

Актуальные способы совершения мошеннических действий

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Самым «действенным» способом мошенничества остаётся **социальная инженерия** – обман на доверии. Суть социальной инженерии состоит в том, что злоумышленник **вводит в заблуждение жертву** и та выполняет его инструкции, сама отдаёт ему деньги либо пароль от личного кабинета в онлайн-банке.

Надо отметить, что характерной чертой современных правонарушителей является **беспринципность действий**. Мошенники с помощью психологического манипулирования заставляют людей делать то, что они делать не собирались, обманным путём выманивая у них последние сбережения, заставляя брать на себя кабальные кредитные обязательства.

Ключевым фактором, способствовавшим совершению указанных преступлений, является низкий уровень правовой и финансовой грамотности населения.



МВД РОССИИ ПРЕДУПРЕЖДАЕТ
Будьте бдительны! звоните 02 или 102

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖОСХ и т.д. перезвоните и уточните, направляли ли к Вам этого специалиста!

НЕ ДОВЕРЯЙТЕ, если Вам звонит и сообщает, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться. **Это ОБМАН!**

СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ
Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!

Не подписывайте никакие документы!

Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам? **НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!**

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

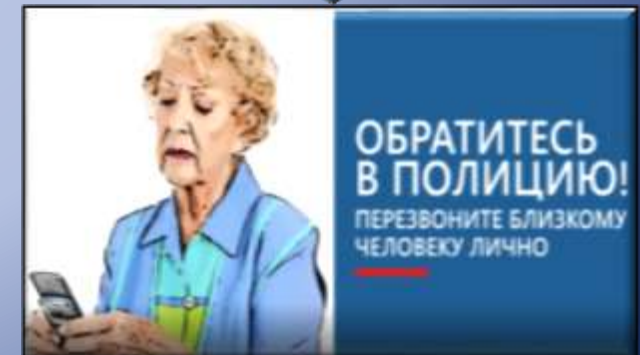
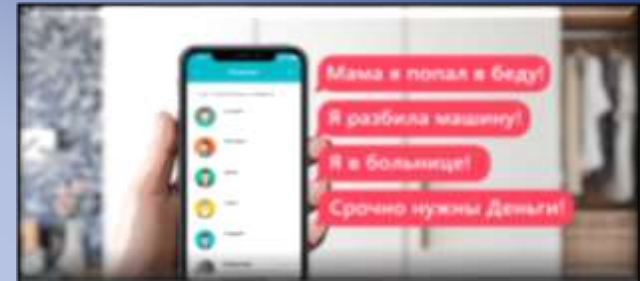
Обман по телефону: «Меня задержали, но можно откупиться»

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном заявляет, что уже не раз помогал людям таким образом. Для решения вопроса необходима определённая сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.

Поступил сомнительный звонок ? Вам необходимо:

- прервать разговор и перезвонить тому, о ком идёт речь;
- если телефон отключён, связаться с его родственниками и друзьями для уточнения информации;
- если разговор происходит якобы с представителем правоохранительных органов, узнать, из какого он подразделения;
- набрать «02» и уточнить в дежурной части названного Вами подразделения, действительно ли родственник туда доставлен.



SMS, СООБЩЕНИЯ – ПРОСЬБА О ПОМОЩИ



Абонент получает сообщение на мобильный телефон: «У меня проблемы, кинь денег на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

Пожилым людям, детям и подросткам следует объяснить, что на сообщения с незнакомых номеров реагировать нельзя, это могут быть мошенники!



ТЕЛЕФОННЫЙ НОМЕР – ГРАБИТЕЛЬ

Вам приходит сообщение с предложением перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, проблемы со связью или с Вашей банковской картой и другие.

После набора номера Вас долго держат на линии. Когда это надоест, Вы отключаетесь – и оказывается, что с Вашего счёта списаны крупные суммы.

НА САМОМ ДЕЛЕ:

Мошенники регистрируют сервис с платным звонком без предупреждения абонента о снятии платы за звонок.

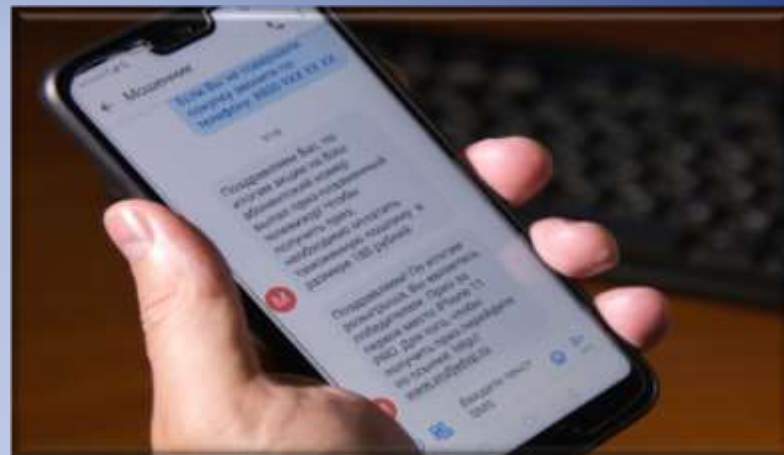
Будьте бдительны, совершая звонок по чужой просьбе!

Единственный способ обезопасить себя от телефонных мошенников – это не звонить по незнакомым номерам!

«ВЫИГРЫШ» В ЛОТЕРЕЮ

Мошенники направляют сообщения с неизвестных номеров о выигрыше с просьбой осуществить перевод денежных средств для его получения либо вернуть якобы направленные (переведённые) ошибочно Вам денежные средства.

Если раньше мошенники звонили людям по телефону и рассказывали о выигрыше в лотерее, потом посылали такую информацию в SMS или по электронной почте, то сейчас им достаточно создать группу в социальной сети или мессенджере – «клиенты» придут сами.



Необходимо помнить, что человек не может выиграть приз, не участвуя в лотереях, родственники не будут отправлять сообщения с неизвестных номеров. Это обман. В этой связи не стоит отвечать на данные сообщения, а тем более отправлять информацию о своей банковской карте и переводить денежные средства!

«ОШИБОЧНЫЙ» ПЕРЕВОД СРЕДСТВ

Вам приходит SMS-сообщение о поступлении средств на счёт, переведённых с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг. Сразу после этого поступает звонок и Вам сообщают, что на Ваш счёт ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

Если Вас просят перевести якобы ошибочно переведённую сумму, посоветуйте с чеком о проведённой операции обратиться в отделение банка.

Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник.

ДЕНЬГИ ЗА ОНЛАЙН-ОПРОС

Мошенники предлагают ответить на несколько простых вопросов в Интернете, обещая выплатить баснословные деньги. Однако, чтобы их получить, нужно заплатить «комиссию». Естественно, после этого никакие деньги участнику опроса не приходят.



Бесплатный адвокат

Юридическая Консультация
БЕСПЛАТНО



Мошенники звонят гражданам и сообщают, что они стали потерпевшими по уголовному делу и им полагается адвокат. Его услуги якобы бесплатны, но нужно заплатить «госпошлину» – несколько тысяч рублей. Следует иметь в виду, что законом это не предусмотрено.

Если Вам предлагают просто так что-то очень выгодное, то скорее всего это обман. Не нужно верить таким предложениям.

КОМПЕНСАЦИЯ ОТ «МИНЗДРАВА РОССИИ»

Мошенники в социальных сетях рассылают фейковую информацию, в которой сообщают гражданам, что им положены социальные выплаты, например, компенсация расходов на лекарства, а дальше предлагают пройти по указанной ссылке.

Зачастую злоумышленники пишут от первого лица: «Да, действительно вышел новый закон, я на себе проверил!». В доказательство прикладывают скриншоты с переводом денег от «Сбербанка». Их цель, чтобы человек перешёл по ссылке на сайт, в названии которого иногда даже используется слово «Минздрав», и ввёл свои персональные данные.



КОМПЕНСАЦИЯ ОТ «МИНФИНА РОССИИ»

Обычно таким образом обманывают потерпевших от преступлений. Им звонят и говорят, что правительством выделена значительная компенсация для тех, кто пострадал от финансовых пирамид и других мошенничеств. Но, чтобы получить деньги, нужно якобы заплатить 1% от суммы компенсации.



Необходимо помнить, что мошенники рассылают подобные фейковые сообщения от различных государственных органов. Не поддавайтесь на их уловки!

МОШЕННИЧЕСТВА, СВЯЗАННЫЕ С ПРОВЕДЕНИЕМ ЧАСТИЧНОЙ МОБИЛИЗАЦИИ И СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

В настоящее время злоумышленники хорошо ориентируются в политической ситуации в стране, изобретая все новые предложения для вымогательства денежных средств у граждан. Например, участились мошеннические действия, связанные с проведением частичной мобилизации, путем осуществления злоумышленниками звонков:

- с предложением на платной основе услуг по обжалованию действий, связанных с нарушениями в ходе частной мобилизации;
- под видом сотрудников правоохранительных органов с угрозами лицам мужского пола уголовной ответственностью за уклонение от частичной мобилизации, одновременно предлагая за денежное вознаграждение «освобождение от призыва»;
- о предоставлении услуг по переводу из «первой очереди призыва» в «третью очередь призыва», оформлении отсрочки от призыва с использованием поддельных документов (справки о болезни, дипломы IT-специалиста и т.д.), оказание помощи в трудоустройстве по специальности, не подпадающей под частичную мобилизацию;
- под видом сотрудников правоохранительных органов с угрозами уголовной ответственностью за перевод денег в Украину и спонсирование террористических организаций;
- под видом участников волонтерских организаций о сборе денежных средств, якобы, для участников специальной военной операции и беженцев или «перевода» денежных средств в фонд «Вернись живым»;
- об «оказании помощи» в переезде граждан из Украины на территорию Российской Федерации за денежное вознаграждение.

В соответствии с законодательством Российской Федерации граждан, воспользовавшийся указанными «услугами», подлежит привлечению к уголовной ответственности наравне с тем, кто данную «услугу» оказал.



МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определённый номер для получения подробной информации. Когда Вы это делаете, Вас просят сообщить номер карты, CVC-код или ПИН-код для её перерегистрации.

Для того, чтобы ограбить Вас, злоумышленникам нужны лишь реквизиты Вашей карты. Получив их, мошенники незамедлительно снимут деньги с Вашего счёта!



Необходимо помнить, что ни одна организация, включая банк, не вправе требовать Ваши CVC-код (трёхзначный код) или ПИН-код. Для того, чтобы проверить поступившую информацию о блокировке карты, следует самим позвонить в клиентскую службу поддержки банка (её телефон указан на оборотной стороне карты). Скорее всего, специалисты ответят, что Ваша карта продолжает обслуживаться банком.

ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ОБРАЩЕНИИ С БАНКОВСКИМИ КАРТАМИ

Нельзя:

- хранить ПИН-код рядом с картой, записывать его на бумаге;
- прибегать к помощи третьих лиц при проведении операций с банковской картой в банкоматах;
- позволять посторонним лицам использовать Вашу пластиковую карту.

ФИШИНГ

Вид интернет-мошенничества, цель которого – получить Ваши персональные данные, получил название (от англ. fishing – рыбная ловля, выуживание).

Злоумышленники рассылают электронные письма от имени банков, платёжных систем, маркетплейсов и сервисов. Пользователю предлагается зайти на интернет-ресурс – точную копию настоящего сайта организации, которой человек склонен доверять.

Для дальнейшей возможности использовать свою пластиковую карту Вас просят указать её CVC-код и другие данные. Впоследствии эти данные используются для хищения денежных средств, содержащихся на Вашем счёте.

Фишинг используется мошенниками также на сайтах знакомств, поиска работы, консультационных услуг и т.д.



Следует помнить:

- банки и платёжные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой о предоставлении своих данных;
- сотрудники банка располагают достаточной информацией о своих клиентах;
- сотрудники банка могут у Вас спросить кодовое слово в том случае, если Вы им сами позвонили.

Если звонят «из банка», то попросите «сотрудника» набрать Вам через пять минут. Прервав разговор с незнакомцем, позвоните сами в свой банк по номеру, который указан на Вашей карте, и поговорите с реальной службой поддержки банка.

ВРЕДОНОСНЫЕ ПРОГРАММЫ И ТАКТИКА БОРЬБЫ С НИМИ

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и распространяют вредоносные программы.

Вредоносные программы – любое программное обеспечение, которое предназначено для скрытного (несанкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом «вирусы». Их можно разделить на три группы: компьютерные вирусы, сетевые черви, троянские программы.



ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

- установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы;
- регулярно обновляйте: антивирусные программы либо разрешайте автоматическое обновление при запросе программы, пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы;
- не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников – скачанные с неизвестных веб-сайтов, присланные по электронной почте;
- по возможности, не сохраняйте в системе пароли и периодически меняйте их.

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



Выберите Участника

Заходите и голосуйте за конкурсантов

продолжить



Пройдите аутентификацию

Это нужно для подтверждения уникальности голосов

 **РОССИЯ**

+7 ### ## ## ##

ДАЛЕЕ



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

**под видом другой
учётной записи»**

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!

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

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК
БАНКА»

«С вашей карты пытаются перевести деньги»

«Ваша карта (счет) заблокирована»

«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 расстаётся 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...»



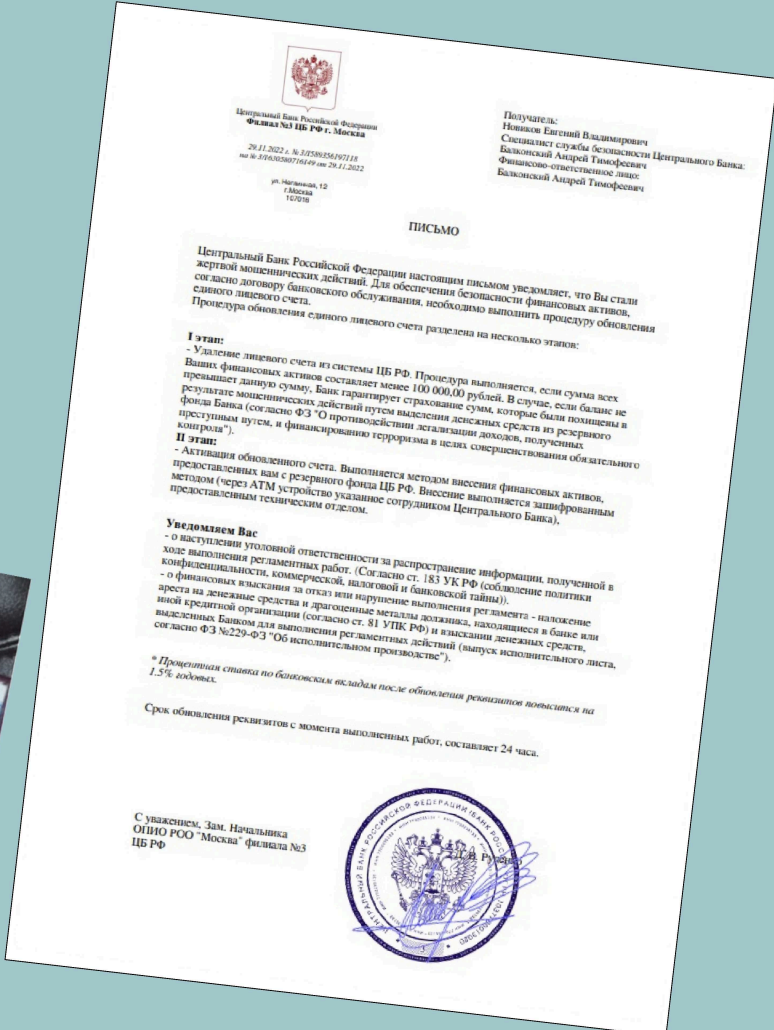
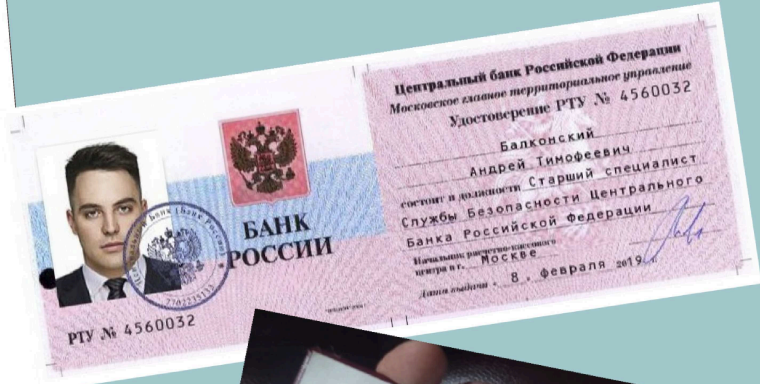
ОТРИЦАТЕЛЬНЫЕ

- 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

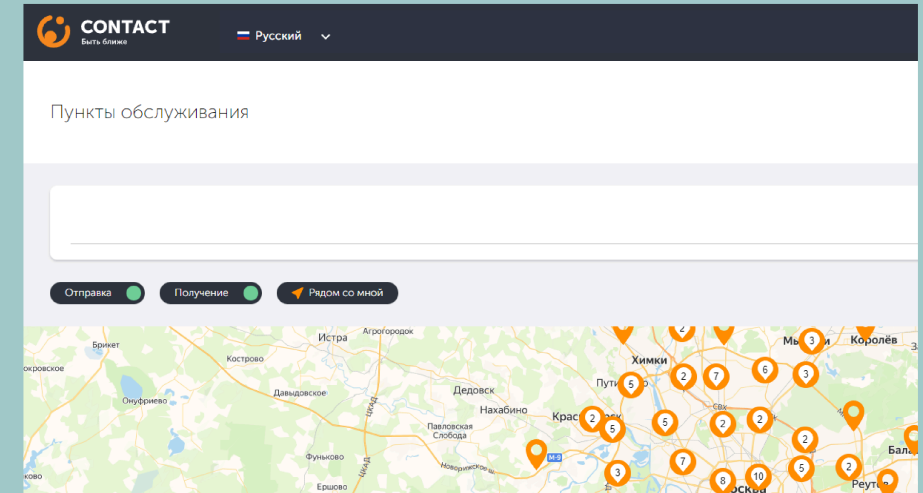
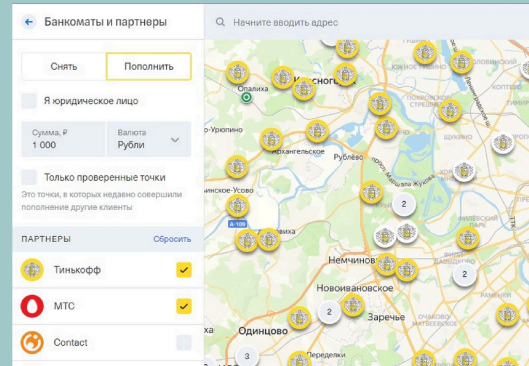
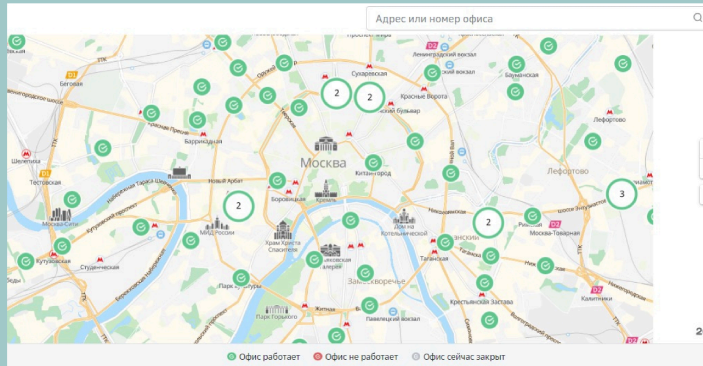
[illegible]

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

[illegible]

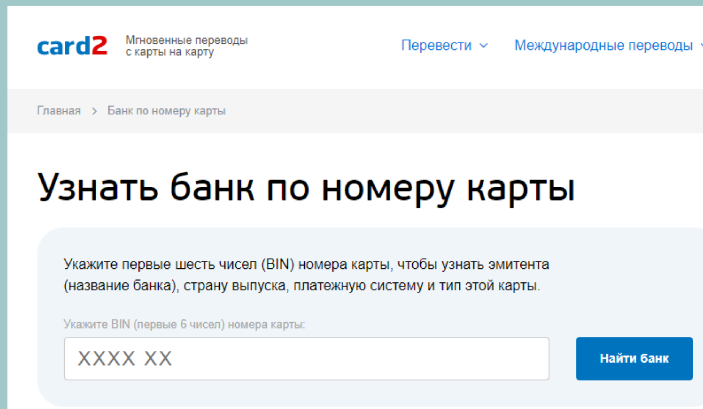
Шаг 2 – моментальная загрузка отрисованного поддельного документа в формате PDF

Общедоступные сервисы в быстром доступе

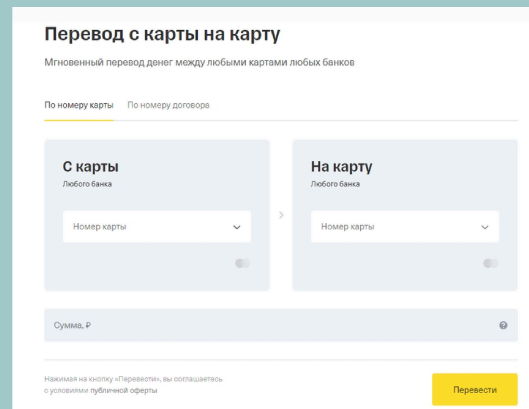


Банкоматы Сбера и Тинькофф с CASH IN

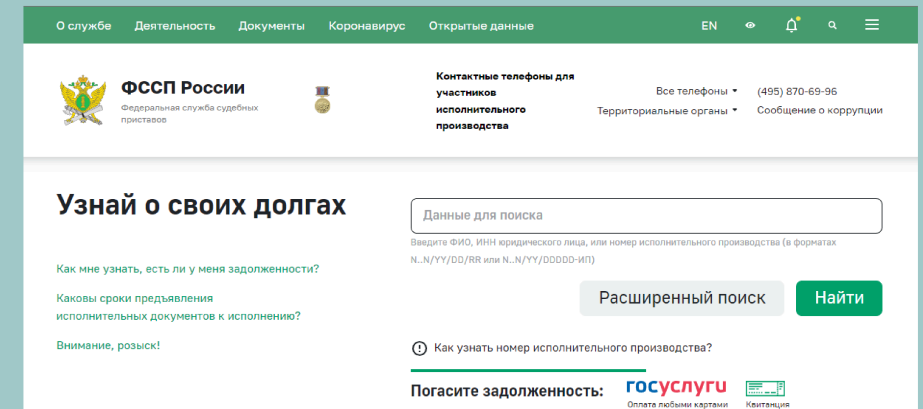
Карта терминалов Contact (денежные переводы)



База BIN банковских карт

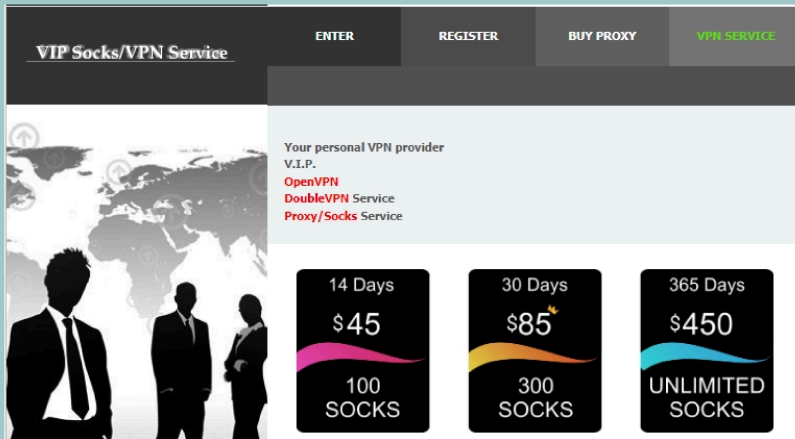


C2C от Тинькофф

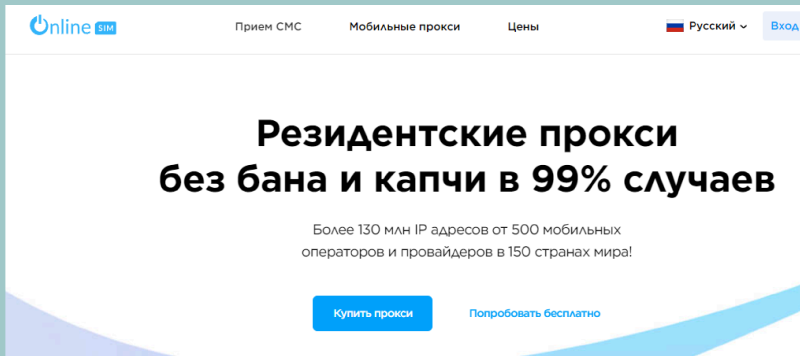


ФССП проверка долгов

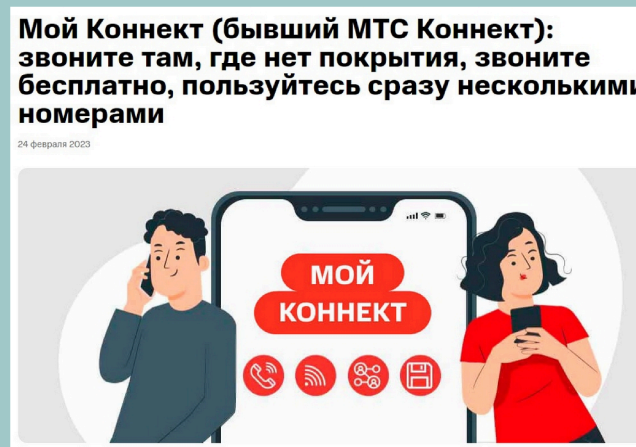
Инструментарий мошеннического КЦ



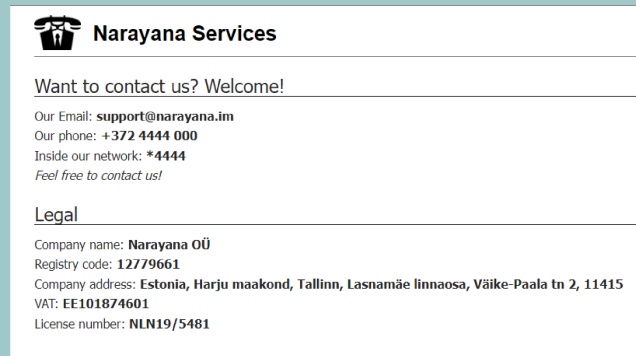
Прокси в РФ, VPN от vip72.com



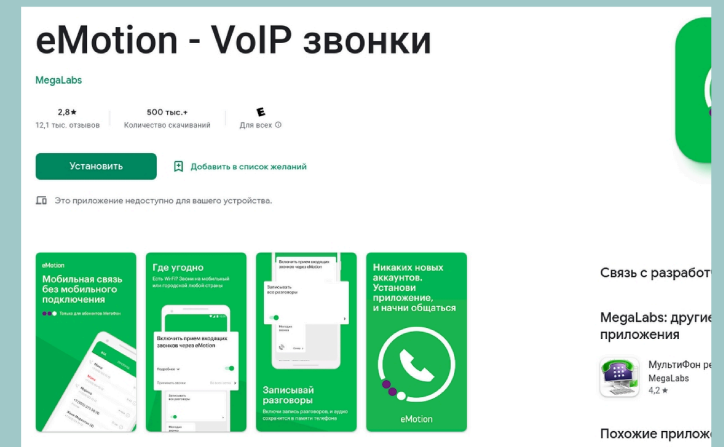
Прокси в РФ, виртуальные номера телефонов от OnlineSim.io



VoIP звонки через МТС Коннект



SIP телефония от Narayana (Эстония)



VoIP звонки eMotion от Мегафона



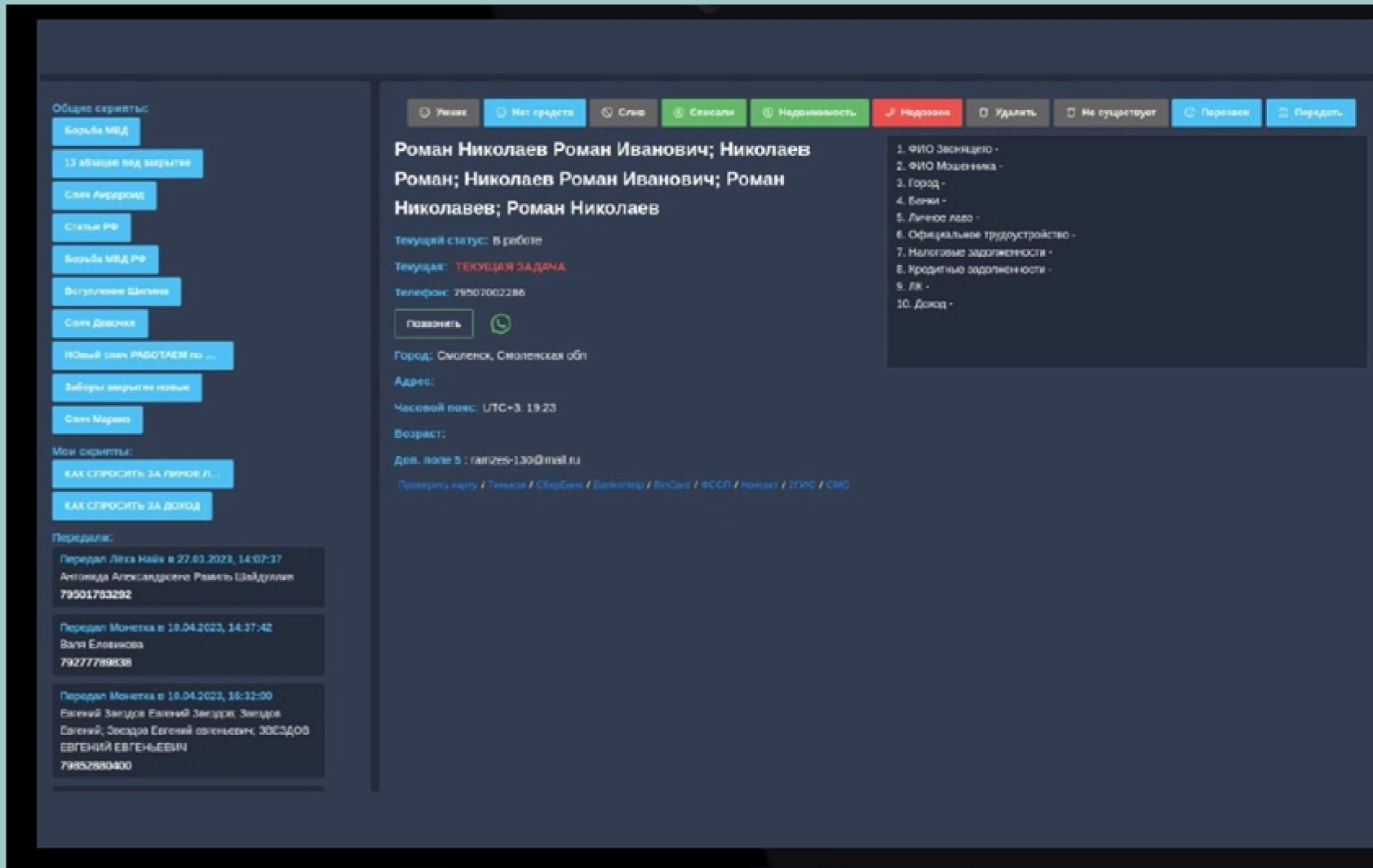
SIP телефония + подмена номера от Gargona Telecom



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

+ покупка номеров с балансом операторов РФ и номеров для WhatsApp

Интерфейс оператора мошеннического КЦ



- 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

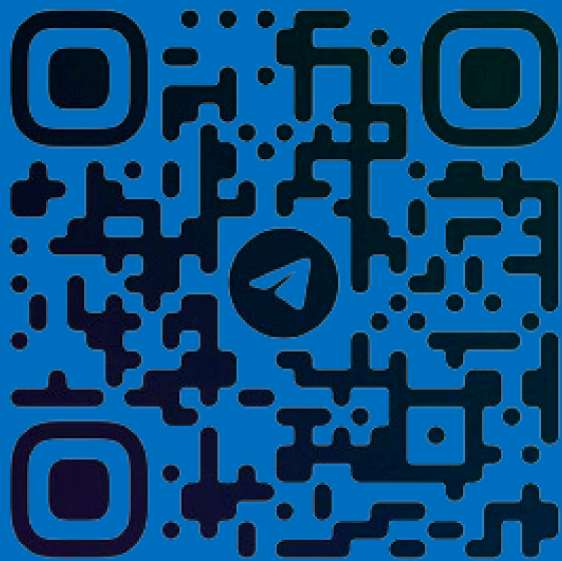


- 5** Самостоятельно позвоните близкому человеку /в банк / в организацию
- 6** Не перезванивайте по незнакомым номерам
- 7** Не сообщайте CVV/CVC и иные данные банковских карт
- 8** Внимательно проверьте от кого поступают сообщения



**Возьмите паузу
и спросите совета
у родных и друзей!**

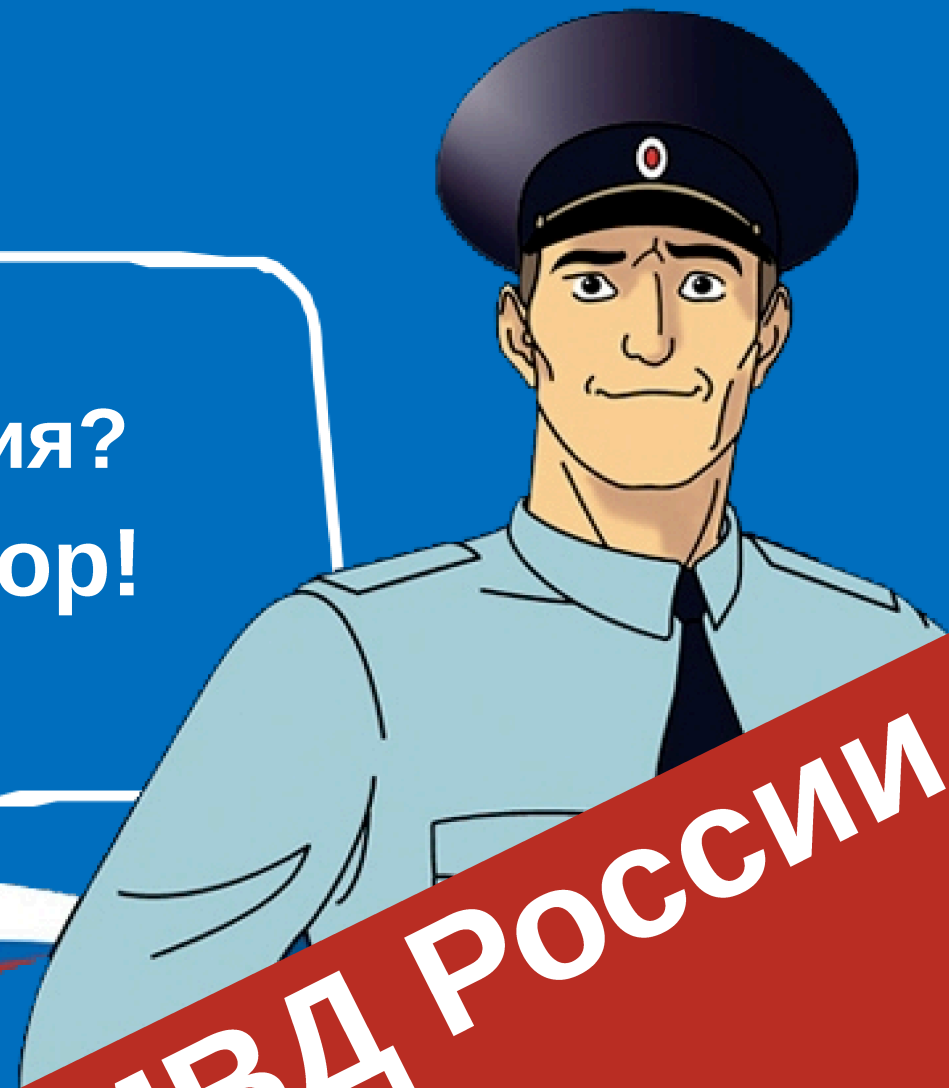
Подписывайся чтобы быть в курсе
и не попасть на уловки мошенников



@CYBERPOLICE_RUS



Возникли сомнения?
Прерви разговор!
ЗВОНИ В 112!



УБК МВД РОССИИ