Управление МВД России по г. Улан-Удэ

ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

СТАТИСТИЧЕСКИЕ ДАННЫЕ

за 2023 год

- **По Республике зарегистрировано:**
- 2684 мошенничеств (рост на 66,7%)
- 1481 краж с банковских счетов (рост на 8,9%)
- 425 взломов аккаунтов и страниц (рост на 320,8%)
- **По г. Улан-Удэ зарегистрировано:**
- 1805 мошенничеств (рост на 56,4%).
- 978 краж с банковских счетов (рост на 3,5%).
- 288 взломов аккаунтов и страниц (рост на 678,4%)

За 3 месяца 2024 года

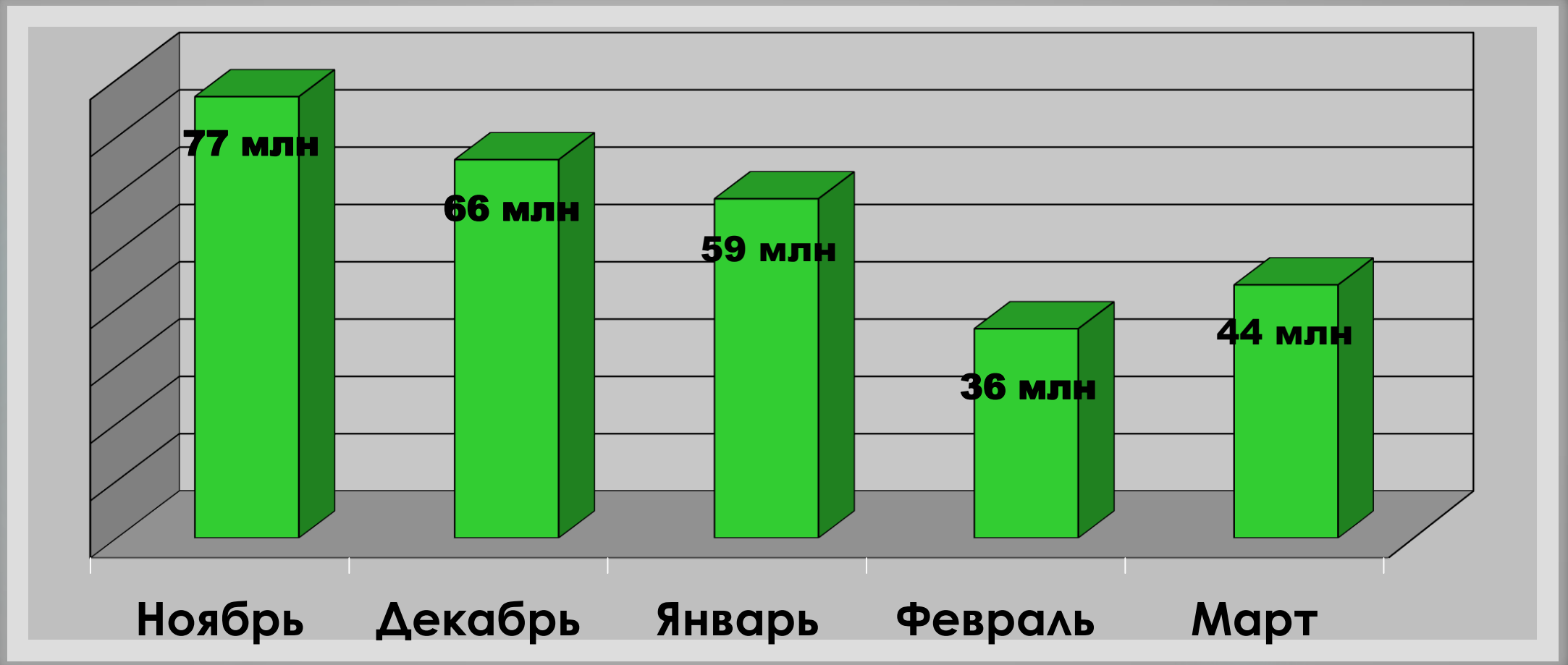
- **По Республике зарегистрировано:**
- 578 мошенничеств (рост на 10,1%)
- 287 краж с банковских счетов (снижение на 15,6%)
- 249 взломов аккаунтов и страниц (рост на 632,4%)
- **По г. Улан-Удэ зарегистрировано:**
- 363 мошенничеств (снижение на 2,9%).
- 177 краж с банковских счетов (снижение на 21,0%).
- 137 взломов аккаунтов и страниц (рост на 356,7%)

УЩЕРБ

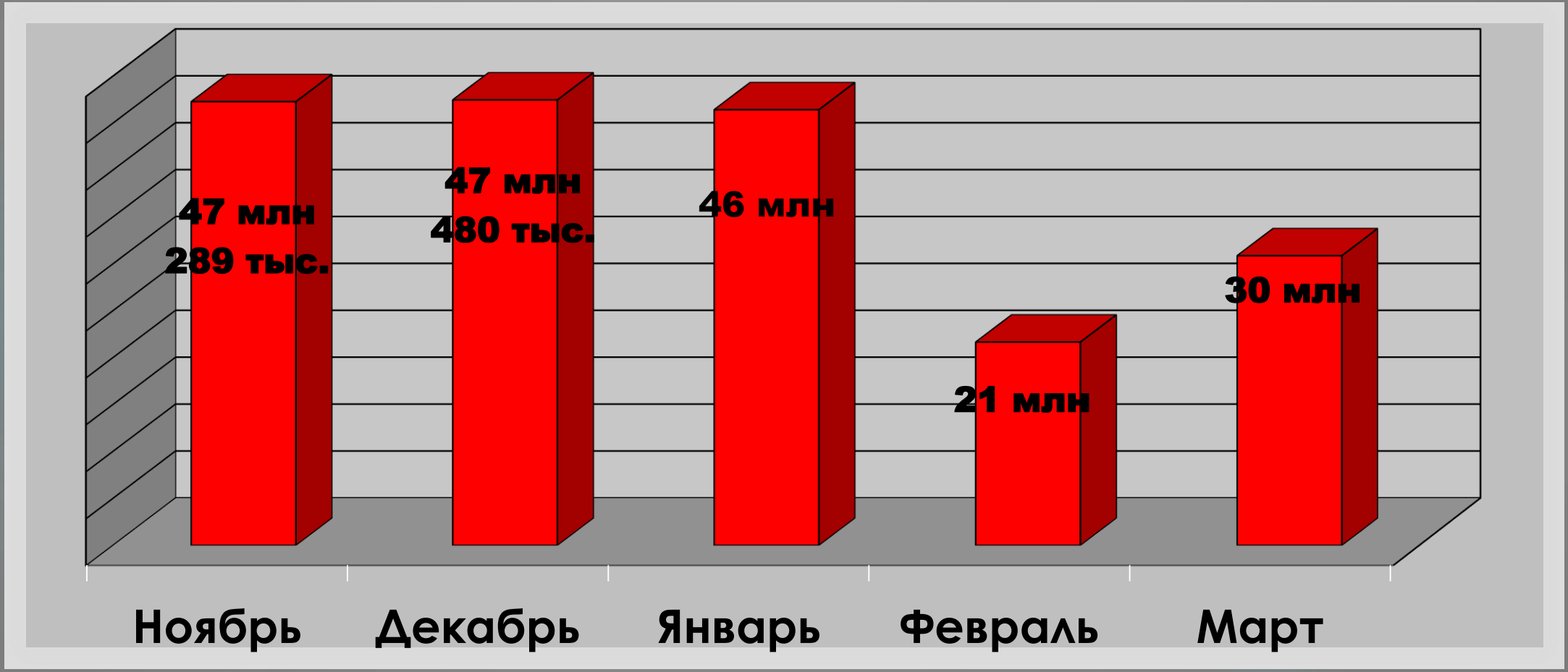
За 2023 год
По России 156 млрд.,
по Республике 664 млн.,
По г. Улан-Удэ 460 млн.

За 3 месяца 2024 года
по Республике 135 млн,
по г. Улан-Удэ 90 млн.

Динамика причиненного ущерба в период с ноября 2023 года по март 2024 года по Республике Бурятия



Динамика причиненного ущерба в период с ноября 2023 года по март 2024 года по г. Улан-Удэ



Геолокация мошеннических КЦ

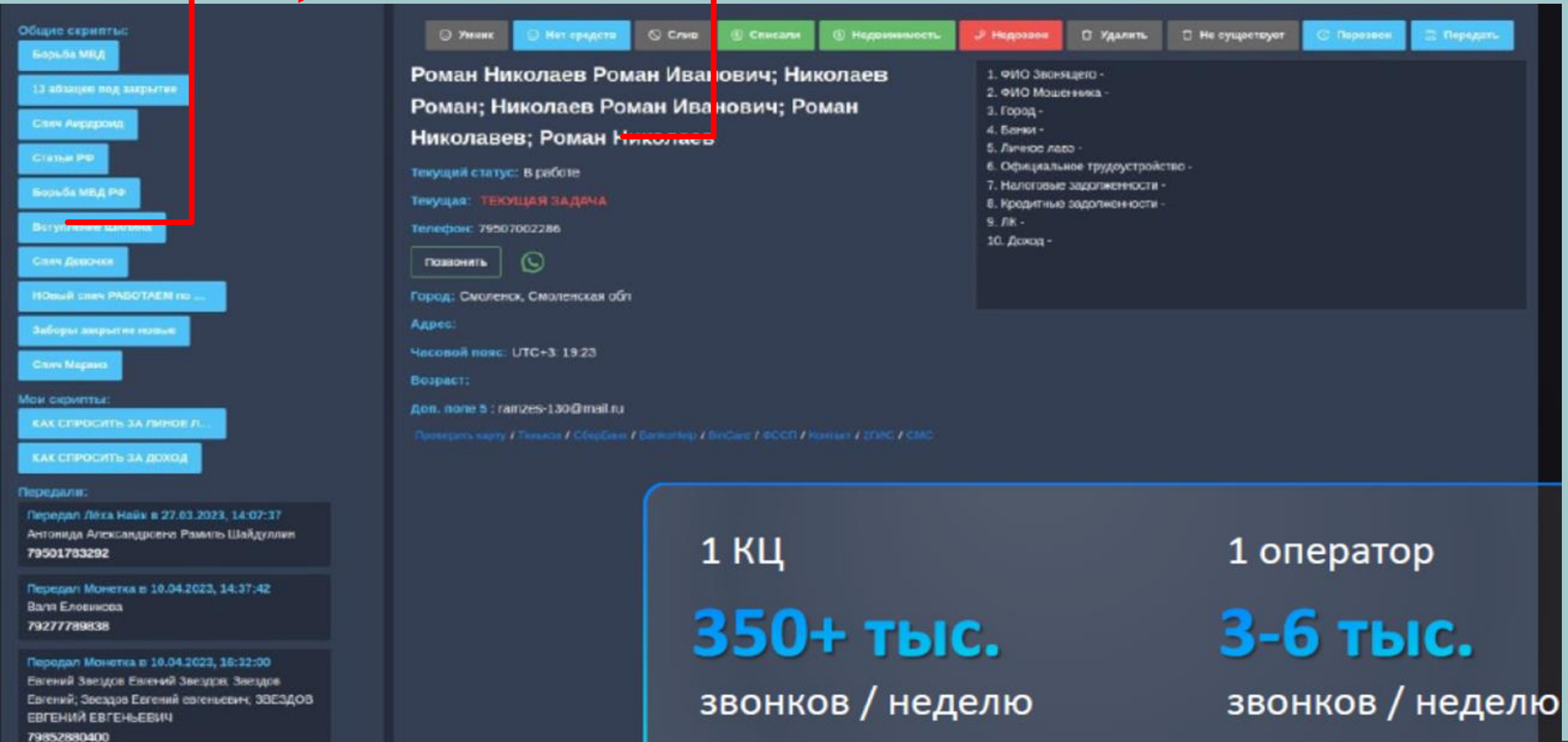
Установлено местоположение:

- Администратор управляющего CRM – г. Запорожье;
- 3 CRM – г. Запорожье;
- 5 CRM – г. Днепр, проспект Дмитрия Яворницкого;
- 3 CRM – г. Одесса, Люстдорфская дорога;
- 3 CRM – г. Одесса, Высокий переулок;
- 2 CRM – г. Киев;
- 1 CRM – г. Чернигов;
- 1 CRM – г. Черновцы;
- 1 CRM – г. Луцк;
- 1 CRM – г. Львов;

Рабочее место мошенника КОЛЛ-ЦЕНТРА

Способы обмана

Информация о жертве



Спич мошенника

Пример: ЗВОНОК СОТРУДНИКА ПОЛИЦИИ!

Здравствуйте (имя клиента) ожидаем ответ
С вами связывается ГУ МВД по г. Москве лейтенант юстиции Кириллов Сергей Игоревич, приятно познакомиться
Связались с вами по оперативной необходимости, примите во внимание что наш диалог ведется под запись, после чего он будет предан в Единый реестр до судебных расследований.
Мы получили материалы возбужденного уголовного дела по статье 327 УК РФ это подделка официального документа предоставляющего право собственности.
Скажите, кем вам приходится некий Буйнов Сергей Петрович 1997 года рождения?
А вы сейчас территориально в Москве находитесь? (ЕСЛИ КЛИЕНТ ОТВЕЧАЕТ «НЕТ», И НАЗЫВАЕТ ГОРОД, ТЕМ САМЫМ ВЫ ПОНИМАЕТЕ ЧТО ОН ВКИНУЛСЯ НА ВАШЕ ПРИВЕТСТВИЕ И ПОКА ВЕРИТ ВАМ)…

В рабочем месте мошенника в быстром доступе имеется функция:

Онлайн редактор документов

СБЕРБАНК

ул. Вавилова, д. 19, Москва, 117997
19 Vavilova St., Moscow, 117997
900 +7 495 500-55-50
www.sberbank.ru

Сформировано в Сбербанк Онлайн года

Справка по операции

ПАО «Сбербанк» сообщает, что указанная ниже операция списания была совершена по карте , держателем которой является ЕЛЕНА .

Операция совершена	Статус операции
сентября в 23:02	Исполнена

Управляющий директор Дивизиона «Забота о клиентах»

Публичное акционерное общество «Сбербанк России» Центр заботы о клиентах ПАО Сбербанк Межрегиональный Центр заботы о клиентах СБЕРБАНК г. Москва

В редакторе документов возможно создать скан-копию любого официального документа, от офиального банковского уведомления до документов удостоверяющих личность

Базы данных для обзвона

Способы утечки/пополнения баз данных для обзвона:

1. Взлом популярных сайтов (грузоперевозок, сетевых магазинов по продаже одежды, организаций оказывающих платные медицинские услуги, интернет магазины по продаже цифровой и бытовой техники). **20 млн. данных**

2. Предоставление баз данных недобросовестными работниками организаций. **40 млн. данных**

3. Не соблюдение гражданами "Цифровой гигиены" в сети интернет. (Указывают персональные данные на специально созданных мошенниками сайтах. Например: при регистрации на сайте для просмотра кинофильмов) **70 млн. данных**

Наиболее часто встречающиеся виды мошенничеств:

Первый способ.

Обман в ходе телефонного разговора

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ

ПРОСТОЙ ЗВОНОК

ЛЖЕСОТРУДНИК БАНКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

"Замечена подозрительная активность"

"Кто-то пытается оформить на вас кредит"

"Вы переводите деньги террористам..."

"В отношении Вас возбуждено уголовное дело"

ПРОСТОЙ ЗВОНОК

ЗВОНОК БЛИЗКОГО РОДСТВЕННИКА (ДОЧЬ, СЫН, БРАТ, СЕСТРА, ПЛЕМЯННИК)

"Я совершил ДТП срочно нужны деньги"

"Произошла беда! Переведи мне деньги"

МОШЕННИЧЕСКАЯ КОМБИНАЦИЯ

Создается ФЕЙКОВЫЙ или взламывается аккаунт РУКОВОДИТЕЛЯ.
От имени которого направляется сообщение подчиненному о том, что ФСБ проводит проверку
Руководитель предупреждает, что поступит звонок от ФСБ.

ДАЛЕЕ

Подчиненному поступает звонок от лже-сотрудника ФСБ который:
- угрожает уголовной ответственность за пособничество врагу;
- сообщает что в "мошенник" имеет генеральную доверенность по которой может оформить кредиты.

ДАЛЕЕ

Подключается банковский работник, сотрудник Росфинмониторига и др. Который в целях безопасности, дает указание идти оформлять кредиты в банках, что бы опередить дейтсвия "мошенников". Далее рекомендует кредитные средства перевести на "безопасный счет".

ПРИ ЭТОМ МОШЕННИКИ МОГУТ ПОДДЕЛЫВАТЬ ГОЛОСА ИСПОЛЬЗУЯ ВОЗМОЖНОСТИ НЕЙРОСЕТЕЙ

Пример: в марте 2024 года поступило заявление от директора одной из школ Улан-Удэ, что в Телеграмм пришло сообщение от председателя комитета по образования о том, что в отношении директора школы проводится проверка со стороны ФСБ. Далее директору сотрудник ФСБ сообщил, что «мошенники» завладели данными и хотят оформит кредиты. Под предлогом предотвращения действий мошенников она взяла кредиты в различных банках на общую сумму 2 700 000 рублей и перевела их на якобы «СПЕЦИАЛЬНЫЙ БЕЗОПАСНЫЙ СЧЕТ».

Общий ущерб 2 700 000рублей.

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ОТРИЦАТЕЛЬНЫЕ

- СТРАХ ПАНИКА
- ЧУВСТВО СТЫДА

«Вы выиграли крупную сумму денег»

«Вам положены социальные выплаты»

«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере…»

«С вашего счета списали все деньги»

«Ваш родственник попал в аварию и сбил человека»

«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела»

Увы, мы готовы сделать ВСЁ, что просят от нас мошенники

УБК МВД России

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!

Второй способ.
МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ ЗАРАБОТКА В СЕТИ ИНТЕРНЕТ ИЛИ ТРУДОУСТРОЙСТВА

- **Можно выделить два варианта обмана:**
- **- при поиске работы через интернет;**
- **- при поиске пассивного заработка (инвестирование, биржи, трейдинг);**

ПОСЛЕ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЯ О ПОИСКЕ РАБОТЫ:
- поступает звонок менеджера;
- проводит опрос, оговаривает условия работы.

ДАЛЕЕ МОШЕННИКИ ПРЕДЛАГАЮТ:
1) пройти платные курсы;
2) зарегистрироваться на сайте, с подтверждением личности посредством ввода СМС-кода;
3) зарегистрировать банковскую карту для получения заработной платы, подтверждая кодом из СМС.

НА САМОМ ДЕЛЕ СМС-КОД ДЛЯ ВХОДА В ПРИЛОЖЕНИЕ БАНКА ИЛИ ГОСУСЛУГИ

Заработки под предлогом накрутки рейтинга положительных отзывов, либо при продаже на популярных маркетплейсах «Вайлдбериз» и «Озон»

Мошенники предлагают:

Счала ставить «Лайки», а затем «закупить» товар для реализации.

Перейти по ссылке на сайт маркетплеса, однако при переходе вы попадаете на сайт двойник, на котором при регистрации предоставляете всю информацию о себе, а так же коды из СМС

Денежные средства уходят мошенникам

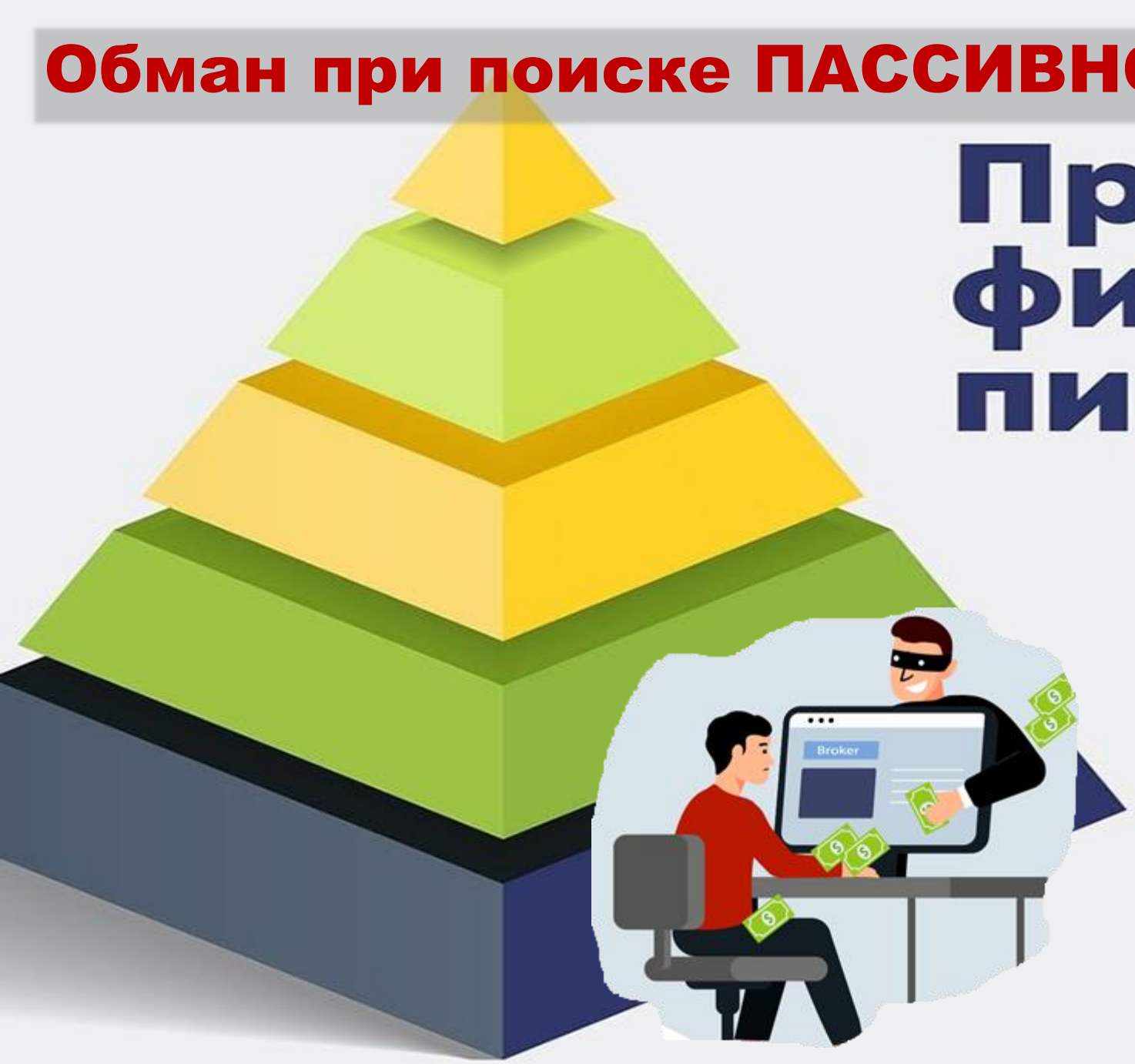
Пример

- **В апреле 2024 года в полицию обратилась девушка с заявлением о том, что в мессенджере «Телеграмм» ей пришло сообщение с предложением заработка на маркетплейсе «Вайлдберис», суть работы заключалась в повышении рейтинга продавцов, то есть ставить лайки на товарах. Девушка согласилась на предложение и выполняла задания вечером после основной работы. За работу девушка действительно получала заработную плату в размере 300 и 500 рублей на свою банковскую карту.**
- **Войдя в доверие, «работодатель» предложили более крупный заработок, а именно выкупить товар для получения дохода в размере 30% от продаж, на что девушка согласилась и якобы выкупила товар на сумму 480 000 рублей.**
- **В последующем работодатель перестал выходить на связь.**

Как себя обезопасить

- Поиск информации о компании в открытых источниках. Если не имеется никаких сведений — это повод насторожиться.
- Не совершайте платежи/переводы в адрес потенциального работодателя (даже если вам объясняют их необходимость для будущей работы — например, плата за вводное обучение, рабочую форму или рабочие инструменты).
- Не сообщайте/не указывайте коды из поступивших смс-сообщений;
- Не выполняйте действия в «Банковских приложениях» по чьей либо просьбе/указанию (Например для открытия «Рабочего счета» и др.)

Обман при поиске ПАССИВНОГО ЗАРАБОТКА



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

Пример:

Гр. А оформил дебетовую и кредитную банковские карты АО «Тинькофф банк» и подключил услугу «Инвестиции». Далее на его сотовый телефон позвонил мужчина, который представился сотрудником банка АО «Тинькофф банк» и предложил заработать на инвестициях, установив приложение «BYBIT» для обмена денежных средств на криптовалюту и приложение «ТЕРМИНАЛ» для пополнения счета. После установки приложений заявитель перевел денежные средства в размере 10 000 рублей на счет приложения «ТЕРМИНАЛ», где через несколько дней увидел, что сумма увеличилась на 1 800 рублей.

Далее ему предложили получить еще больше прибыли, заявитель внес денежные средства в размере 180 тысяч, 600 тысяч и 500 тысяч рублей. Затем пришло уведомление о том, что приложение «ТЕРМИНАЛ» заблокировано, для разблокировки необходимо внести 1 000 000 рублей.

Гр. А. оформил несколько кредитов в ПАО «Сбербанк», АО «Тинькофф банк» на супругу в размере 1 986 000 рублей и совершал переводы злоумышленникам, полагая, что инвестирует свои денежные средства.

Как себя обезопасить:

- **- проверять брокерскую компанию на сайте Банка России на наличие лицензии. Следует знать, что мошенники могут действовать от имени официальных компаний.**
- **- 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».**

Третий способ.
МОШЕННИЧЕСТВА НА САЙТАХ ОБЪЯВЛЕНИЙ, ИЛИ ИНТЕРНЕТ МАГАЗИНАХ

- **Можно выделить два варианта обмана:**
- **- МОШЕННИК ПРОДАВЕЦ;**
- **- МОШЕННИК ПОКУПАТЕЛЬ;**

Мошенник продавец

Признаки мошенничества

- Отказ от личной встречи
- Отказ от наложенного платежа
- Заниженная стоимость товара
- Требование предоплаты
- Необходимо перейти по ссылке на сайт (двойник) для безопасной сделки
- Настойчивые просьбы быстрее оплатить товар

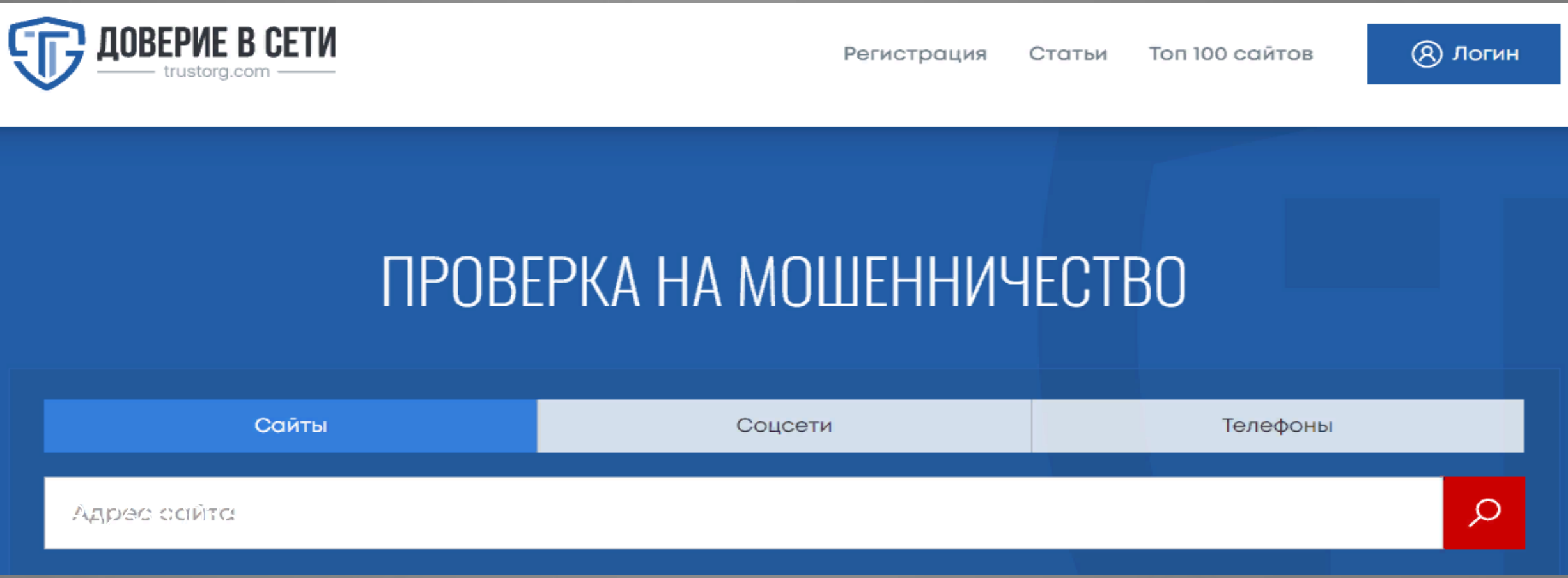
- *Насторожитесь если номерная емкость телефона продавца не соответствует региону его местонахождения

Мошенник продавец

- **ЭТАПЫ ОБМАНА:**
- **1. Продавец-мошенник размещает в сети интернет заманчивое объявление о продаже товара.**
- **2. Жертва откликается на объявление, оговаривают условия купли-продажи.**
- **3. Продавец-мошенник просит внести предоплату или оплатить полную стоимость товара;**
- **4. Жертва совершает оплату/предоплату.**

- ***В ноябре 2023 года в полицию обратился житель г. Улан-Удэ, котрый обнаружил на сайте «ДРОМ» объявление о продаже автомобиля по очень заниженной цене, автомобиль со слов продавца находится в пос. Онохой. Далее созвонившись с продавцом по номеру +79526680036 договорился о предоплате за данный автомобиль и перевел 250 000 рублей.***
- ***Однако когда мужчина приехал по указанному адресу в пос. Онохой, там его ожидал пустой участок, телефон продавца был отключен.***

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



Мошенник покупатель

ЭТАПЫ ОБМАНА:

1. **Мошенник откликается на объявление.**
2. **Предлагает оплату безналом, просит доставку.**
3. **Для расчета с продавцом скидывает ссылку на сайт двойник, якобы для осуществления безопасной сделки;**
4. **При переходе по ссылке сайт запрашивает данные банковской карты (номер карты, защитный CVV-код карты, код из СМС).**
5. **Продавец (жертва) вводит требуемые данные карты.**
6. **Мошенник КРАДЕТ ДЕНЬГИ.**

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.**

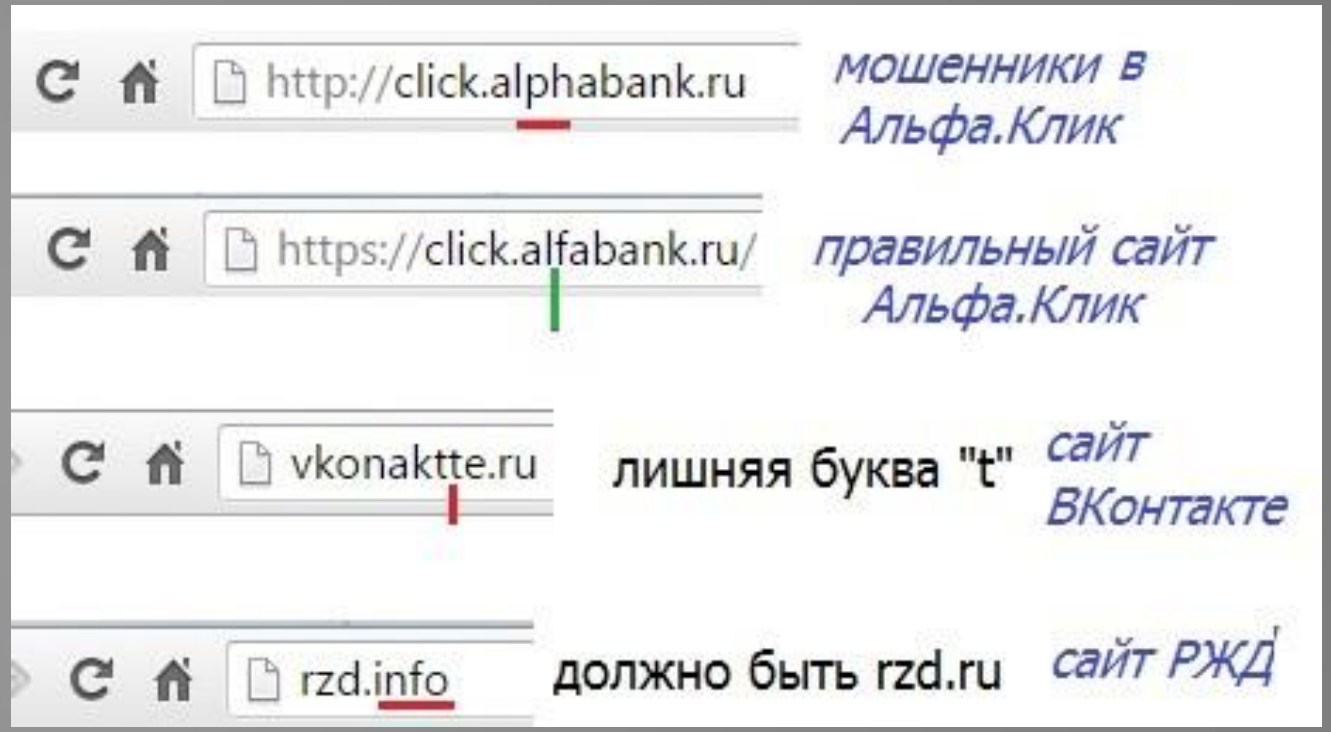
Четвертый способ.
ФИШИНГ

Мошенники создают сайты двойники с целью:

- **Списания денег путем выманивания у жертв банковских сведений для совершения ПЛАТЕЖЕЙ/ПЕРЕВОДОВ;**
- **Взлома аккаунтов социальных сетей, портала Госуслуг и др.;**
- **Заражения устройств жертвы «Вирусом».**

КАК РАСПОЗНГАТЬ САЙТ ДВОЙНИК

- **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**



Пятый способ.
Взлом личного кабинета Госуслуг

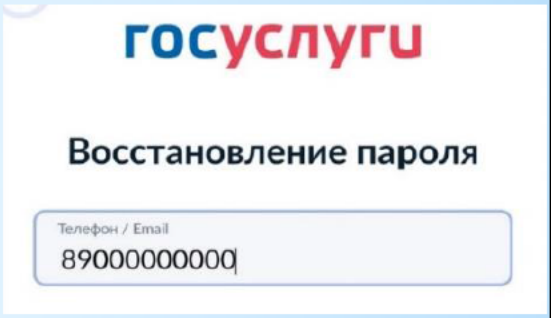
1. Звонок от имени сотового оператора или других служб;
2. Переоформление сим-карты.

1. Звонок от работника сотового оператора

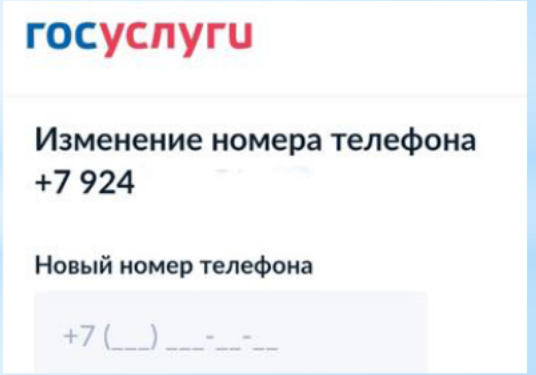
1. Поступает телефонный звонок от оператора сотовой связи, сообщают что необходимо продлить срок действия SIM-карты или обновить паспортные данные.

2. После чего в целях подтверждения личности, также под другим предлогом попросят 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.



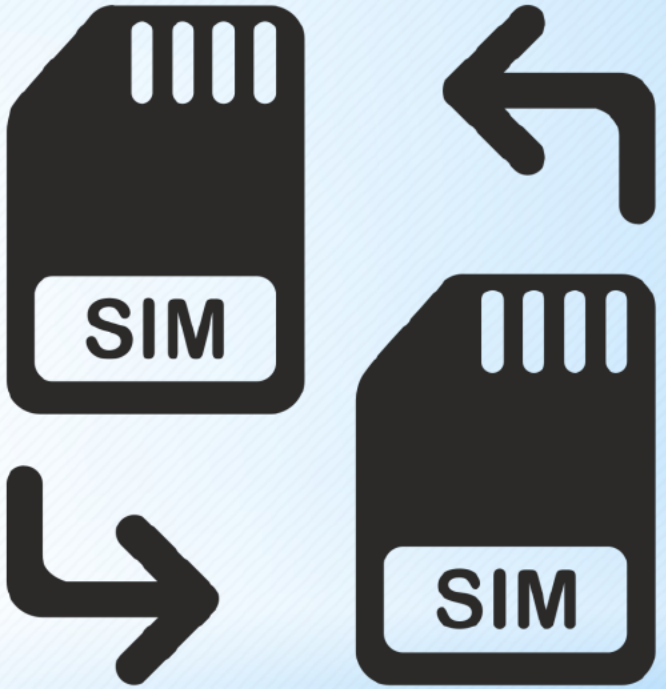
- Для личных кабинетов где установлен вход на портал по SMS-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. На самом деле повторно приходит КОД для изменения номера телефона.



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.



Как себя обезопасить от взлома

1. НИКОМУ НЕ СООБЩАЙТЕ КОД ИЗ СМС-СООБЩЕНИЯ ПОСТУПИВШИЙ С ПОРТАЛА ГОСУСЛУГ.

2. НАСТРОИТЬ ВХОД НА ГОСУСЛУГИ ПО ПАРОЛЮ И КОДУ ИЗ СМС-СООБЩЕНИЯ (ДВУХ ЭТАПНАЯ АУТЕНТИФИКАЦИЯ).

3. В ПРОФИЛЕ ГОСУСЛУГ ОТОЗВАТЬ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ У БАНКОВСКИХ ОРГАНИЗАЦИЙ;

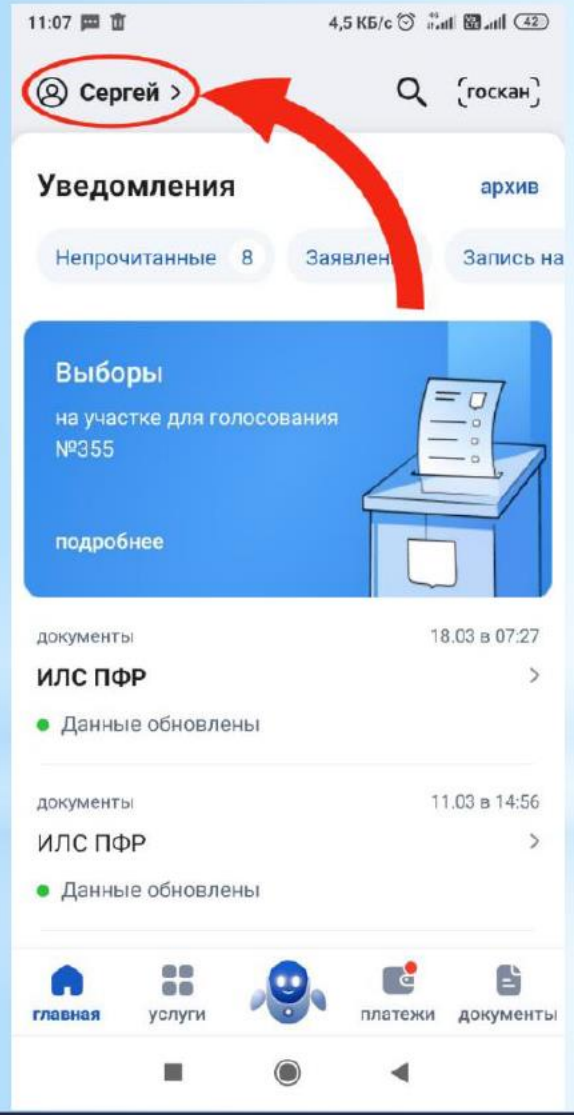
4. НЕ ИСПОЛЬЗУЕМЫЕ АБОНЕНТСКИЕ НОМЕРА ОТКРЕПИТЕ ОТ ПРОФИЛЯ ПОРТАЛА ГОСУСЛУГ.

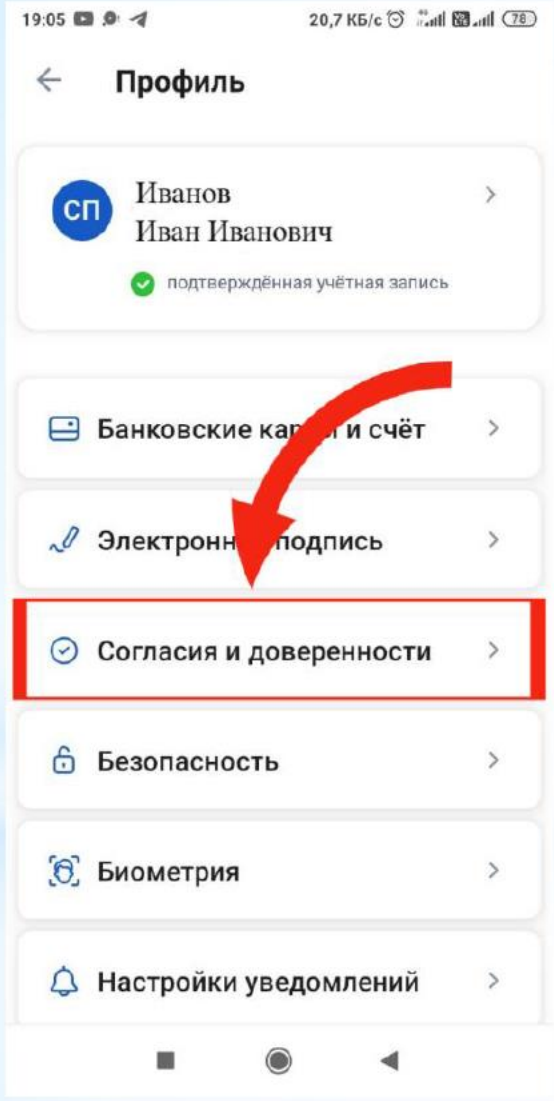
5. РЕГУЛЯРНО, РАЗ В ПОЛГОДА, МЕНЯТЬ ПАРОЛИ ДОСТУПА.

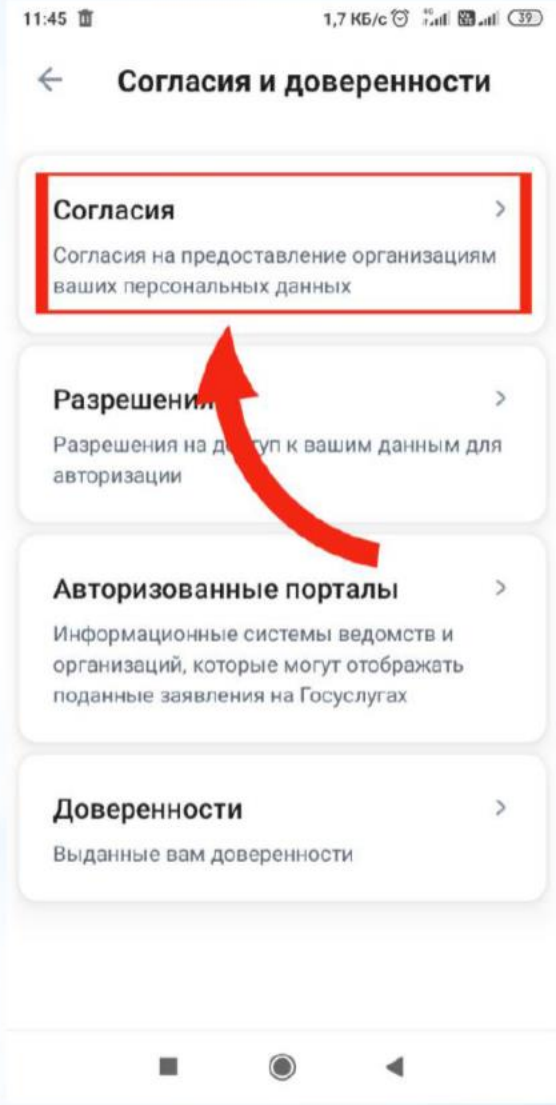
ДОПОЛНИТЕЛЬНО

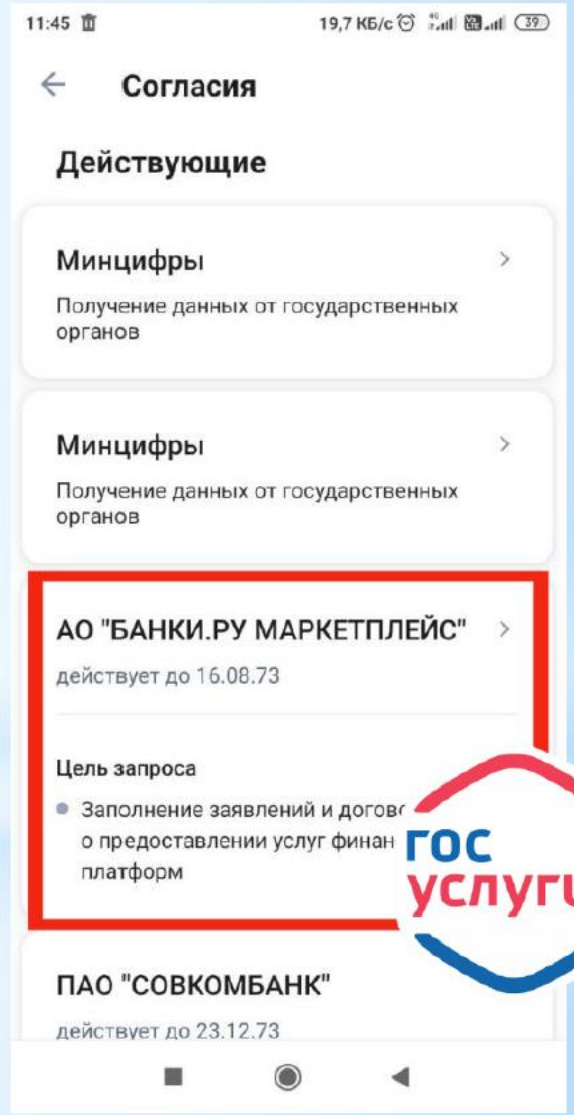
ДЛЯ ЗАЩИТЫ ЛИЧНОГО КАБИНЕТА ПОРТАЛА ГОСУСЛУГ МОЖНО ВКЛЮЧИТЬ ФУНКЦИЮ «ВОСТАНОВЛЕНИЕ ДОСТУПА КОНТРОЛЬНЫМ ВОПРОСОМ».

Отзыв согласий

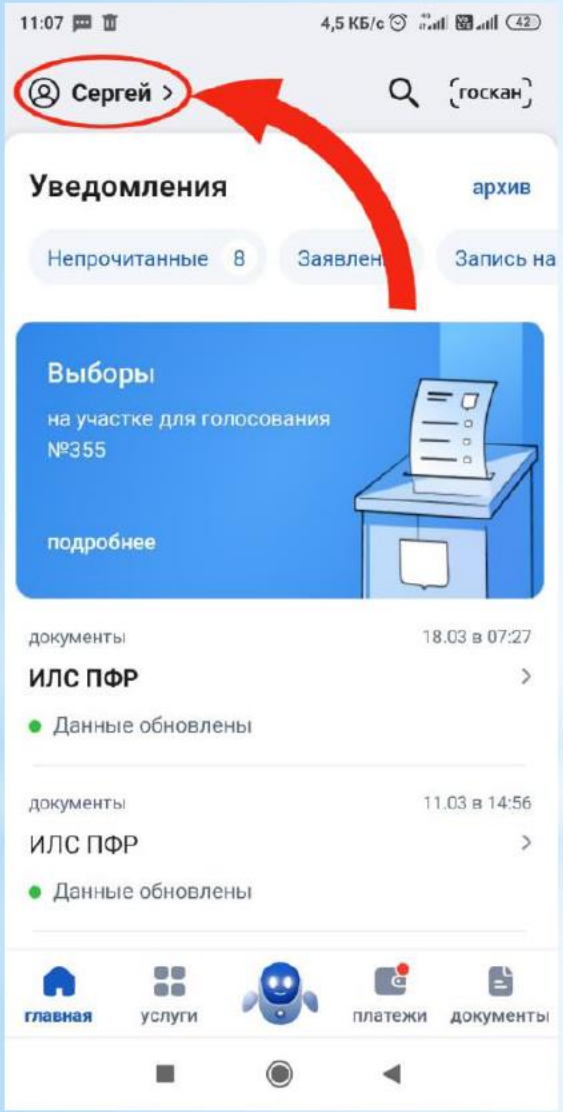


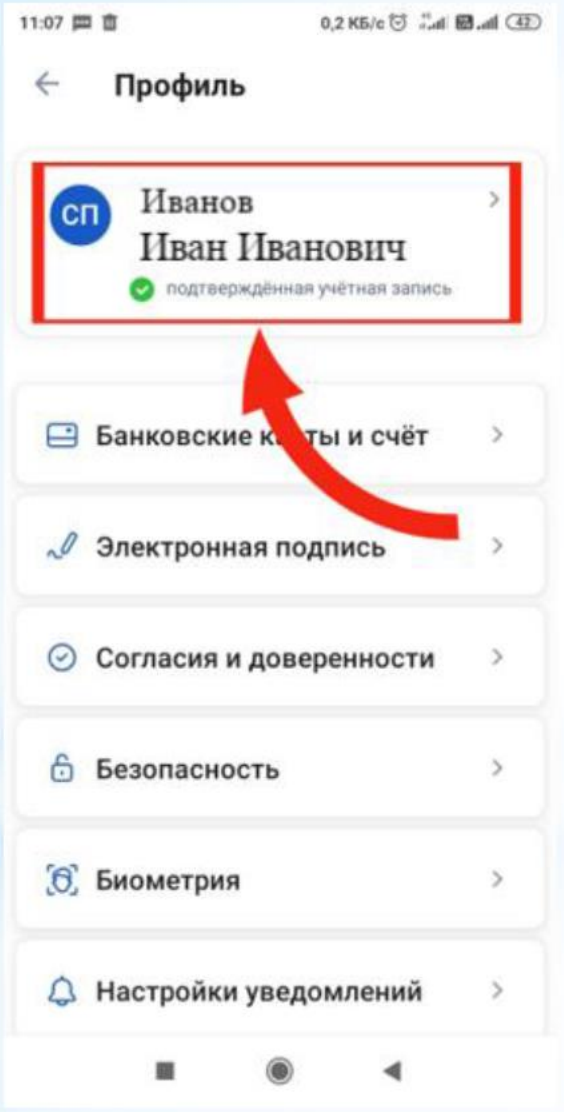


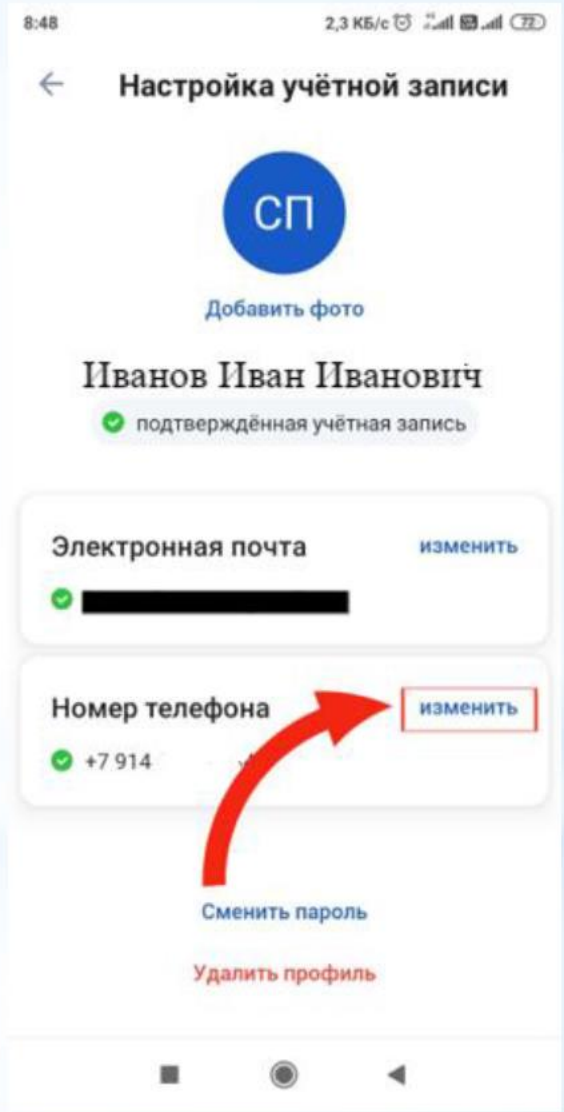


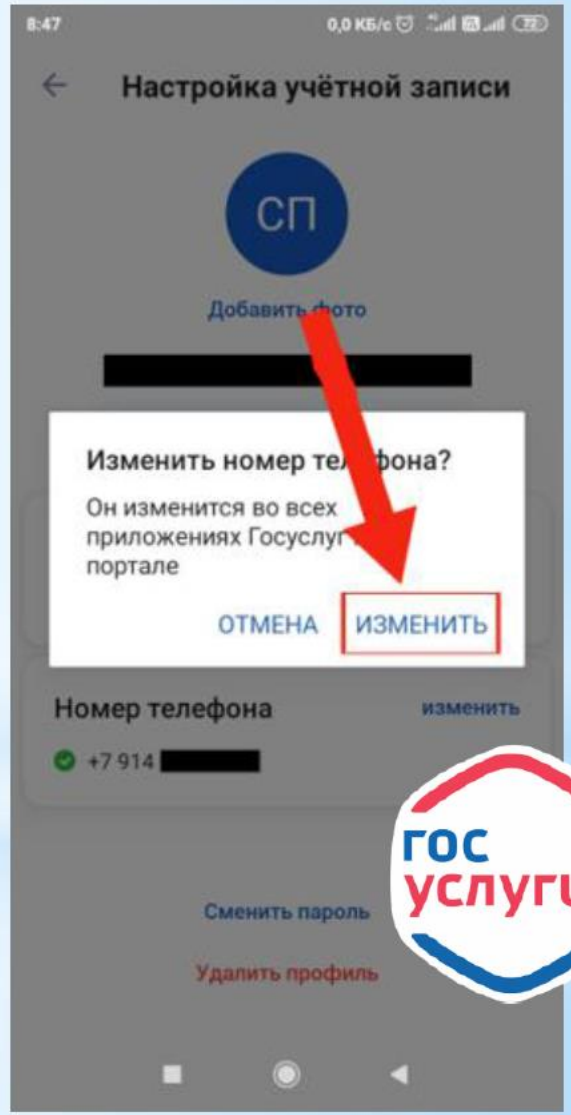


Способ открепления номера телефона

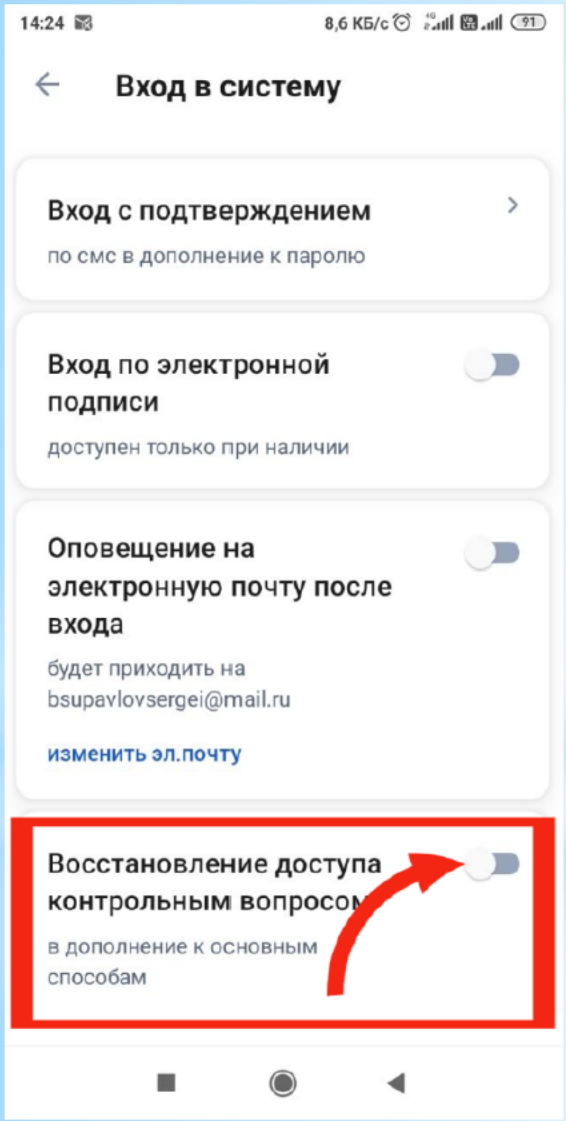


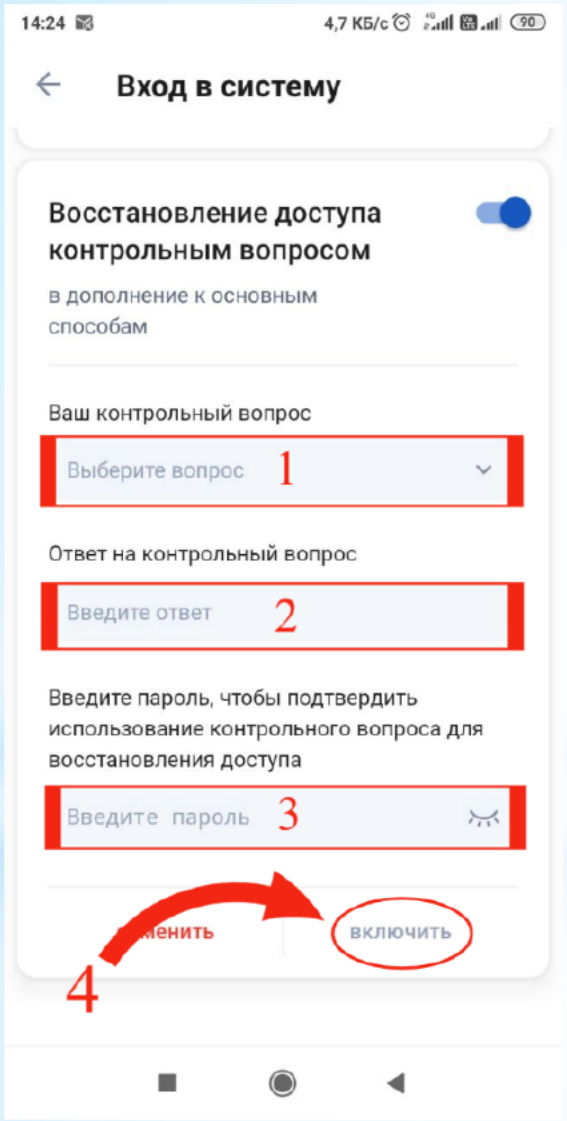






Дополнительная защита личного кабинета





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.

Шестой способ.
Совершение покупок/переводов по утерянным/похищенным банковским картам

РЕКОМЕНДАЦИИ:

- **При обнаружении пропажи банковской карты сообщите в Банк и заблокируйте карту;**
- **Если нашли банковскую карту позвоните или обратитесь в Банк, для блокировки карты;**
- **Не храните банковскую карту в чехлах телефона (с случае утери или кражи телефона, злоумышленники имея номер банковской карты и телефон могут войти банковское приложение).**

ВНИМАНИЕ!
МОШЕННИКИ МОГУТ ИСПОЛЬЗОВАТЬ ДЕТЕЙ ДЛЯ ХИЩЕНИЯ ВАШИХ СРЕДСТВ.

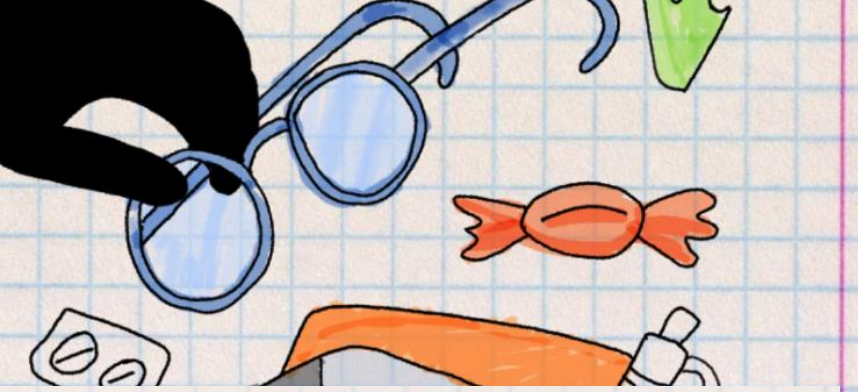
ПРИМЕР:

11.03.2024 в полицию поступило заявление от гр. М. о том, что ее несовершеннолетний сын, 2014 г.р., хотел приобрести ВИРУТАЛЬНОЕ «золото» ДЛЯ игры «Stend Off» и перешел по ссылке в телеграмм-канал «Твой менеджер», где ребенка проинструктировали, что для получения игрового «золота» выполнить следующие действия:

- **ввести данные банковской карты;**
- **выполнить определенные действия в приложении «Сбербанк-Онлайн»;**

Мальчик без спроса взял телефон родителя и выполнил все действия которые ему сказали сделать для получения игрового «золота».

В результате мальчик оформил кредит и перевел 282 120 рублей на неустановленные счета.

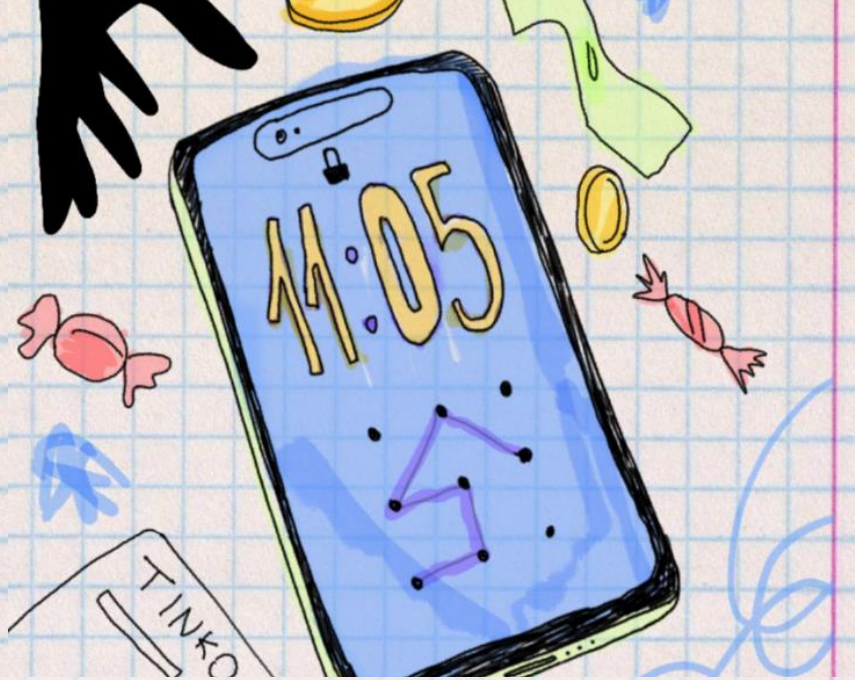


Поговорите с ребенком

Расскажите про мошенников и пообещайте, что поможете выбрать надежного продавца.

Не оставляйте карты без присмотра

В некоторых сервисах и приложениях все еще можно заплатить без подтверждения операции кодом из СМС. А если ребенок догадается, какой у вас ПИН-код, он сможет ненадолго взять карту и снять деньги в банкомате.

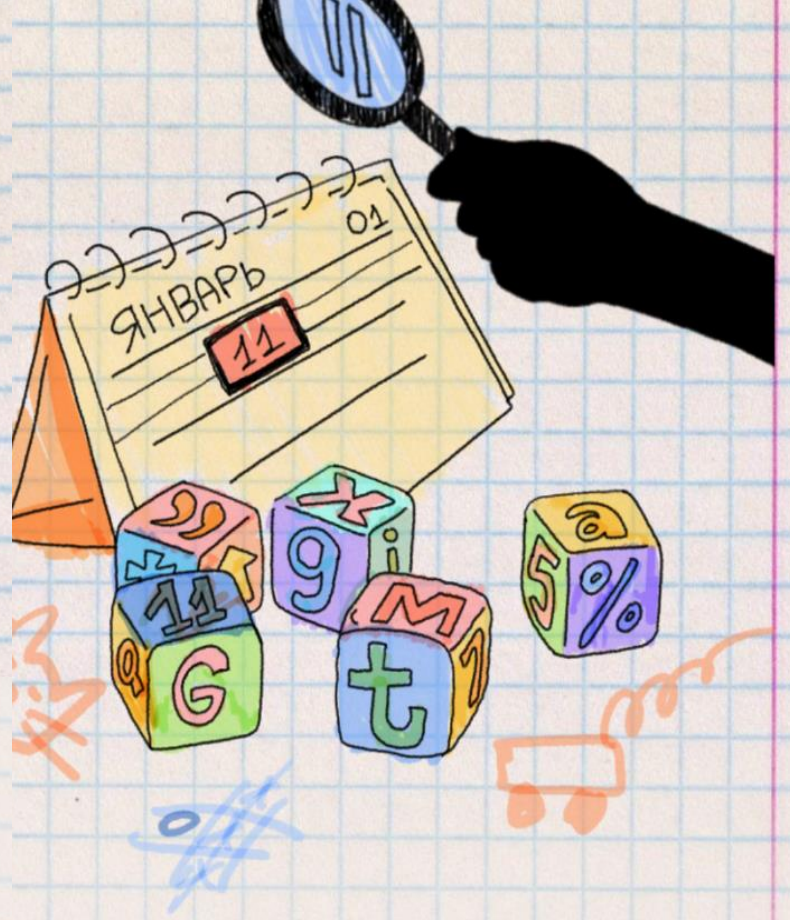


Отключите уведомления при блокировке экрана

Даже если ребенок получит доступ к реквизитам карты, он не сможет подтвердить покупку, когда банк пришлет код.

Поставьте защиту на вход в смартфон

Это ПИН-код, пароль или графический ключ. Он не должен быть тем же, что и от банковского приложения.



Не используйте в ПИН-кодах важные даты

Если вы поставите такой пароль, ребенок сможет разблокировать телефон и оплатить с него покупки без спроса. Это же касается и семейных слов.

В целях безопасности рекомендуется использовать «Программы по блокировки спам-звонков» и «Антивирусы»

«ПРОГРАММЫ ПО БЛОКИРОВКИ СПАМ-ЗВОНКОВ»:

- Наиболее популярные приложения «Who Calls», «Truecaller», «Не звони мне», «Call Blocker», «Яндекс антиспам».
- Так же у всех операторов сотовой связи имеется услуга «Антиспам»;
- Приложения сверяют входящий звонок с базой номеров, которая у них имеется. Если звонок идентифицируется как спам, то приложение уведомляет об этом владельца телефона.

«Антивирусы»:

- Популярные «Касперский», «Avast», «ESET», «NORTON».
- У антивирусов также имеется функция защита от ФИШИНГА, и опасных сайтов;
- Защита от утечки данных о контактах.
- Функция «Антивор» для удаленной блокировки, очистки и поиска телефона.

Как мошенники побуждают граждан совершать преступления!

- **Под предлогом работы по оказанию курьерских услуг, мошенники дают указания забирать деньги у граждан, которые стали жертвами аферистов, и переводить на счета мошенников;**

В 2023 году задержано 7 курьеров действовавших в сговоре с мошенниками в возрасте от 16 до 20 лет.

Указанные действия квалифицируются по ст. 159 УК РФ мошенничество. Указанным лицам грозит лишение свободы сроком от 2 до 10 лет.

- **Лицам которые ранее пострадали от действий мошенников обещают вернуть похищенные деньги, и предлагают совершить незаконную акцию.**

В августе 2023 года 34-летний мужчина и 69-летняя женщина совершили поджог здания бывшего военкомата. Тем самым совершили преступления предусмотренное ст. 205 УК РФ (Террористический акт, то есть совершение поджога устрашающего населения и создающего опасность гибели человека). Предусмотрено наказание до 20 лет лишения свободы.

- **Получение заработка путем предоставления банковских карт мошенникам для обналичивания и перевода денежных средств. (ДРОП)**

Указанные действия наказуемы по ст. 187 УК РФ (Неправомерный оборот средств платежей).

Предусмотрено наказание до 7 лет лишения свободы.

С профилактической информацией можете ознакомиться на сайте МВД по Республике Бурятия

Просканируй меня