ФИНАНСЫ

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН

справедливо-центр.рф
8-800-755-55-77

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Как распознать мошенника
Если украли деньги со счета
Если на вас взяли кредит
Если взломали «Госуслуги»

ПРОГРАММА ПРАВОВОГО ПРОСВЕЩЕНИЯ ГРАЖДАН

ЦЕНТР ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Как распознать мошенника

Если украли деньги со счета

Если на вас взяли кредит

Если взломали «Госуслуги»

СОДЕРЖАНИЕ

В декабре 2023 года пенсионеру Владимиру Ушакову позвонил псевдосотрудник оператора сотовой связи. Сообщил, что истек срок действия сим-карты.

Услуга по замене платная, но при дистанционной замене скидка составит 20%. И прислал ссылку на применение скидки.

Пенсионер нажал на кнопку. На телефон тут же стали сыпаться СМС с ПИН-кодами. Через какое-то время «сотрудник» перезвонил и попросил продиктовать коды для активации сим-карты.

В считаные минуты телефонные мошенники опустошили счет пенсионера и оформили на него кредит в 430 000 рублей. После чего вывели кредитные деньги и заблокировали телефон.

Во владимирском Центре защиты прав граждан пострадавшему помогли обратиться в полицию. Там возбудили уголовное дело по краже, совершенной с банковского счета (п. «г» ч. 3 ст. 158 УК РФ).

Одновременно с этим сотрудники Центра составили исковое заявление в суд, чтобы признать кредитный договор недействительным.

Ленинский районный суд города Владимира освободил пенсионера от обязательств по погашению кредита.

Эта история закончилась благополучно. Но далеко не каждый, кто угодил в сети мошенников, может вернуть украденные деньги или отказаться от чужого кредита.

В стрессовой ситуации, когда требуется срочно что-то предпринять, человек теряется. Это естественно. А мошенник, который вогнал в этот стресс, «помогает» разрешить ситуацию. Всего-то понадобится назвать код из СМС или продиктовать реквизиты банковской карточки.

В 2024 году мошенники украли у россиян 150 млрд рублей. Однако вернуть обманутым гражданам удалось только 12% выведенных средств.

Увы, вопреки предупреждениям и горькому опыту знакомых, граждане верят звонкам «следователей» и из «Центробанка», диктуют одноразовые коды, которые высылают мошенники, чтобы заполучить доступ к карточному счету или аккаунту жертвы на «Госуслугах», переводят деньги знакомым, якобы попавшим в трудную ситуацию.

В новой инструкции Центров защиты прав граждан расскажем, как противостоять любым уловкам преступников, если соблюдать правила финансовой безопасности.

4 ПРИЗНАКА ТОГО, ЧТО ВАМ ЗВОНИТ МОШЕННИК

ПРИЗНАК 1. Мошенник всегда звонит сам

Во всех случаях мошенник звонит или пишет первым. И всегда с новостями: «у вас истек срок действия сим-карты», «вам положена надбавка к пенсии», «вы подозреваетесь в спонсировании терроризма», «у вас долг по налогам».

ПРИЗНАК 2. Разговор всегда про деньги или льготы

Вас начинают либо запугивать потерей денег, либо предлагать деньги и «плюшки».

В первом случае – это «срочно переведите деньги на безопасный счет», «кто-то прямо сейчас оформляет на вас кредит».

Во втором случае – обещания легкого заработка, приглашение на диспансеризацию, бонусы за покупку или выигрыш в лотерею.

ПРИЗНАК 3. Выуживает данные, просит коды из СМС

Даже если разговор как бы не про деньги, а, к примеру, запись на «диспансеризацию», разговор все равно сведется к тому, что вы должны назвать личные данные.

Задача мошенника – получить информацию, которая даст доступ к банковскому счету или порталу «Госуслуги».

ПРИЗНАК 4. Призывает действовать немедленно

Прямо сейчас нажать на ссылку, назвать отправленный в СМС код, данные банковской карты, подтвердить номер СНИЛС и т. п.

Вам не дают возможности на раздумье. А в случае промедления злоумышленник начинает на вас наседать, шантажировать или откровенно запугивать.

КАК ЗАЩИТИТЬ БАНКОВСКУЮ КАРТУ

Доступ к вашим банковским сбережениям получить довольно просто.
К сожалению, доверчивые граждане сами сообщают необходимые сведения злоумышленникам:

- ❑ называют срок действия карты;
- ❑ называют три цифры с оборота карты (CVV/CVC-код);
- ❑ диктуют одноразовые коды из СМС, которые позволяют войти в Личный кабинет в банковском приложении;
- ❑ переходят по вредоносным ссылкам, которые активируют доступ к вашему счету, направленным в СМС, на почту или в мессенджерах.

Какие банковские реквизиты МОЖНО СООБЩАТЬ посторонним лицам

Вообще лучше не сообщать никакие. Но, допустим, вам на счет должны перевести деньги. Перевод ожидаемый. Деньги должны перевести частное лицо или организация.

Без опаски вы можете сообщить отправителю следующие сведения:

- **Название банка и номер телефона, к которому привязан счет.**

Этого вполне достаточно, чтобы вам перевели деньги по номеру телефона через Систему быстрых платежей (СБП).

- **Номер банковской карты, который расположен на лицевой стороне карты (состоит из длинного набора цифр).**

Этих данных вполне достаточно, если вам хотят перевести деньги через приложение другого банка, терминал или банкомат.

При этом ни в коем случае не называйте данные с обратной стороны карты – CVC-код (или CVV-код), который состоит из трех цифр.

- **Номер расчетного счета. Он состоит из 20 цифр.**

Эти реквизиты может попросить организация. Которая, допустим, рассчитывается с вами за какие-то услуги и ей требуются полные реквизиты того банка, где у вас открыт счет. Получить выписку с реквизитами своего банка можно на сайте банка, скачать из мобильного приложения или в отделении банка в бумажном виде по паспорту.

Запрос расчетного счета банка, а также БИК банка, корреспондентского счета, ОГРН и т. п. не представляет риска для ваших личных сбережений на счете.

Какие банковские реквизиты НЕЛЬЗЯ СООБЩАТЬ никому. Даже настоящему сотруднику банка

Никому, даже сотрудникам банка, где у вас хранятся сбережения, нельзя называть:

1) **Три цифры с оборота карты (CVV-код или CVC-код).** Эти три цифры на оборотной стороне вашей карты должны быть известны только вам.

2) **Пароли и одноразовые коды банковских уведомлений**, которые банк вам присылает для подтверждения поступления или списания денег, входа в Личный кабинет банка и т. п.

Настоящие сотрудники банка сами могут его проверить.

3) **ПИН-код банковской карты.** Вы получаете его в запечатанном конверте, когда заключаете договор с банком. Храните его вместе с договором дома, никому не предоставляйте доступ к этим документам.

ЗАПОМИНАЕМ!

1. Не передавайте информацию о своих счетах и картах посторонним лицам без надобности.

2. Не публикуйте данные своей карты или ее фото в соцсетях и в мессенджерах. К примеру, пересылая фотографию родственнику, чтобы он перевел на карту деньги.

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИК ПОЛУЧИЛ ДОСТУП К СЧЕТУ

Если мошенники не успели вывести деньги, необходимо успеть заблокировать карту.

1. СРОЧНО ЗАБЛОКИРУЙТЕ КАРТУ

Заблокировать карту, данные которой вы назвали мошеннику, можно несколькими способами:

- **Через мобильное приложение банка.** Если у вас на телефоне установлено приложение вашего банка, зайдите в него и найдите опцию блокировки карты. Выберите нужную карту (если у вас их несколько и вы назвали CVV/CVC-код конкретной карты), нажмите «Заблокировать».

- **По телефону горячей линии банка.** Номер для экстренной связи указан на оборотной стороне карты и на официальном сайте банка. Лучше всегда иметь номер банка под рукой, чтобы не тратить время на поиски. Оператор попросит назвать паспортные данные, кодовое слово или код из СМС-сообщения, которое вышлет. После этого сотрудник банка заблокирует карту.

- **Онлайн, на сайте банка.** Зайдите в Личный кабинет на сайте банка, найдите опцию «Заблокировать карту» и подтвердите свое действие кодом из СМС.

- **По СМС.** Некоторые банки позволяют блокировать карты по СМС. Надо отправить на короткий номер банка кодовое слово (например, «блокировка») и через пробел последние четыре цифры номера карты. Если у вас только одна карта, цифры можно не вводить – банк поймет, о какой карте речь. Вы получите код, который надо снова отправить на номер банка для подтверждения блокировки.

Если карт несколько, введите четыре последние цифры счета той карты, данные которой передали мошеннику.

Вы получите код, который надо снова отправить на номер банка для подтверждения блокировки.

- **В отделении банка.** Если отделение банка расположено неподалеку, возьмите паспорт и отправляйтесь в офис банка. Сотрудник банка заблокирует карту по вашему заявлению. Тут же можно сразу подать заявление на возврат денег, если мошенники уже произвели списание *(как это сделать, расскажем ниже)*.

После блокировки закажите в банке новую карту.

У нее будут новые реквизиты. Для онлайн-банка необходимо будет придумать новые логин и пароль.

2. ОДНОВРЕМЕННО С БЛОКИРОВКОЙ КАРТЫ ОГРАНИЧЬТЕ ДИСТАНЦИОННЫЙ ДОСТУП К БАНКОВСКОМУ СЧЕТУ

Если злоумышленники заполучили доступ к вашему Личному кабинету на сайте банка (такое возможно, если по продиктованному вами ПИН-коду мошенники получили доступ к порталу «Госуслуги» и отвязали карту от вашего номера телефона), попросите сотрудника банка немедленно отключить дистанционный доступ к счету.

Иначе мошенники не просто все деньги украдут – оформят по этим реквизитам на вас онлайн-кредит, а деньги выведут.

Если мошенники начали списывать деньги, задача – заблокировать карту и вернуть похищенные деньги.

3. ПОДАЙТЕ В БАНК ЗАЯВЛЕНИЕ НА ВОЗВРАТ ПОХИЩЕННЫХ ДЕНЕГ

Даже если вы сами назвали все коды-пароли мошеннику, обязательно напишите заявление о несогласии с операцией по списанию средств и требуйте вернуть списанные деньги на ваш счет.

Во-первых, с сентября 2018 года банки обязаны приостанавливать денежные переводы и платежи с карт, если те выглядят подозрительными.

Основания: Федеральный закон от 27.06.2018 №167-ФЗ *(«О внесении дополнений в Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе» и Федеральный закон №395-1 «О банках и банковской деятельности»)*.

При любой подозрительной активности на счете клиента, особенно если ранее клиент не был замечен в такой активности, банк обязан блокировать подозрительный перевод и оповестить об этом клиента.

- **Если клиент подтвердит действия по карте,** банк разблокирует операцию и проведет транзакцию.

- **Если клиент сообщит, что не делал перевод,** банк обязан отменить операцию и предложить клиенту перевыпустить карту.

Во-вторых, согласно Федеральному закону от 24 июля 2023 года №369-ФЗ (которым были внесены поправки в Федеральный закон «О национальной платежной системе»), банк обязан вернуть похищенные мошенниками деньги, если:

- *банк допустил перевод средств на мошеннический счет, данные о котором находятся в специальной базе Банка России;*
- *банк не направил гражданину уведомление о совершении перевода без согласия клиента;*
- *банковская карта была потеряна (или ей воспользовались без согласия владельца), и владелец ранее уведомил банк об этих фактах.*

ВАЖНО ЗНАТЬ!

Если мошенники украли деньги с карты, а ваш банк не сообщил вам об операции, он обязан возместить потери. Даже в том случае, если вы обнаружили кражу денег со счета не сразу, а через месяц или год после того, как она произошла.

Итак, пишем заявление в банк с требованием вернуть незаконно списанные деньги.

Заявление подаем в двух экземплярах.

На экземпляре, который останется у вас, потребуйте поставить отметку о дате и времени регистрации заявления у банковского работника.

Это нужно для того, чтобы у вас были доказательства, что банк такое заявление принял.

Банк обязан провести служебное расследование.

Если мошенники действовали на территории России, расследование займет 30 дней, если операция была международной – 60 дней.

По итогам расследования с вами свяжется сотрудник банка и сообщит о решении. Если банк убедится, что вы не нарушали правила использования карты, вам вернут деньги.

Если банк не вернул деньги на ваш счет в течение 30 дней (60 – для международных денежных операций), можете обращаться в суд.

Обязательно потребуйте предоставить вам письменный отказ с обоснованиями причины отказа.

Если банк не предоставил отказ в письменной форме или вы не согласны с приведенными аргументами в отказе, следует обратиться в суд.

4. ОБЯЗАТЕЛЬНО ОБРАТИТЕСЬ В ПОЛИЦИЮ

Кража денег – уголовное преступление. Напишите заявление в полицию. Возможно, ваша информация поможет быстрее вычислить и поймать преступников.

ЗАЧЕМ МОШЕННИКАМ ВАШ НОМЕР СНИЛС

«Пройдите диспансеризацию!»

Злоумышленники маскируют свои действия под звонок из поликлиники на прохождение диспансеризации. «Сотрудник» поликлиники не просит паспортные данные или номер карты.

Все вполне безобидно – продиктуйте свой СНИЛС.

СНИЛС требуется, когда:

- вас прикрепляют к поликлинике;
- при регистрации на портале «Госуслуги», где СНИЛС может выполнять функцию логина;
- при заключении трудового договора с работодателем;
- при голосовании в электронных общих собраниях собственников жилья на ГИС ЖКХ;
- при подаче заявления о поступлении в образовательное учреждение (в вуз, колледж);
- **в составе персональных данных при подаче заявки на выдачу кредита (займа).**

СНИЛС не даст мошеннику мгновенного доступа к деньгам. Но с помощью СНИЛС мошенники перехватывают коды подтверждения из государственных или банковских сервисов. Чтобы оформить, к примеру, кредит.

Схема работает так: сначала заполучили СНИЛС. А спустя какое-то время вам перезвонят из «поликлиники», «МФЦ» или «пенсионного Фонда», обратятся по имени-отчеству, для достоверности назовут даже СНИЛС, а потом попросят подтвердить какую-либо социальную услугу и для подтверждения продиктовать поступивший на телефон ПИН-код.

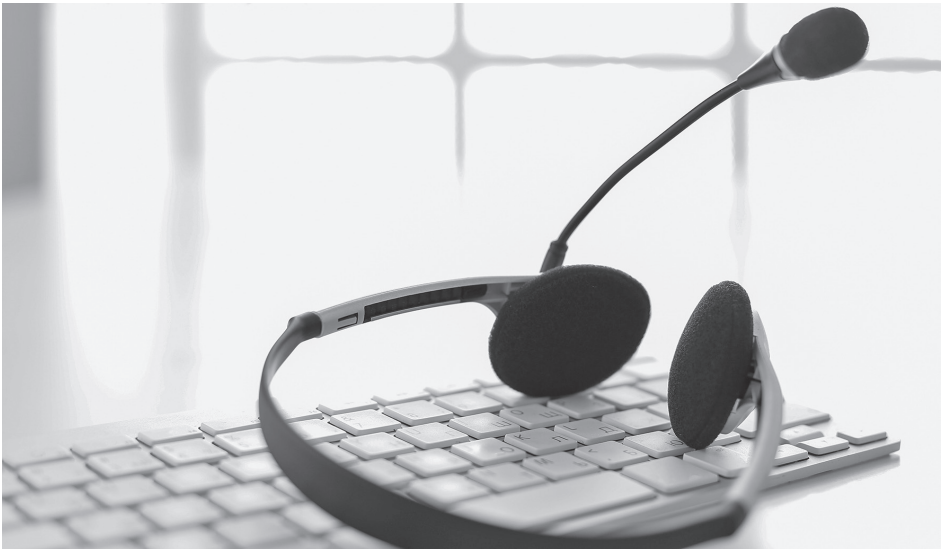
ЗАЧЕМ МОШЕННИКАМ ДОСТУП К ВАШЕМУ АККАУНТУ НА ПОРТАЛЕ «ГОСУСЛУГИ»

Взлом аккаунта позволит мошеннику:

- *заказать справку о ваших доходах;*
- *получить информацию о ваших счетах в банках и отвязать банковские карты от вашего телефонного номера;*
- *получить информацию о пенсионных накоплениях;*
- *оформить на ваше имя фиктивный бизнес;*
- *переоформить от вашего имени имущество в чужую собственность;*
- *подать заявку на выдачу кредита или микрозайма.*

К примеру, получив доступ, злоумышленник регистрируется онлайн в банке под вашим логином и паролем и подает заявку на кредит от вашего имени.

Кредитор одобряет заявку и перечисляет деньги на карту или счет, указанные мошенником. Преступник исчезает, а вы становитесь должником по чужому кредиту.



РАСПРОСТРАНЕННЫЕ СХЕМЫ КРАЖИ ПО ТЕЛЕФОНУ

Звонок из прокуратуры, ФСБ, от полицейского или следователя

Лжесиловики – майоры и полковники полиции, сотрудники ФСБ, Следственного комитета или прокуратуры – излюбленная тема мошенников.

Позвонивший уверенным голосом представляется, называет вас по имени-отчеству и напористым тоном предупреждает, что разговор будет конфиденциальным, сообщать о нем никому нельзя.

А потом заявляет, что вы являетесь «пособником террористов, так как с вашей карты осуществлялись списания на противоправные действия».

Второй вариант – «вы – соучастник денежной махинации».

Третий вариант – «вы – жертва крупной махинации, и необходимо оказать содействие следствию».

Вариантов много, результат один – вам предлагают ряд манипуляций, чтобы снять с себя подозрения.

Дальше вас просят либо установить на телефон специальное приложение для удаленного доступа, с помощью которого можно раскрыть преступную сеть.

Либо оформить «защищенный» счет и перевести на него все деньги на период «следственных действий».

Особо продвинутые аферисты могут прислать даже поддельные документы, где значится, что вы соучастник преступления.

Если вы вовремя не положите трубку, потеряете не только сбережения на карте. На вас могут взять кредит. И даже довести до продажи имущества.

ЗАПОМИНАЕМ!

1. Сотрудники ФСБ, силовых ведомств, судебных и правоохранительных органов никогда не звонят и не рассылают СМС. Они не работают в мессенджерах.

2. Правоохранительные органы не переводят звонки на банк или Центробанк. Даже если к вам есть вопросы у правоохранительных органов, вам не станут звонить через мессенджеры, просить устанавливать какие-то программы на телефон или переводить деньги на «безопасный» счет.

3. Если установлен факт правонарушения, эти структуры воспользуются повестками, могут произвести задержание, вызвать в суд. Но никак не вести сомнительные беседы по телефону.

Что делать, если вам позвонили из «органов»

- Сразу блокируйте такой контакт.
- Если все же вступили в диалог, ни в коем случае не сообщайте личные данные: серию и номер паспорта, информацию о количестве денег на счетах, реквизиты счета. Сотрудники госструктур никогда не запрашивают такую информацию.
- Не верьте, если вам говорят, что решить вопрос можно деньгами, например с помощью перевода на карту физлица. И тем более не соглашайтесь привозить наличные по определенному адресу или передавать их лично в руки какому-либо человеку.
- Если вы решили убедиться, что вам не звонили настоящие силовики, положив трубку, позвоните по официальным номерам в те органы, сотрудником которых представился мошенник.

Звонок из «Центробанка»: переведите деньги на хранение в Центробанк

Вам звонят якобы из Банка России и предупреждают, что кто-то пытается украсть деньги с вашего счета. Чтобы «спасти» их, надо срочно перевести все средства на хранение в «Центробанк».

По легенде, деньги переводятся на «спецсчет» (вариации – «технический счет», «зеркальный счет») на период розыска преступников. После поимки всю сумму вам вернут наличными в «приемной банка в Москве».

Чтобы убедить, что все чинно-благородно, мошенники даже «запишут» вас на личный прием в ЦБ. На ваш телефон тут же поступит СМС-подтверждение такой записи с короткого номера Центробанка (300).

По аналогии, как ранее подделывали короткий номер Сбера (900), вместо ноликов там могут быть буквы З-О-О. Или все три цифры будут с короткими пробелами. Тем не менее это работает!

Особо сомневающимся могут направить в мессенджер даже поддельное удостоверение сотрудника ЦБ с логотипом и печатью Банка России.

Ну а дальше все по схеме: злоумышленники высылают реквизиты «безопасного» счета, куда вы собственноручно переводите все сбережения.

ЗАПОМИНАЕМ!

- Центробанк не работает с физическими лицами как с клиентами.
- Сотрудники ЦБ не звонят гражданам.
- Центробанк не ведет денежные счета граждан и не направляет им копии своих документов.

Даже если у вас в телефоне высветился короткий номер Центробанка (300), помните: отображаемый номер абонента на вашем мобильном устройстве не означает, что именно с него осуществляется звонок.

Что делать, если позвонили из «Центробанка»

1. Не вступайте в диалог – сразу положите трубку.
2. Если прислали СМС с «записью на прием», ни в коем случае не открывайте ссылку – сразу удалите. Ссылка может содержать вредоносную программу, которая предоставит мошенникам доступ к содержимому вашего телефона.
3. После прекращения разговора заблокируйте номер телефона, с которого вам звонили, и пожалуйтесь на звонок в настоящую Службу Центробанка.

Звонок из «пенсионного Фонда»: вам положена прибавка к пенсии

Такие аферы проворачивают с пожилыми людьми. Мошенник представляется работником некоего «пенсионного Фонда» и сообщает пожилому человеку, что у того обнаружен неучтенный трудовой стаж. Если прямо сейчас подать заявку, ему переведут прибавку к пенсии и компенсацию за все прошлые годы.

Или: «Государство решило всем пенсионерам сделать надбавку. Как, вы не читали закон? Вам положены 10 000 рублей.

За деньгами никуда ходить не надо. Продиктуйте реквизиты карты и назовите ПИН-код из СМС. Мы вам все переведем прямо сейчас».

Так аферисты получают доступ к деньгам пенсионера. В том числе и пенсионным накоплениям.

ЗАПОМИНАЕМ!

- Сотрудники Соцфонда не обзванивают граждан, чтобы пересчитать пенсию или начислить доплату.
- Даже если пенсионеру причитается надбавка к пенсии, доплата будет произведена Соцфондом на ту карту, куда приходит ежемесячная пенсия, автоматически.

Звонок из «соцзащиты»: вам положены льготы на ЖКУ

В условиях подорожания жилищно-коммунальных услуг на такую уловку покупаются не только пожилые граждане.

Мошенник сообщает, что пенсионеру (льготнику, многодетной семье и т. п.) положена 50-процентная скидка на плату, к примеру, за свет.

Оформить скидку надо в МФЦ, но там большие очереди, и лучше записаться на прием заранее.

Для подтверждения записи просят сверить номер СНИЛС, а затем продиктовать ПИН-код из СМС.

После того как вы назовете код, мошенник получит доступ к вашему аккаунту на «Госуслугах». Зайдет в вашу учетную запись, отвяжет банковские карты от вашего телефона или возьмет на вас онлайн-кредит.

ЗАПОМИНАЕМ!

Чтобы узнать, какие виды социальной помощи действуют в вашем регионе, а также уточнить, положены ли вам какие-то льготы, необходимо лично обратиться в клиентскую службу Социального фонда России по месту жительства или МФЦ.

Звонок от «инженеров»: идет проверка связи

Мошенник представляется инженером оператора сотовой связи или интернета. Объясняет, что много жалоб на качество связи и проводится проверка телефонной линии.

Далее просит набрать на телефоне комбинации #09 или #90, чтобы убедиться, что сигнал в порядке.

При наборе этой комбинации можно потерять доступ к сим-карте и мобильному банку. Мошенник без проблем зайдет в ваше мобильное приложение и опустошит все счета и вклады.

Звонок от «оператора связи»: истек срок пользования номером

Мошенник сообщает, что у вас закончился срок договора с сотовым оператором либо закончился срок использования телефонного номера. Если не продлить, номер передадут другому абоненту.

Вас попросят назвать код из СМС. А в итоге вы предоставите доступ к банковскому приложению, с которого оплачиваете услуги оператора связи.

Пример из практики Центров защиты прав граждан

Так, жительнице Архангельска Наталье Иевлевой «сотрудник оператора сотовой связи» пригрозил: если не перезаключите срочно договор, потеряете номер телефона. И тут же обрадовал: в офис идти не нужно – назовите код из СМС, и все продлим.

Наталья согласилась. Поступившие коды назвала «специалисту».

Таким образом мошенники получили доступ к Личному кабинету на сайте сотового оператора, который оказывал в том числе и банковские услуги.

На имя Натальи открыли счет и оформили кредит на 300 000 рублей, 250 000 рублей злоумышленники успели обналичить в банкомате.

Наталья обратилась в полицию. Конечно, преступников не нашли. Сотовый оператор отказался списывать кредит с обманутой пенсионерки.

В архангельском Центре защиты прав граждан пенсионерку успокоили: злоумышленники обманным путем получили доступ к Личному кабинету в приложении сотового оператора. Кредитный договор был подписан в онлайне. Это противоречит ст. 820 ГК РФ, где четко говорится, что кредитный договор должен быть заключен в письменной форме, иначе он считается ничтожным. Банк оператора связи должен был обеспечить безопасность дистанционного предоставления услуг.

Правозащитники помогли Наталье обратиться в суд.

Ломоносовский районный суд признал кредитный договор недействительным и избавил истицу от погашения кредита.

СХЕМЫ КРАЖИ ДЕНЕГ В МЕССЕНДЖЕРАХ

«Это был голос внука, я перевела деньги!»

Мошенники с помощью искусственного интеллекта могут подделать голос или видеоизображение родственника, друзей и коллег по работе. И вот уже «родственник» просит выручить деньгами или прислать фотографию банковской карточки, чтобы перевести вам деньги.

Так, 67-летняя Вера Георгиевна ранним воскресным утром получила аудиосообщение от внука, что тот попал в ДТП. Чтобы «договориться на месте», внук попросил перевести на карту «гаишника» 25 тысяч рублей. Перевела. «Внук» сообщил, что платеж не проходит, прислал ссылку, по которой перевод точно дойдет. Так мошенники обнулили карту Веры Георгиевны. Никакой внук, разумеется, денег у нее не просил.

ЗАПОМИНАЕМ!

1. Прежде всего обезопасьте персональные данные.

Создайте сложный пароль доступа к аккаунтам в мессенджерах и соцсетях, в Личные кабинеты приложений банка, на порталах официальных ведомств, различных служб поддержки и даже интернет-магазинов. Подключите двухфакторную идентификацию для входа. Ограничьте доступ в свой профиль посторонних людей.

2. Проанализируйте, что вы размещаете на просторах интернета, какой информацией делитесь в мессенджерах.

3. Удалите из частных переписок с родственниками, коллегами или друзьями любую информацию, содержащую персональные данные. К примеру, фото банковской карточки, паспорта, служебных удостоверений, СНИЛС, водительских прав и т. д.

4. При получении аудио- или видеосообщения с просьбой дать денег (или срочно выслать данные банковской карты, ПИН-код от входа в «Госуслуги» и т. п.) **первым делом свяжитесь с тем, от кого получено сообщение.**

Нет возможности сделать это сразу – не спешите реагировать.

Найдите способ убедиться, что сообщение направлено знакомым вам человеком, а не нейроподделкой.

Придумайте секретный вопрос с ответом или кодовое слово, известное только близким, на тот случай, если действительно возникнет чрезвычайная ситуация.

5. Позаботьтесь о финансовой безопасности пожилых родственников.

Подключите в их телефонах защиту от спама. Объясните, что делать, если звонят из «Центробанка» или «полиции». Расскажите, что предпринять, если вдруг от вашего имени и вашим голосом попросят срочно перечислить деньги.

6. Сообщите о попытках мошенничества в полицию и службу техподдержки сервиса, откуда поступил запрос.

Оповестите о взломе аккаунта или попытке цифрового шантажа всех, с кем контактируете в соцсетях и мессенджерах.

Звонок из «банка»: срочно переведите деньги на безопасный счет»

Телефонный мошенник звонит и сообщает, что с вашего счета прямо сейчас кто-то пытается снять деньги (или оформляет кредит). Необходимо переложить все деньги на «защищенный» счет.

Схема не новая. Теперь ее слегка модернизировали.

Если вы кладете трубку, вам тут же перезванивает «представитель службы безопасности банка» и подтверждает, что ваши деньги хотят украсть.

Он подчеркивает, что до этого вам наверняка звонил мошенник. И пока банк «ищет преступника», действительно следует переложить сбережения на «безопасный» банковский счет.

«Представитель службы безопасности банка» просит вас активировать высланный код в СМС либо назвать CVV-код вашей карты, чтобы собственноручно переложить ваши сбережения на временный безопасный счет.

Пример из практики Центров защиты прав граждан

Осенью 2023 года жительнице Томска Лидии Козловой через WhatsApp позвонил «сотрудник службы безопасности» банка, клиенткой которого она является.

Звонивший сообщил, что прямо сейчас неизвестные пытаются оформить на нее онлайн-кредит. Поэтому немедленно нужно «сделать защиту» счета. Женщина от неожиданности поверила и нажала на ссылку в сообщении, которое ей прислали.

После чего телефон «сошел с ума», Лидия даже не смогла его выключить и просто в ужасе наблюдала на экране, как на ее имя оформили онлайн-кредит, после чего деньги тут же начали выводить частями по разным счетам. В общей сложности мошенники вывели 85 600 рублей.

Пока Лидия пыталась перезагрузить смартфон, чтобы попробовать блокировать карту, ее супруг звонил в банк с просьбой помочь заморозить дистанционный доступ к счету жены.

Но в банке, похоже, никого не смутило, что в течение нескольких минут женщина оформила кредит и тут же вывела средства в шесть разных направлений.

В блокировке карты отказали на том основании, что об этом просил муж Лидии, который звонил со своего телефона. Мужчина пытался сказать сотруднику, что телефон жены взломали, но оператор горячей линии сообщил, что ничем помочь не сможет.

Лидия обратилась в полицию. Там по факту хищения с банковского счета возбудили уголовное дело по п. «г» ч. 3 ст. 158 Уголовного кодекса РФ, пенсионерку признали потерпевшей. Но мошенников никто не нашел, а кредит так и остался за обманутой пенсионеркой.

На помощь пришли правозащитники томского Центра защиты прав граждан.

Козловых успокоили: с точки зрения закона сделка, совершенная под влиянием существенного заблуждения или обмана, может быть признана недействительной. Об этом говорится в ст. 178 и в п. 2 ст. 179 Гражданского кодекса РФ. Кроме того, в ст. 820 ГК РФ указано, что кредитный договор должен быть заключен в письменной форме, а не онлайн. Специалисты Центра помогли пенсионерке подготовить иск в суд. В иске подчеркнули недобросовестные действия сотрудников банка, которых предупредили о происходящем, но те отказали в содействии и не пресекли мошеннические действия.

Советский районный суд г. Томска признал кредитный договор недействительным и снял с Лидии Козловой обязательства по погашению кредита.

Сообщение от знакомых: «Проголосуйте за племянницу»

От вашего родственника или знакомого приходит сообщение с просьбой проголосовать за талантливого ребенка, который принимает участие в конкурсе (танцевальном, рисунка, хорового пения и т. п.). На кону – путевка в детский лагерь или любое другое поощрение.

К сообщению прикреплена ссылка, по которой надо перейти.

Кликнув на нее, вы окажетесь на сайте, где вас попросят ввести личные данные, пароль, номер карты и так далее. Или предоставите мошенникам доступ к вашей учетной записи. А дальше от вашего имени все ваши коллеги, друзья и знакомые получат сообщения с просьбой дать денег взаймы.

Пример из практики Центров защиты прав граждан

Иван Бочаров чуть не испортил отношения с родственниками из-за взлома учетной записи в WhatsApp.

Получить доступ к учетке Бочарова мошенники смогли благодаря проверенной схеме. От имени родственницы они направили мужчине сообщение с текстом: «Наша племянница участвует в конкурсе. Главный приз – путевка в детский лагерь. Пожалуйста, проголосуй».

И далее – ссылка на страницу с голосованием. Бочаров перешел по ссылке, этим действием подключив к своему профилю в WhatsApp удаленное устройство.

Мошенники тут же разослали от имени Ивана сообщения с просьбой дать взаймы от 5000 до 30 000 рублей.

Как только Иван Бочаров обнаружил, что с его номера идет «ковровая» рассылка, тут же обратился к оператору мобильной связи. Но оператор не помог. Решение нашел мастер одного из центров, оказывающих услуги по установке программного обеспечения.

Спаситель зашел в настройки мессенджера и отключил все синхронизированные с аккаунтом устройства. Также мужчина обратился в полицию, где подал заявление о совершении мошенничества.

ВАЖНО ЗНАТЬ!

Схема «Проголосуй за племянницу» опасна не только тем, что жуликам отправят деньги. Получив доступ к профилю в WhatsApp, мошенники ищут в переписках персональные данные, фотографии паспортов и других документов, с помощью которых могут добраться до карточного счета или оформить на вас кредит.

Если вас взломали в WhatsApp, сделайте следующее:

1. Откройте приложение WhatsApp на своем устройстве.
2. Перейдите в раздел меню «Настройки».
3. Выберите пункт «Связанные устройства».
4. Проверьте список всех устройств, на которых используется ваш аккаунт в WhatsApp.
5. Удалите незнакомые устройства, оставив только те, которым доверяете. А лучше удалите все, нужные потом легко перепривязать.

Если у вас телефон на Android:

WhatsApp: три звездочки в правом верхнем углу → «Настройки» → «Аккаунт» → «Двухшаговая проверка» → «Включить». Придумайте шестизначный пароль (его нужно ввести два раза) и напишите свою электронную почту, чтобы получить новый пароль.

Telegram: «Настройки» → «Облачный пароль» → «Задать пароль». Придумайте пароль и введите его два раза. Дальше программа предложит ввести напоминалку пароля и электронную почту для восстановления учетной записи. На почту придет шестизначный код, введите его в появившемся поле. Готово!

Если у вас IOS:

WhatsApp: «Настройки» (шестеренка в правом нижнем углу) → «Учетная запись» → «Двухшаговая проверка» → «Включить». Придумайте и введите два раза шестизначный код и электронную почту.

Telegram: «Настройки» (шестеренка в правом нижнем углу) → «Конфиденциальность» → «Облачный пароль» → «Задать пароль».

Теперь зайти в ваш профиль с любого другого устройства будет гораздо сложнее.

6. Если мошенники уже взломали аккаунт и разослали сообщения контактам с просьбой одолжить деньги, позвоните каждому и объясните ситуацию.
Скачайте в интернете и поставьте аватарку «меня взломали, никому не отправляйте денег».
Удалите с телефона мессенджер и установите заново.

ЗАПОМИНАЕМ!

- Не переходите по незнакомым ссылкам, даже если очень просят «проголосовать за племянницу».
- Никому никогда не сообщайте приходящие на телефон коды. Особенно если до этого вы никуда не обращались.
- Если знакомые просят денег взаймы, всегда перезванивайте человеку, чтобы убедиться, что не ведете переписку с мошенником.
- Установите в мессенджерах двухфакторную аутентификацию.

Сообщение: «заказ готов к доставке» или «заканчивается срок хранения письма (посылки)»

Злоумышленники копируют профили транспортных компаний или служб доставки, таких как СДЭК, «Яндекс Еда», Delivery Club, «Купер», а также магазинов цветов или других товаров.

Вы получаете звонок или сообщение в WhatsApp, что заказ готов к доставке (либо у вашего заказа истекает срок хранения).

Подробности предлагается узнать, перейдя по ссылке.

Вы ничего не заказывали или не ждете доставку, но решаете проверить, в чем дело. Нажимаете на ссылку, она перенаправляет вас на поддельный сайт, копирующий официальный сервис маркетплейса или службы доставки.

- В некоторых случаях вас просят ввести номер банковской карты, имя пользователя и даже пароль от мобильного приложения банка. Если вводите – открываете доступ мошенникам к своим счетам.

- В некоторых случаях сообщается, что срок бесплатного хранения заказа закончился. Нужно либо отменить заказ, либо доплатить за хранение. Вы нажимаете «Отменить». Для отмены просят ввести код, который вам отправят по СМС.

Мошенник получает доступ либо к Личному кабинету на портале «Госуслуги», либо напрямую к банковскому счету.

Сообщение от начальника: «Будь на связи, сейчас тебе позвонят…»

Взлом корпоративной почты, корпоративных мессенджеров или аккаунтов в соцсетях в последнее время принял массовый характер.

Схема работает так: злоумышленники сначала взламывают почту или мессенджер, а потом жертва (как правило, сотрудник бухгалтерии или финансового отдела) получает сообщение от своего «руково-

дителя» в стиле «Будь на связи, с тобой сейчас свяжется специалист банка / следователь. Окажи содействие, я в курсе».

Звонит «специалист банка (следователь)», после чего жертва следует всем инструкциям от позвонившего. Вплоть до того, что переводит все деньги фирмы на указанный счет или оформляет кредит.

Звонок от потенциального «работодателя»: приглашаем на онлайн-собеседование

Вы ищете работу, разместили анкету и резюме на популярных порталах по поиску работы. Раздается звонок. Вам предлагает работу компания мечты. Условия – невероятные, высокая зарплата, соцпакет, гибкий график. Вы согласны, но специалист предлагает пройти первое собеседование онлайн.

Как правило, звонок производится через мессенджер (WhatsApp или Telegram).

Там же вам присылают ссылку на подключение к программе.

Уже сама ссылка может привести к потере всех персональных данных и опустошению ваших счетов.

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИК ОФОРМИЛ НА ВАС КРЕДИТ

Как только вы узнали о кредите, обратитесь в банк, где был оформлен кредит на ваше имя, с заявлением, что кредит оформлен не вами.

Если заявку еще не одобрили, отменить будет проще.

Но что делать, если кредит был одобрен, мошенник уже вывел кредитные деньги, а заемщиком значитесь вы?

Если банк уже выдал деньги, следует предпринять следующее:

1. Запросите в организации, которая оформила на вас чужой кредит, копию заявки на выдачу кредита и копию паспорта, приложенного к этой заявке. Пусть банк предоставит перечень документов, которыми руководствовался для одобрения кредита.

В каждом банке или МФО есть служба безопасности, которая в таких ситуациях проводит внутреннюю проверку и выясняет все обстоятельства.

2. Возьмите копии этих документов и отправляйтесь в полицию.

Кража денег – уголовное преступление. Полиция обязана принять от вас такое заявление, установить лиц, которые от вашего имени заключили договор займа, и владельцев банковских карт, куда были перечислены заемные деньги.

После того как в полиции примут ваше заявление о мошенничестве с оформлением кредитных средств, вам выдадут на руки талон, который подтверждает факт обращения и регистрации вашего заявления в полиции. Он называется талон-уведомление.

3. С талоном-уведомлением возвращайтесь в банк (или МФО) и пишите заявление о мошенничестве с требованием к кредитной организации аннулировать кредитный договор и снять с вас все обязательства по погашению кредита.

Форму заявления вам выдадут в банке (МФО). В заявлении подробно опишите ситуацию и приведите доказательства того, что вы не обращались за кредитом (чужая подпись в договоре, вход в Личный кабинет выполнен из места, не совпадающего с вашим IP-адресом, и т. п.), и потребуйте аннулировать на этом основании кредитный договор.

4. Приложите к заявлению в банк (или МФО) талон – уведомление из полиции. При наличии – иные доказательства.

Заявление подайте в двух экземплярах. На экземпляре, который останется у вас, поставьте отметку о дате и времени регистрации заявления у банковского работника. Это нужно для того, чтобы у вас были доказательства, что банк такое заявление принял.

Как правило, если подтвердится факт мошенничества при оформлении онлайн-кредита, финансовая организация идет клиенту навстречу и помогает ему аннулировать кредитный договор.

Банк обязан провести служебное расследование. Если мошенники действовали на территории России, расследование займет 30 дней, если операция была международной – 60 дней.

По итогам расследования с вами свяжется сотрудник банка и сообщит о решении. Если банк убедится, что вы стали жертвой мошенников, кредитные обязательства будут аннулированы.

Если служба безопасности банка провела внутреннее расследование и убеждена, что вы выразили свое согласие на оформление займа, придется обратиться за помощью:

– в Центробанк – если мошенники взяли кредит в банке;

– к финансовому уполномоченному – если мошенники оформили кредит в МФО.

Можно сразу обратиться в суд с иском о признании кредитного договора недействительным.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАМ «СЛУЧАЙНО ПЕРЕВЕЛИ ДЕНЬГИ»

В последнее время набирает обороты схема случайно переведенных на ваш счет денег. Якобы по рассеянности гражданин отправил деньги не туда и просит вас их вернуть.

Схема работает так: вы получаете СМС о зачислении средств на счет. СМС внешне напоминает банковское уведомление. Затем (практически сразу же) вам перезванивает отправитель перевода и просит вернуть ошибочный перевод ему на карту.

Как быть? Бывает же, человек мог ошибиться в одной цифре телефона или номере счета. Но не спешите возвращать деньги. Убедитесь, что это не мошенник!

В таких ситуациях необходимо:

1. Проверить, от кого пришло сообщение. Возможно, что вы получили СМС вовсе не от банка.

Дело в том, что мошенники научились подделывать короткие номера банков и внешне СМС будет даже напоминать официальное уведомление от вашего банка. Однако посмотрите внимательно. Сообщение входит в перечень всех уведомлений от вашего банка или пришло отдельно?

Сообщение содержит полную информацию, где помимо суммы, даты, последних цифр карты зачисления значатся такие сведения, как баланс карты с учетом полученных средств?

2. Убедиться, что на ваш счет действительно зачислены деньги. Возможно, никаких зачислений не произошло.

- Если у вас есть мобильное приложение банка на телефоне, вы можете туда зайти, посмотреть историю операций и изучить подробности последней операции по зачислению.
- Если у вас нет мобильного приложения, перезвоните в банк (только по официальному номеру горячей линии банка) и уточните, поступил ли вам перевод (дата, время, сумма) и кто отправитель.

В свою очередь, чтобы убедиться, что звонит держатель карты, сотрудник банка уточнит ваши ФИО и паспортные данные. Кроме того, сотрудник может запросить у вас:

- последние четыре цифры номера вашей карты.
  Внимание: это цифры на лицевой стороне карты (где 16-значный номер карты).
  Нужно назвать последние четыре цифры;
- кодовое слово. Когда вы подписывали договор с банком, вы его придумывали для подобных ситуаций.

3. Помнить: даже если это действительно перевод (и перевод сделан по ошибке), отправленный перевод имеет период охлаждения.

Отправитель может его отозвать. И вот тогда уже банк попросит вас вернуть случайно «присвоенные» деньги.

Если столкнетесь с такой операцией, подстрахуйтесь, сопроводите перевод коротким сообщением: «Возвращаю».

Сделайте фото или скрин операции по возврату средств. Чтобы в случае, если на вас поступит жалоба в банк о присвоении чужих средств, у вас были доказательства, что вы вернули чужие деньги.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЗЛОМАЛИ «ГОСУСЛУГИ»

Взлом аккаунта на портале «Госуслуги» предоставляет мошеннику широкое поле для деятельности.

Ведь он получает доступ абсолютно ко всем вашим данным. Может перепривязать ваши банковские карты к своему телефону, взять на вас кредит, продать все ваши данные в Сеть, загрузить поддельную нотариальную доверенность на распоряжение всем вашим имуществом.

Что предпринять, если вы все же назвали мошеннику ПИН-код, открыв доступ к учетной записи на «Госуслугах»

Если мошенники НЕ УСПЕЛИ ПОМЕНЯТЬ ДАННЫЕ ДЛЯ ВХОДА

И у вас еще есть доступ к телефону и почте, которые были указаны при авторизации.

СПОСОБ № 1: оперативно сделать это самостоятельно на портале

1. Нажмите кнопку «Восстановить» на странице авторизации. Затем укажите номер телефона или адрес почты, а также данные паспорта, ИНН или СНИЛС.

2. Перейдите по ссылке из письма или введите код из СМС. После этого вам предложат придумать новый пароль. Установите новый пароль.

3. Попав в Личный кабинет, первым делом проверьте, какие подозрительные действия зафиксировала система после взлома аккаунта.

Для этого в профиле перейдите в раздел «Безопасность». А затем последовательно пересмотрите вкладки:

- «Вход в систему» (когда, с какого устройства и IP-адреса входили);
- «Действия в системе» (что делали);
- «Мобильные приложения» (с каких гаджетов);
- «Межведомственные запросы» (куда были сделаны, когда и с какой целью выдано разрешение на доступ к вашим персональным данным).

4. Отключите вход от всех устройств, которые вам не принадлежат. Выйдите из всех приложений, куда вы не заходили. Отзовите все разрешения на использование ваших персональных данных, которые не вы выдали ведомствам и организациям.

Даже если ничего подозрительного не видите, обязательно запросите свою кредитную историю. Два раза в год это можно сделать абсолютно бесплатно.

Если окажется, что кто-то взял кредит или заем от вашего имени, сразу обратитесь в банк или МФО, которые выдали кредит, а также в полицию.

Дополнительно защитить свой аккаунт от взлома
Заказать кредитную историю
Установить самозапрет на кредиты на портале «Госуслуги»

Подробнее – на ***справедливо-центр.рф*** *в разделе* ***ФИНАНСЫ***

СПОСОБ №2: восстановить онлайн через приложение своего банка

Банк подтвердит вашу личность по тем данным, которые есть у него в системе. Пароль для первого входа на «Госуслуги» придет в СМС по указанному в банке номеру телефона.

Если мошенники СМЕНИЛИ ДАННЫЕ ДЛЯ ВХОДА

Аккаунт необходимо удалить и создать новую учетную запись.

1. Сразу обратитесь в сервисный центр «Госуслуг» (в МФЦ) с просьбой удалить взломанный аккаунт и создать новую учетную запись. Понадобятся паспорт и СНИЛС. После восстановления или регистрации новой учетной записи обязательно установите дополнительные средства защиты.

2. Уведомите о случившемся техподдержку «Госуслуг» и полицию. Передайте все известные вам подробности: время взлома, чужие контактные данные, которые появились в аккаунте вместо ваших. Сохраните копию заявления в полицию и талон – уведомление о его приеме. Если мошенники наберут долгов на ваше имя, будет проще доказать, что займы брали не вы.

3. Обязательно закажите кредитную историю – данные обо всех кредитах и займах на ваше имя. Так вы быстро узнаете, что мошенникам все-таки удалось взять кредиты на ваше имя, и сможете их оспорить.

4. Задайте сложный пароль для доступа к аккаунту на «Госуслугах» и поставьте дополнительную защиту аккаунта.

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

СПРАВЕДЛИВОЕ РАДИО

Радиостанция Центров на сайте
справедливоерадио.рф

RUTUBE

Канал
«Центр справедливости»

ДОМОВОЙ СОВЕТ

Газета «Домовой совет»
домовой-совет.рф

Телефон горячей линии
8 800 755 55 77

Сайт Фонда
«Центр защиты прав граждан»
справедливо-центр.рф

Пособие: МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Изготовитель: ООО «Имидж», 143306, МО, Наро-Фоминский район,
г. Наро-Фоминск, ул. Ленина, д. 28, офис 1, этаж 1
Заказчик: Фонд «Центр защиты прав граждан», ИНН 9710010183.
Тираж: 10 000 экз. Заказ 682. 2025 год.
Распространяется бесплатно

В ТРУДНОЕ ВРЕМЯ РЯДОМ С ТОБОЙ!