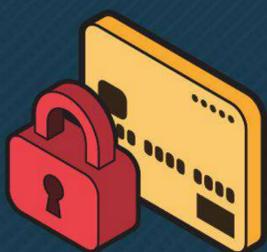




Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ



- Заявление должно быть написано:
- в течение суток после сообщения о списании денег
 - на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию



Банк не компенсирует потери, если вы нарушили правила безопасного использования карты



Подробнее о правилах безопасности
читайте на fincult.info



Финансовая
культура



Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА



1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений



ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

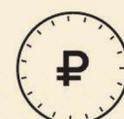


НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные



Как защитить свои финансы,
читайте на fincult.info



Финансовая
культура



Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций



КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

- ! Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой символов
- В адресной строке нет https и значка закрытого замка
- Дизайн скопирован некачественно, в текстах есть ошибки
- У сайта мало страниц или даже одна – для ввода данных карты



КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Установите антивирус и регулярно обновляйте его
- Сохраняйте в закладках адреса нужных сайтов
- Не переходите по подозрительным ссылкам
- Используйте отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой



Подробнее о правилах кибергиены читайте на fincult.info



Финансовая культура



Банк России

КАК ЗАЩИТИТЬСЯ

ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ

Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

ЗАМАНИВАЮТ НА РАСПРОДАЖИ

Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ

Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

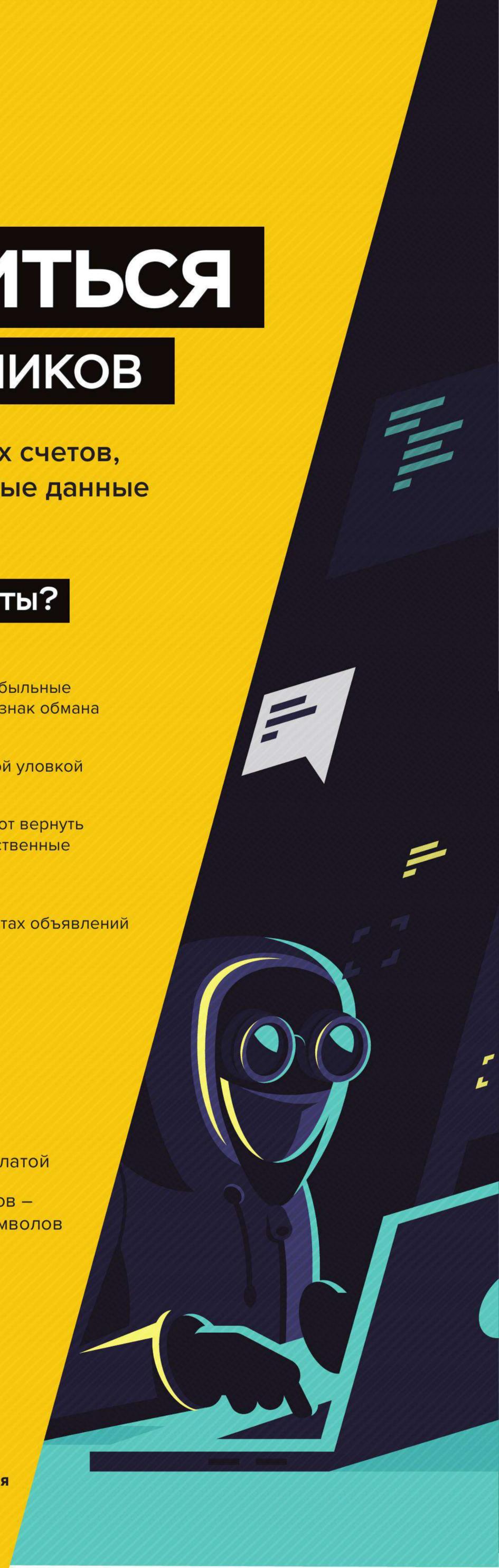
- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на fincult.info



Финансовая культура





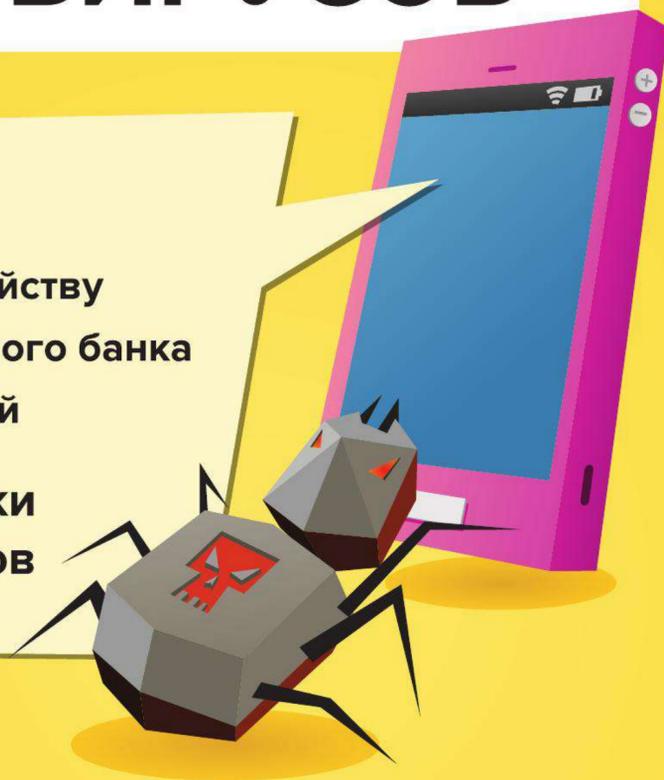
Банк России

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- Позвоните в банк и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- Обратитесь в сервисный центр, чтобы вылечить гаджет
- Перевыпустите карты, смените логин и пароль от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- Используйте антивирус и регулярно его обновляйте
- Не переходите по ссылкам от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения только из проверенных источников
- Обновляйте операционную систему устройства
- Избегайте общедоступных Wi-Fi-сетей



Подробнее о защите гаджетов
читайте на fincult.info



Финансовая
культура

ВНИМАНИЕ!

УЧАСТИЛИСЬ ФАКТЫ МОШЕННИЧЕСТВА

Ежегодно свыше 2,5 тысяч жителей Тамбовской области становятся жертвами мошенников, ущерб от действий которых составляет более 200 миллионов рублей.

КАК РАСПОЗНАТЬ, ЧТО ВАМ ЗВОНИТ МОШЕННИК:

1. Вам поступил звонок от сотрудника банка или сотрудника правоохранительных органов, который сообщает, что от Вашего имени пытаются незаконно оформить кредит и чтобы предотвратить незаконную операцию, необходимо самим оформить кредит и перевести деньги на защищенный счет.



2. Вам поступил звонок от Вашего оператора сотовой связи, который сообщает, что истекает срок действия абонентского договора и чтобы его продлить необходимо продиктовать код из СМС-сообщения, который поступит от портала государственных услуг Российской Федерации. Воспользовавшись названным Вами кодом преступники взламывают личный кабинет портала госуслуг и получают персональные данные.

В ХОДЕ ОБМАНА ПРЕСТУПНИКИ:

- используют технику подмены номеров, в результате чего телефоны преступников соответствуют официальным телефонам банков, либо правоохранительных органов;
- просят оказать помощь правоохранительным органам в поимке мошенников;
- просят перейти с телефонного разговора на общение в мессенджерах (WhatsApp, Telegram), на которые высылают фото поддельных служебных удостоверений сотрудников ФСБ, полиции или следственного комитета;
- настаивают, чтобы в период перевода денег жертва ни с кем не разговаривала, включая своих близких родственников;
- угрожают возбудить уголовное дело за отказ в сотрудничестве.

3. Вам поступил звонок от родственника, который сообщает что попал в беду, например совершил дорожно-транспортное происшествие, и чтобы избежать уголовной ответственности или помочь пострадавшему необходима определенная сумма денег, после чего передает трубку следователю, который обещает помощь и объясняет как передать деньги.



ПРЕДУПРЕЖДАЕМ – ЭТО МОШЕННИКИ!

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

**НЕЗАМЕДЛИТЕЛЬНО ПРЕРВИТЕ РАЗГОВОРИ ПОЗВОНИТЕ
В ПОЛИЦИЮ ПО ТЕЛЕФОНУ 102**

МОШЕННИКИ ЗВОНЯТ ОТ ИМЕНИ

Работников банка,
центробанка

Сотрудников ФСБ

Сотрудников полиции

Сотрудников прокуратуры

Сотрудников
следственного комитета

Операторов сотовой связи

Родственников,
попавших в беду



➤ мошенники могут обращаться к Вам по фамилии, имени и отчеству, ввиду чего может сложиться впечатление, что разговор ведется с представителями банка или государственной организацией.

➤ Мошенники являются хорошими психологами. Они настойчиво могут звонить в течении недели с разных телефонных номеров с целью обмана и завладения денежными средствами.

ЧТОБЫ НЕ ДАТЬ СЕБЯ ОБМАНУТЬ:

НЕ ДОВЕРЯЙТЕ входящим номерам телефонов.

НЕ СОВЕРШАЙТЕ переводов денежных средств на незнакомые счета или электронные кошельки.

**НЕЗАМЕДЛИТЕЛЬНО ПРЕРВИТЕ РАЗГОВОР
И ПОЗВОНИТЕ В ПОЛИЦИЮ ПО ТЕЛЕФОНУ 102**

УБК МВД России



Актуальные способы совершения мошеннических действий

Захват учётной записи мессенджера



**«Злоумышленник
с учётной записи
друга/знакомого»**

Проголосуй за меня пожалуйста, если не сложно конечно)
<https://goo.su/CTcZ34nN>

ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок. Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

Сайт злоумышленников

The screenshot shows a three-step registration process on a scam website. Each step features a blue checkmark icon in a starburst shape.

- Step 1: Выберите Участника**
Заходите и голосуйте за конкурсантов
[продолжить]
- Step 2: Пройдите аутентификацию**
Это нужно для подтверждения уникальности голосов
РОССИЯ
+7 ### ### ### ###
[ДАЛЕЕ]
- Step 3: Подтвердите код**
Мы выслали вам сообщение в Telegram с кодом подтверждения
Код

Указав номер телефона, вы тут же получите код подтверждения, с помощью которого у вас угонят учётную запись

Варианты использования захваченной учётной записи мессенджера



«Злоумышленник

под видом НО
организации»

Добрый день. Это Станислав Викторович начальник вашего отдела. С вами не может связаться наш генеральный директор Андрей Валерьевич и просит ему перезвонить. (сообщает номер)

Злоумышленник используя чужую учетную запись указывает в ней анкетные данные действующего руководителя организации и от его имени связывается с сотрудниками данной организации и злоупотребляя их доверием переводит на диалог с подельниками.



«Злоумышленник

под видом ГД
организации»

Добрый день! Это Андрей Валерьевич! Наш разговор носит строго конфиденциальный характер, разглашение сведений несет за собой уголовную ответственность и будет расценено как содействие СБУ. В руки СБУ попали личные данные более 2500 сотрудников нашей организации, в том числе доступы к банковским счетам, и ваша кандидатура избрана для оказания содействия в их поиске. В настоящий момент злоумышленники оформляют кредиты на сотрудников нашей организации и все имеющиеся средства выводят предположительно в поддержку ВСУ. Для начала, чтобы пресечь попытку списания ваших денежных средств, вам необходимо исчерпать свой кредитный лимит и все имеющиеся на расчетных счетах денежные средства перевести на резервный счет, который я вам сообщу.

Как только жертва связывается с подставным генеральным директором, злоумышленник всеми возможными способами пытается завладеть денежными средствами жертвы.

Варианты использования фейковой учётной записи Telegram



«Злоумышленник

Иван Сергеевич, здравствуйте. Как ваше здоровье? Как работа? Я пишу вам по делу. Хочу вас предупредить, что сегодня Вам будет звонить Нестеров Алексей Александрович, который курирует наше учреждение.

У него есть к вам несколько вопросов. Звонок очень важный, обязательно пообщайтесь!

**под видом другой
учётной записи»**

Создание фейковой учётной записи, не имеющей отношение к пользователю. Ведение переписки от имени другого лица.

«ПОКАЗАТЕЛИ НЕКОРРЕКТНОГО ПОВЕДЕНИЯ»



«Ваша карта заблокирована из-за подозрительной операции»
«Ваша карта (или) счет заблокирован»

«По карте зафиксирована подозрительная операция»



«ДРУГ,
РОДСТВЕННИК»

«Ваш сын попал в аварию, ему срочно требуется дорогостоящее лекарство»

«Ваш сын только что в результате ДТП сбил человека. Я готов помочь избежать наказания»

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК
ЦЕНТРОБАНКА
(БАНКА РОССИИ)»

«По вашей карте зафиксирована сомнительная операция. Для сохранности денег вам нужно перевести их на «безопасный» («специальный») счет в Центробанке»



«ПРЕДСТАВИТЕЛЬ
ПРАВООХРАНИТЕЛЬНЫХ
ОРГАНОВ (МВД, ФСБ, СК РФ)»

«Следователь Следственного комитета. Вы являетесь свидетелем по уголовному делу»
«Иванов В.В., капитан полиции. По вашему паспорту оформлен кредит и указана ваша карта. Нам необходимо уточнить ее реквизиты»

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – ЗЛО

Телефон — основной инструмент мошенников. Большая часть хищений происходит с помощью социальной инженерии

- 1 Обман или злоупотребление доверием
- 2 Психологическое давление
- 3 Манипулирование



Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств

ФОРМУЛА УСПЕХА ТЕЛЕФОННЫХ МОШЕННИКОВ



эффект
неожиданности

+



яркие
эмоции

+



психологическое
давление, паника

+



актуальная
тема

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

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ



«Вы выиграли крупную сумму денег»
«Вам положены социальные выплаты»
«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере...»



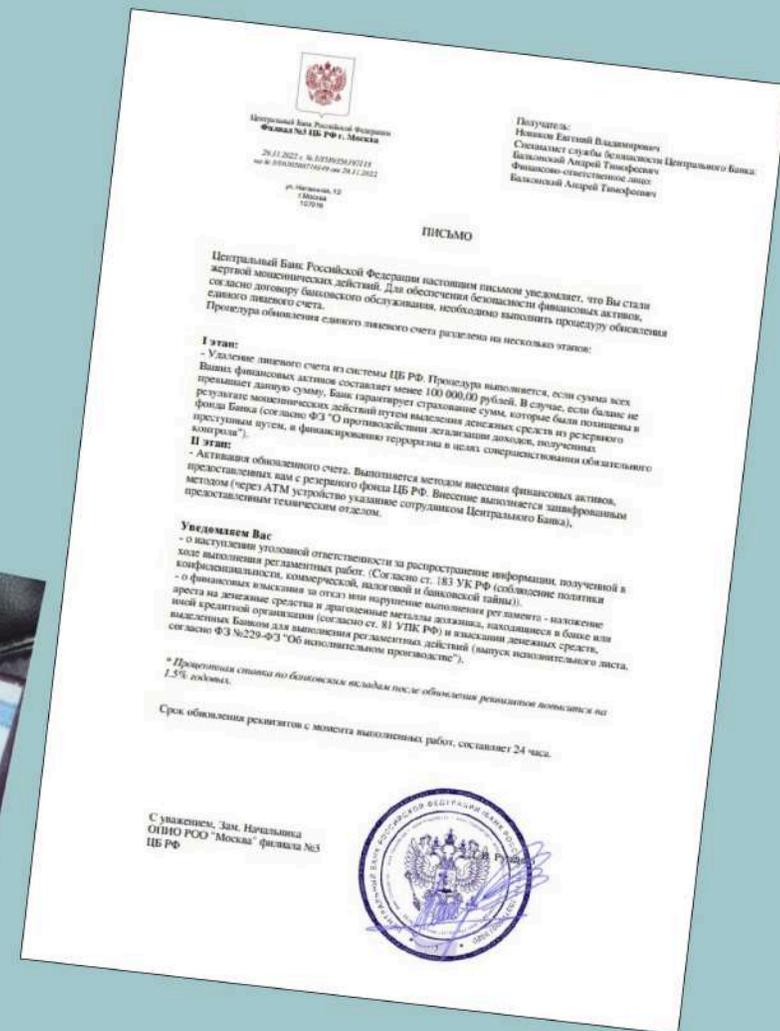
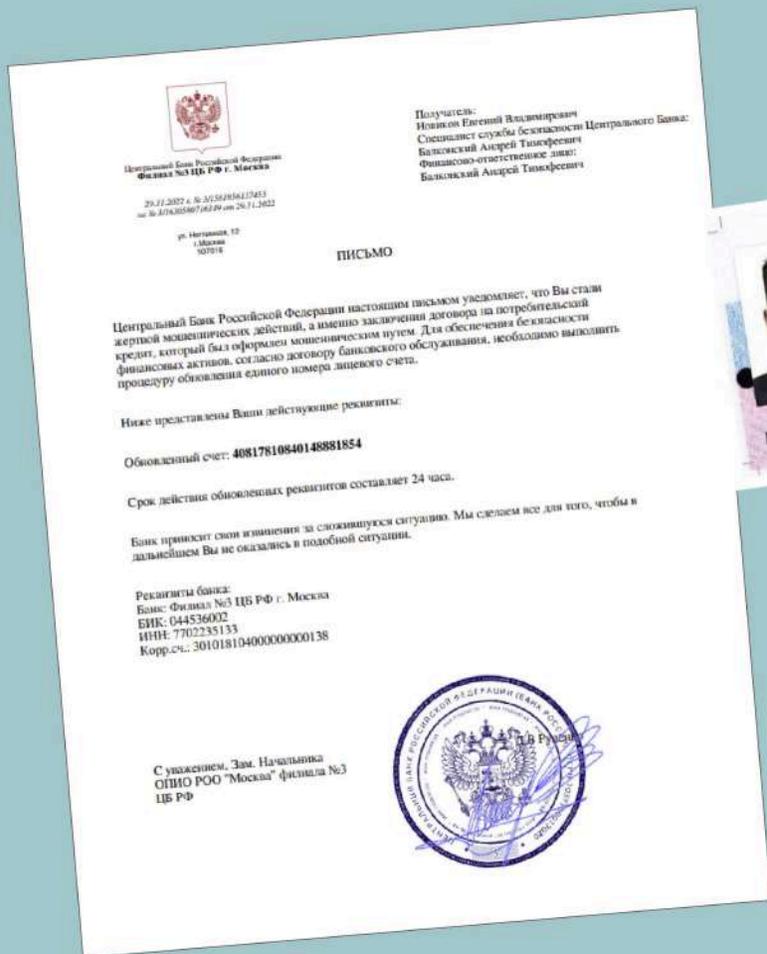
ОТРИЦАТЕЛЬНЫЕ

- СТРАХ ПАНИКА
- ЧУВСТВО СТЫДА



«С вашего счета списали все деньги»
«Ваш родственник попал в аварию и сбил человека»
«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела о... коррупции или...»

ЛЖЕСОТРУДНИКИ ЦЕНТРОБАНКА: ФАЛЬШИВЫЕ ДОКУМЕНТЫ



Онлайн редактор документов

Заполните информацию для документа

Банк ПАО «Сбербанк»

Иск. № 156159602

По месту требования

Документ № 156159602

Paragraph

Банк ПАО «Сбербанк» сообщает, что остаток по счёту г/ки/на ТУТ_ПИШИ_ЧТО_ХОЧЕШЬ_ОНЛАЙН клиента по состоянию на 4/20/2023 составляет:

Тип счёта	Номер счёта	Валюта	Дата открытия счёта	Остаток денежных средств
Счёт погашения	40817810567102536002	Рубли (RUB)	4/20/2023	0.00

Счёт погашения предоставлен для аннулирования возникшей кредитной задолженности из-за компрометации персональных данных в банковской структуре Банк ПАО «Сбербанк». Погашение выполняется через АТМ устройство АО "Альфа-Банк".

Сумма поступления на счет погашения кредита: 0,00 рублей
Сумма возврата кредитных средств: 534 000,00 рублей
Задолженность: 234,00 рублей

Страховой банк - партнер: БАНК

118 WORDS. POWERED BY FINY

Зем. Невьялнина ОГЛЮ РОО "Москва" филиала №1587 СберБанка (ПАО)

А.В. Медведев

Подпись 1

10.09.2021 10.06.2025

Шаг 1 – Внесение данных клиента, редактирование атрибутов стандартных форм под любые Банки и типовые запросы или постановления ПХО

nota.xyz/doc_preview

СБЕР

Иск. № 743297433

Документ № 743297433

Банк ПАО «Сбербанк» сообщает, что остаток по счёту г/ки/на ТУТ_ПИШИ_ЧТО_ХОЧЕШЬ_ОНЛАЙН клиента по состоянию на 4/20/2023 составляет:

Счёт погашения предоставлен для аннулирования возникшей кредитной задолженности из-за компрометации персональных данных в банковской структуре Банк ПАО «Сбербанк». Погашение выполняется через АТМ устройство АО "Альфа-Банк".

Сумма поступления на счет погашения кредита: 0,00 рублей
Сумма возврата кредитных средств: 534 000,00 рублей
Задолженность: 234,00 рублей

Страховой банк - партнер: БАНК

118 WORDS. POWERED BY FINY

Зем. Невьялнина ОГЛЮ РОО "Москва" филиала №1587 СберБанка (ПАО)

А.В. Медведев

Подпись 1

10.09.2021 10.06.2025

Print 1 page

Destination Save as PDF

Pages All

Layout Portrait

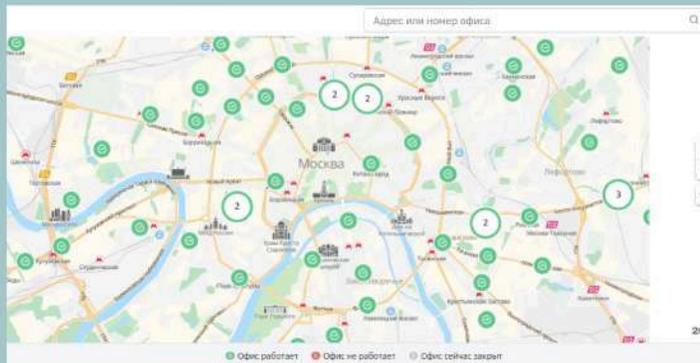
More settings

Содержимое документа:

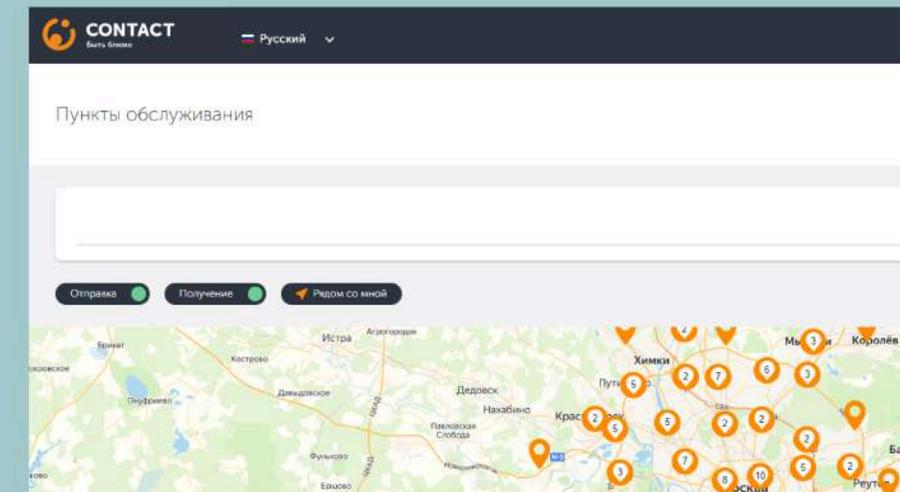
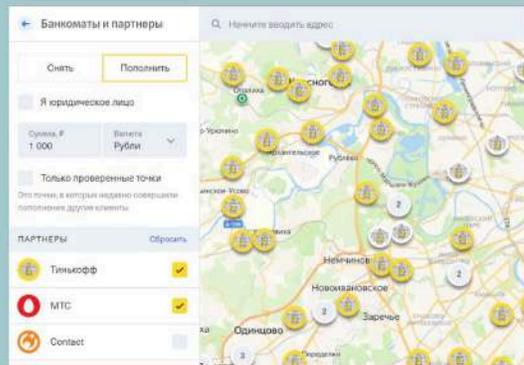
Paragraph

Шаг 2 – моментальная загрузка отрисованного поддельного документа в формате PDF

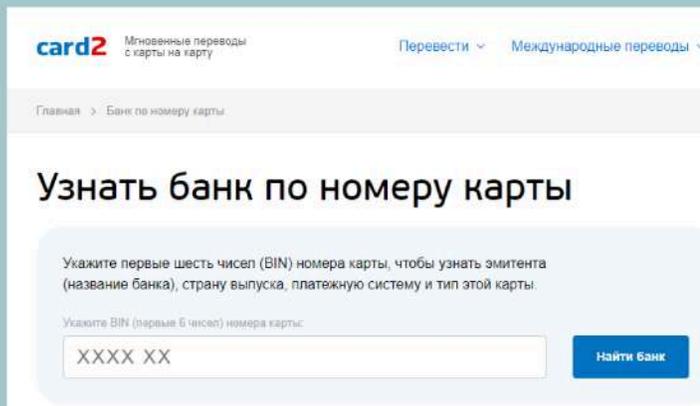
Общедоступные сервисы в быстром доступе



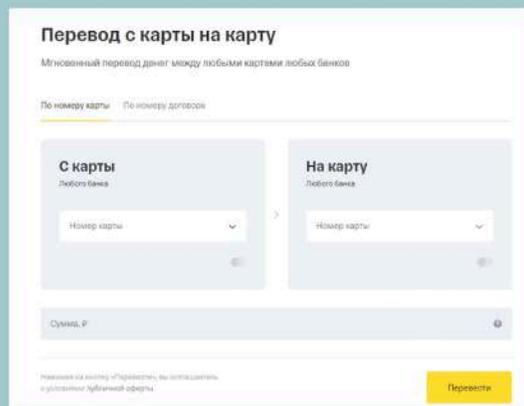
Банкоматы Сбера и Тинькофф с CASH IN



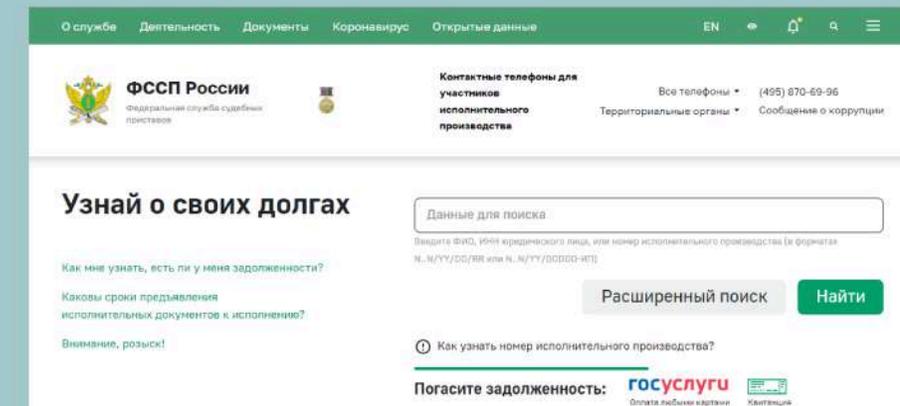
Карта терминалов Contact (денежные переводы)



База BIN банковских карт



C2C от Тинькофф



ФССП проверка долгов

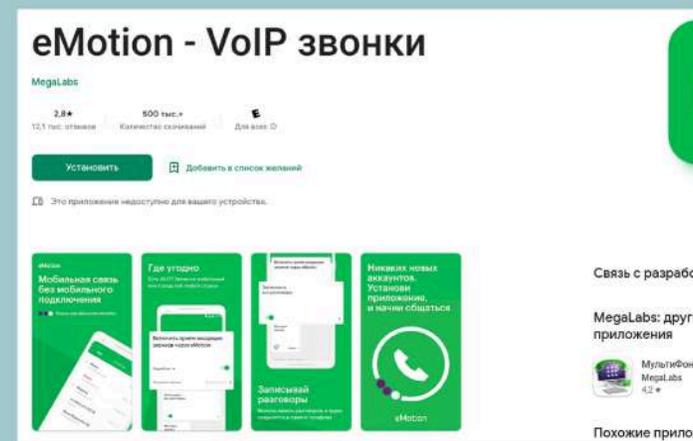
Инструментарий мошеннического КЦ



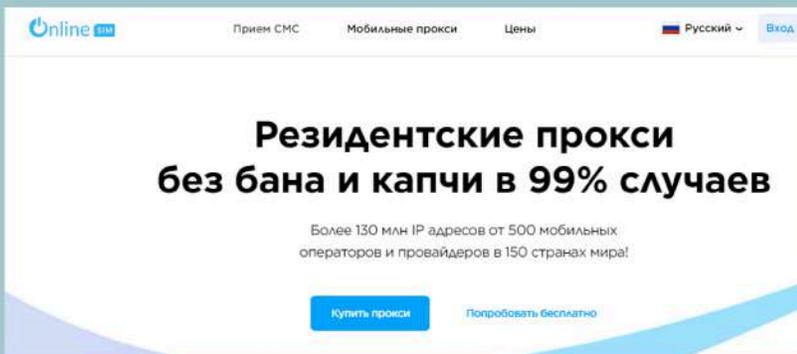
Прокси в РФ, VPN от vip72.com



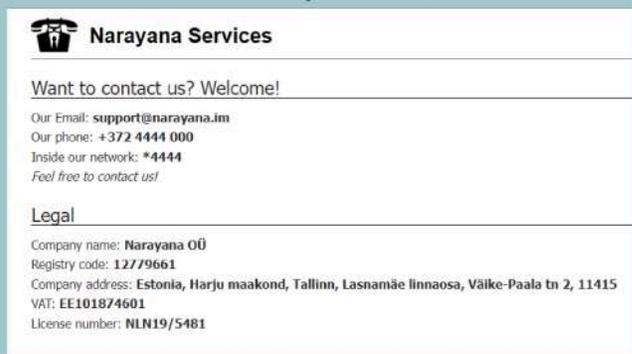
VoIP звонки через МТС Коннект



VoIP звонки eMotion от Мегафона



Прокси в РФ, виртуальные номера телефонов от OnlineSim.io



SIP телефония от Narayana (Эстония)



SIP телефония + подмена номера от Gargona Telecom



Подписка на TG бот «Глаз Бога» («пробив» по номеру телефона)

+ покупка номеров с балансом операторов РФ и номеров для WhatsApp

Интерфейс оператора мошеннического КЦ

Общие скрипты:

- Вариант МВД
- 12 вариантов под прикрытием
- Служба Аварийная
- Служба РФ
- Вариант МВД РФ
- Вступлении Шенгена
- Служба Дворника
- Новый сайт РАБОТАЕМ со ...
- Заблуды закрытие новости
- Служба Маршал

Мои скрипты:

- КАК СПРОСИТЬ ЗА ПМНОЕ П...
- КАК СПРОСИТЬ ЗА ДОХОД

Передачи:

- Передал Лёха Найк в 27.03.2023, 14:07:37
Анонимда Александровна Рамель Шайдуллин
79501793292
- Передал Монетка в 18.04.2023, 14:37:42
Валера Еловикова
79277799838
- Передал Монетка в 18.04.2023, 18:32:00
Евгений Звездоч Евгений Звездоч Звездоч
Евгений Звездоч Евгений Звездоч Звездоч Звездоч
ЕВГЕНИЙ ЕВГЕНЬЕВИЧ
79852880400

Услуги:

- Услуга
- Нет кредита
- Служба
- Служба
- Надёжность
- Надёжно
- Удалить
- Не существует
- Перезвон
- Перезвон

Роман Николаев Роман Иванович; Николаев Роман; Николаев Роман Иванович; Роман Николаев; Роман Николаев

Текущий статус: в работе

Текущая: **ТЕКУЩАЯ ЗАДАЧА**

Телефон: 79507002286

Позвонить

Город: Смоленск, Смоленская обл

Адрес:

Часовой пояс: UTC+3: 19:23

Возраст:

Дов. поле 5 : gajg2e5-130@yml.ru

1. ФИО Звонящего -
2. ФИО Мошенника -
3. Город -
4. Банк -
5. Личное дело -
6. Официальное трудоустройство -
7. Налоговые задолженности -
8. Кредитные задолженности -
9. ЛЯ -
10. Доход -

- Актуализация информации о клиенте
- Быстрый доступ к 350+ вариантам скриптов разговора
- «Тегирование» клиента по результату звонка
- Онлайн редактор поддельных документов
- Онлайн тестирование Сотрудника
- Ссылки на сайты банков и проверки карт

Геолокация мошеннических КЦ



Данные ПАО Сбербанк

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;

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 Самостоятельно позвоните близкому человеку / в банк / в организацию

6 Не перезванивайте по незнакомым номерам

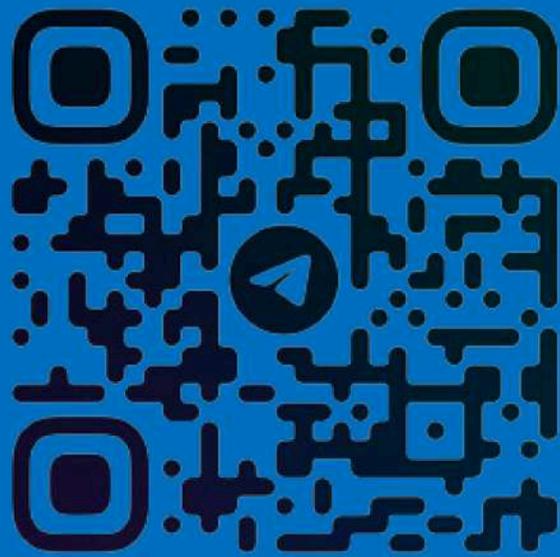
7 Не сообщайте CVV/CVC и иные данные банковских карт

8 Внимательно проверьте от кого поступают сообщения



Возьмите паузу и спросите совета у родных и друзей!

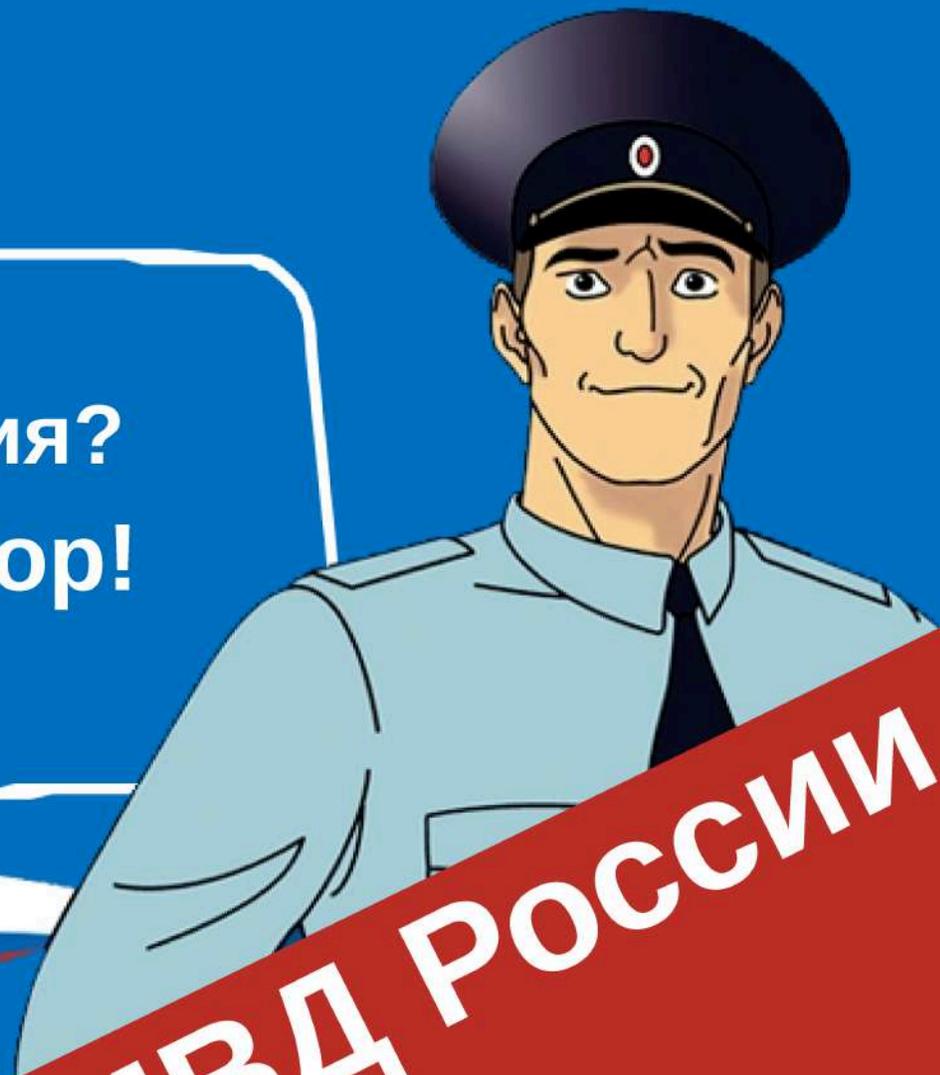
Подписывайся чтобы быть в курсе
и не попасть на уловки мошенников



@CYBERPOLICE_RUS



Возникли сомнения?
Прерви разговор!
Звони в 112!



УБК МВД РОССИИ