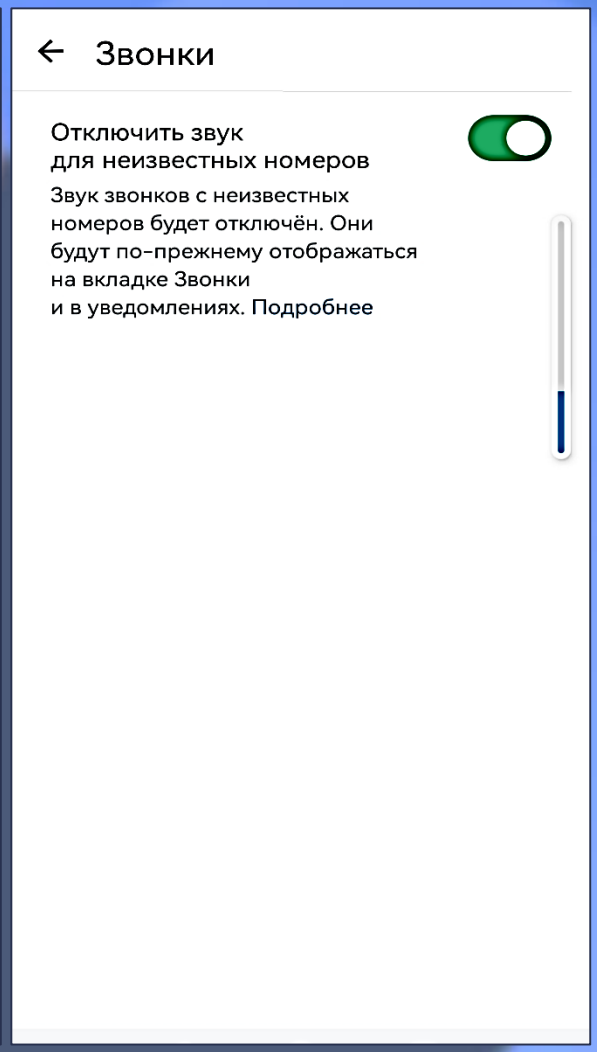


Защита от звонков в *WhatsApp*

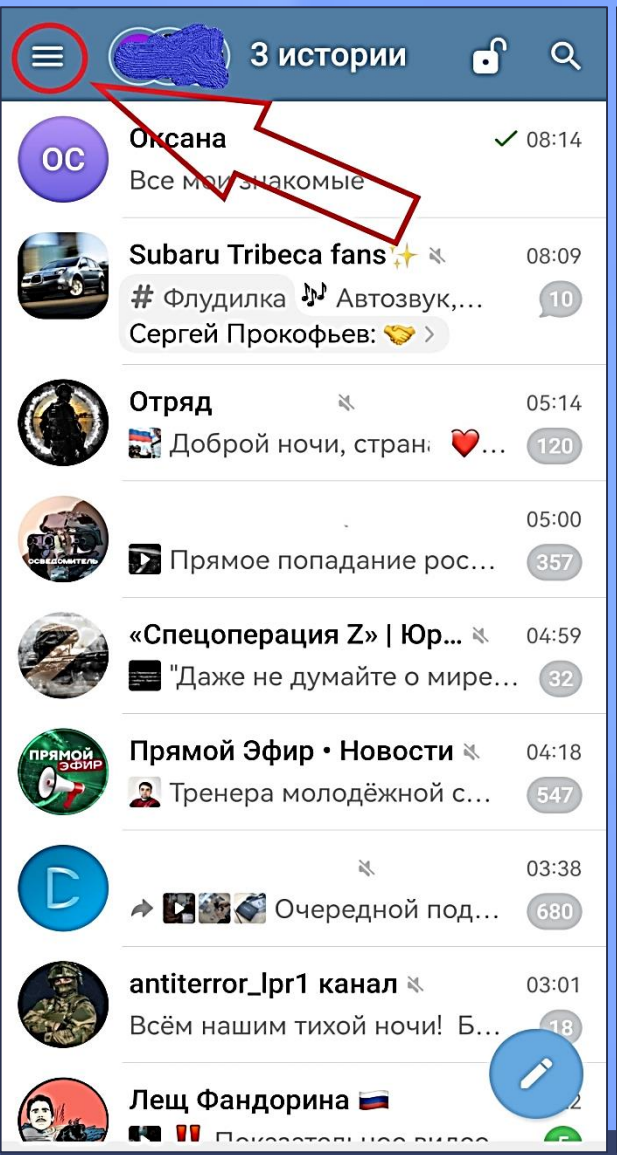


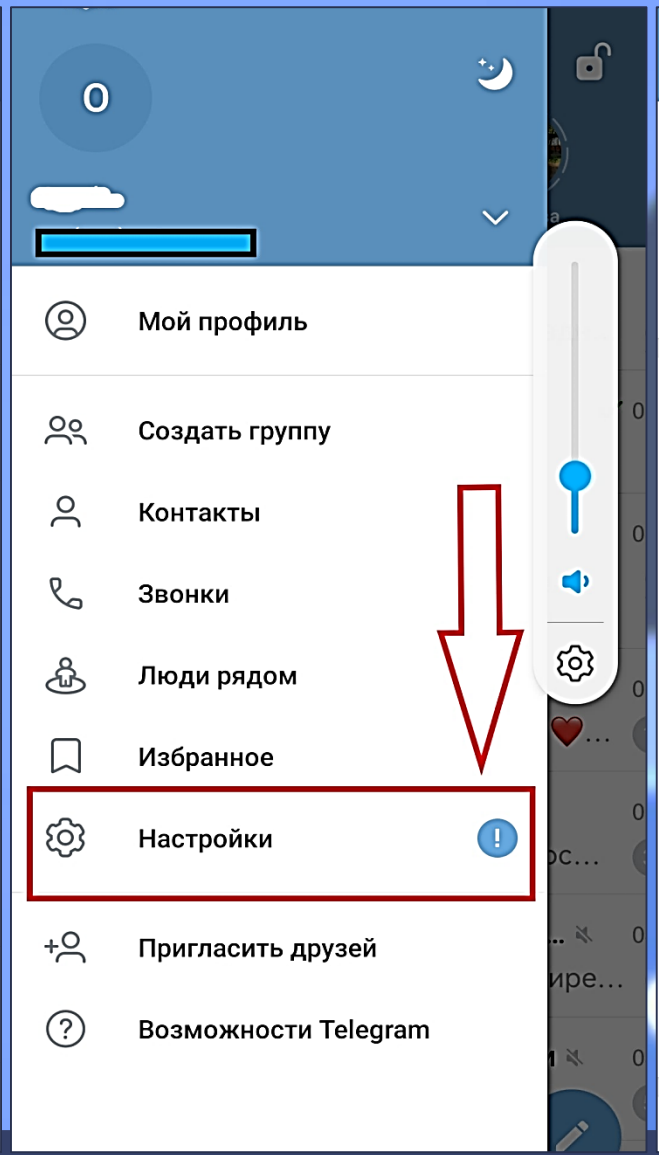


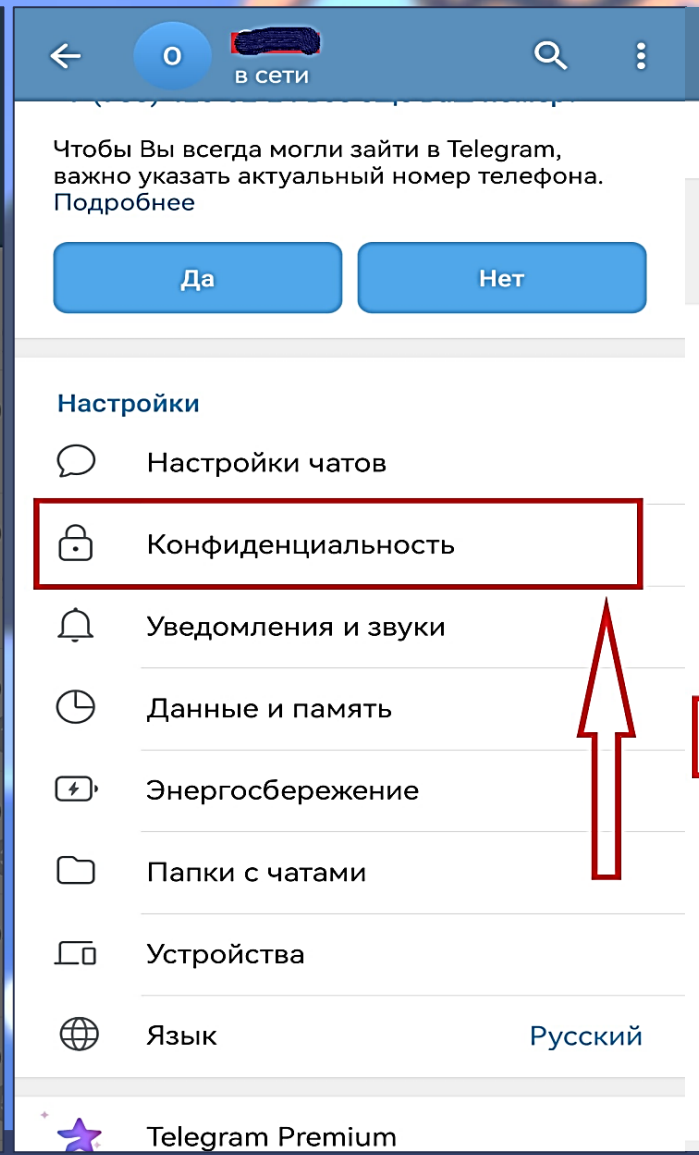


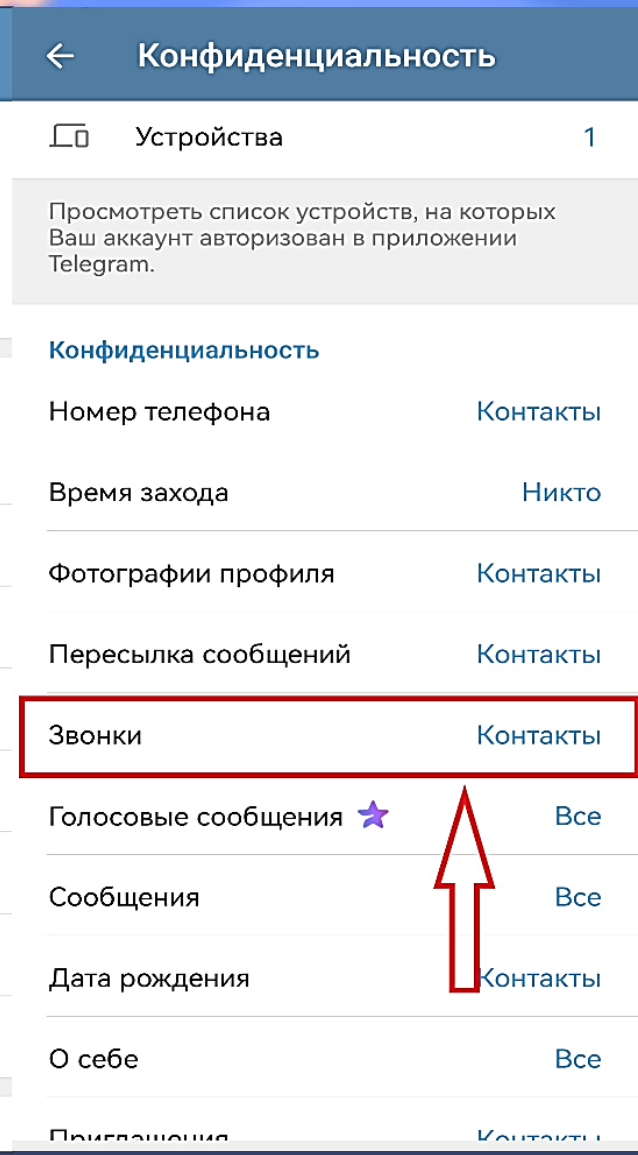


Защита от звонков в *Telegram*

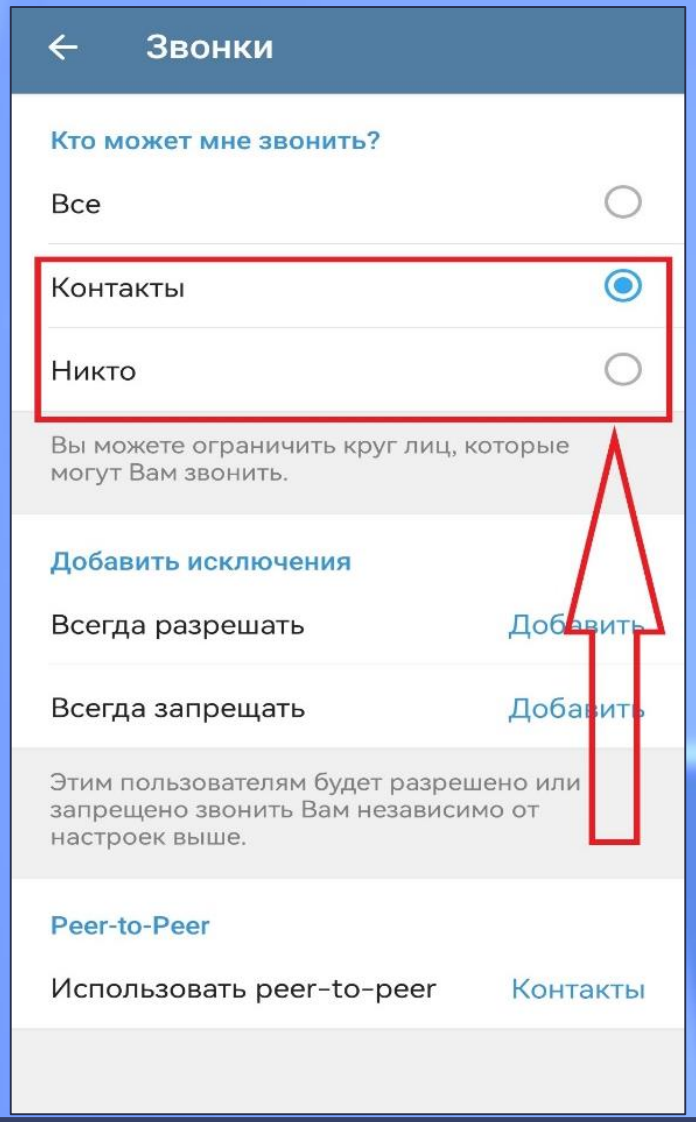


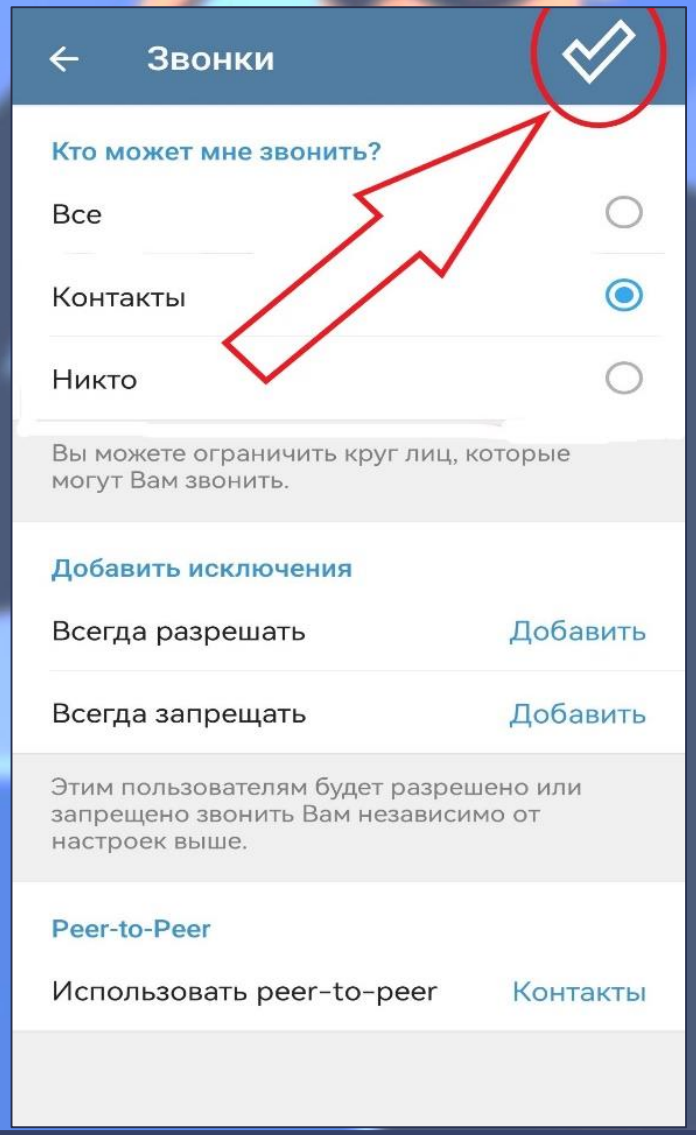






Защита от звонков в *Telegram*





ОСНОВНЫЕ ПРАВИЛА 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!

ИНФОРМАЦИЯ ДЛЯ СТУДЕНТОВ!
ЧЕМ ОПАСЕН ЗАРАБОТОК В СЕТИ ИНТЕРНЕТ?

ДРОППЕР (или дропп) – человек, которого мошенники используют для вывода и обналичивания похищенных денег.

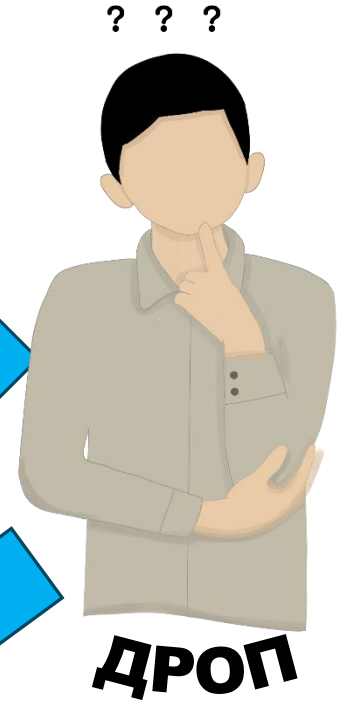
Размещает объявления

- Telegram каналы;
- Форумы;
- Спец. площадки;
- Личный контакт;

Условия работы:

- Короткие сроки;
- % вознаграждения;
- Инструкция по безопасности.

Соглашается



Принимает переводы денежных средств на свои счета;
Обналичивает или переводит деньги за вычетом %

КАКОЕ НАКАЗАНИЕ ДЛЯ ДРОППЕРОВ?

ДРОППЕР

Самое строгое наказание предусмотрено по ст. 159 УК РФ «Мошенничество», эта статья предполагает максимальный срок до 15 лет лишения свободы;
Ст. 187 УК РФ предусмотрена уголовная ответственность за неправомерный оборот средств платежей: максимальное наказание- лишение свободы до 7 лет.

Подписывайтесь на наш
Telegram-канал
МВД по Республике Бурятия

МВД по Республике Бурятия

@MVD_03

ПРИЛОЖЕНИЕ 1

ПРИМЕР:

В декабре 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 оформил кредит на сумму 2 миллиона 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».

ПРИЛОЖЕНИЕ 2

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».

ПРИЛОЖЕНИЕ 3

ПРИМЕР:

В ноябре 2024 года в полицию обратился 50-летний мужчина о том, что в сети интернет он увидел рекламу компании «Газпром Инвестиции» и зарегистрировался на их сайте. Далее на его сотовый телефон позвонил лже-сотрудник «Газпром 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 консультантка 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.

ПРИЛОЖЕНИЕ 4

ПРИМЕР:

В октябре 2024 года в полицию обратилась жительница г. Улан-Удэ, которая сообщила, что на ее сотовый телефон в одном из мессенджеров пришло сообщение от ее знакомойв формате интернет ссылки с текстом «Посмотри, это ты на фото?.apk», далее заявитель нажала на указанный текст, однако в этот момент экран телефона потемнел и перестал реагировать. Через некоторое время женщине удалось включить свой сотовый телефон и она сразу же позвонила той самой знакомой от которой пришло сообщение, однако последняя пояснила, что ее аккаунт в мессенджере был взломан и была рассылка с вирусной ссылкой. Далее при проверке банковских приложений женщина обнаружила. Что с ее банковских счетов были похищены все накопления в размере 400 000 рублей, а так же оформлен кредит на сумму 150 000 рублей.

Таким образом, общий причинённый материальный ущерб составил 550 000 рублей.

ПРИЛОЖЕНИЕ 5

ПРИМЕР:

В ноябре 2024 года в полицию обратился 45-летний мужчина о том, что на его сотовый телефон в мессенеджере «Ватсап» позвонил якобы сотрудник банка который пояснил, что на его имя мошенники пытаются оформить кредит и перевести денежные средства на Украину. Далее для предотвращения данных мошеннических действий необходимо было пройти проверку по биометрии и для этого необходимо включить ДЕМОНСТРАЦИЮ ЭКРАНА. Однако после проведения данной операции на телефон заявителя стали приходить смс-сообщения с кодами доступа к его банковским приложениям и личному кабинету Госуслуг. В этот момент заявитель понял что разговаривает с мошенниками и прекратил разговор. Однако уже потерял доступ к банковским приложениям и личному кабинету Госуслуг. После восстановления доступа, обнаружил что на его имя уже было оформлено несколько кредитов на общую сумму 350 000 рублей а так же похищены личные сбережения в сумме 150 000 рублей.

ПРИЛОЖЕНИЕ 6

ПРИМЕР:

В декабре 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.