Банк России

ЗНАНИЕ – СИЛА: ЗАЩИТИ СЕБЯ И БЛИЗКИХ ОТ МОШЕННИЧЕСТВА НА ФИНАНСОВЫХ РЫНКАХ

Мошенничество в разных сферах нашей жизни присутствовало всегда, и сегодня оно приобретает новые формы, что во многом обусловлено появлением и развитием финансовых технологий. Как защититься от угроз современного финансового рынка, как распознать их и что они из себя представляют — вот основные вопросы, которые предлагается рассмотреть ниже.

Взяв за принцип известное латинское изречение «Praemonitus, praemunitus» («Предупрежден, значит, вооружен»), вооружимся знаниями по финансовой грамотности и таким образом не только оставим мошенников ни с чем, но и научим, как не попасться к ним на удочку, своих родных, друзей и знакомых.

Чаще всего мошенники обнаруживают себя в момент нашего взаимодействия с банкоматом, при совершении покупок, оплаты услуг в интернете, при получении фишинговых рассылок или в более сложных ситуациях — когда происходит утечка конфиденциальной информации, например из-за незащищенного соединения в сети.

Рассмотрим наиболее распространенные мошеннические схемы и выявим правила безопасного финансового поведения.

БАНКОМАТ: ПРАВИЛА ОСТОРОЖНОГО ИСПОЛЬЗОВАНИЯ

Банкоматы бывают адаптированными (доступными) и неадаптированными. Адаптированный (доступный) банкомат — это устройство для обслуживания людей с инвалидностью или ограничениями по здоровью. Такие банкоматы могут отличаться размерами, наличием особого программного обеспечения или, например, специальным аудиоразъемом, в момент использования которого банкомат переходит в специальный режим для работы с незрячими держателями карт.

Однако такие банкоматы расположены не везде. С одной стороны, адаптированный банкомат — это необходимость, и попытки найти его для совершения операций понятны и оправданы. С другой стороны, нельзя забывать о безопасности, ведь расположение банкомата имеет очень важное значение. Например, для незрячего клиента выбор между доступным банкоматом, находящимся на улице, и неадаптированным в офисе банка — неоднозначен. Нельзя забывать, что использовать банкомат на улице более рискованно, чем в офисе банка. Если банкомат не адаптирован — попросите помочь вам сотрудника банка, полицейского, другое должностное лицо или знакомого, которому вы доверяете.

При использовании банкомата не забывайте и о других правилах безопасности. Помните, что ПИН-код необходимо держать в тайне, его никогда нельзя сообщать третьим лицам, и поэтому безопаснее использовать те банкоматы, расположение которых не позволяет посторонним людям находиться рядом с вами. При вводе ПИН-кода всегда прикрывайте клавиатуру рукой. Клавиатура банкомата оснащена тактильными метками, что позволяет незрячим пользователям вводить ПИН-код без посторонней помощи. Такие метки чаще всего представляют собой выступы на кнопках, соответствующих цифре 5, клавишам ввода, коррекции и отмены. В некоторых случаях на клавиатуру банкомата наносится шрифт Брайля.

Транзакции, подтвержденные ПИН-кодом, оспорить очень трудно, поскольку по условиям договора, заключаемого с банком при получении платежной карты, ПИН-код не должен знать никто, кроме владельца карты. Если вам нужно снять наличные, но вы испытываете затруднения, не передавайте свою карту и ПИН-код к ней третьим лицам, лучше переведите нужную сумму на карту тому, кому вы доверяете и кто готов вам помочь, попросив этого человека снять для вас наличные. При обращении за помощью соблюдайте осторожность, не прибегайте к услугам, если вам предложили их без вашей просьбы непосредственно у банкомата. Возможно это обычные неравнодушные граждане, но для обеспечения собственной безопасности лучше от такой помощи отказаться.

Будьте внимательны при завершении операций с банкоматом — по окончании операции можно услышать характерный щелчок, свидетельствующий о том, что банкомат вернул вам карту, — заберите карту сразу же, как услышите его, иначе через 30-40 секунд банкомат в целях безопасности захватит карту обратно. Деньги, выдаваемые банкоматом через презентер (отверстие для выдачи наличных), тоже будут доступны в среднем около 30 секунд, по истечении которых банкомат заберет банкноты обратно в так называемую реджект-кассету, которую вынимают из банкомата только при инкассации. Процесс возврата денег может растянуться на несколько дней. В случае, если вы попали в такую ситуацию, немедленно позвоните или лично обратитесь в банк, изложите суть своей проблемы и следуйте инструкциям оператора. Скорее всего, вас попросят написать заявление: от руки или в системе мобильного/интернетбанка. Не переживайте: карту вам если и не вернут, то перевыпустят, а деньги зачислят на счет вскоре после инкассации и пересчета наличных в банкомате.

Случается, что банкомат, издав характерные звуки, не выдает наличных. Обычно так бывает, если в банкомате закончились деньги вообще или купюры необходимого достоинства. В этом случае деньги не списываются со счета. Если же вы получили СМС-сообщение о списании средств, то, как правило, через несколько секунд вам придет сообщение об отмене операции и деньги вернутся на ваш счет.

Однако существует и другая причина, и связана она с мошенническими операциями. В этом случае злоумышленники блокируют окно выдачи денег (диспенсер) с помощью скотча или различных вилок/рогатин. Банкомат может решить, что деньги вам уже выданы и списать их со счета. Такая ситуация встречается редко, но если вы с ней столкнулись — немедленно звоните в банк и следуйте советам оператора.

ОПЛАТА ТОВАРОВ И УСЛУГ ЧЕРЕЗ ИНТЕРНЕТ ИЛИ ДРУГИЕ ДИСТАНЦИОННЫЕ КАНАЛЫ

Если при использовании банкомата или оплате покупок в торговых точках необходима карта или иное бесконтактное устройство платежа (брелок, браслет, телефон), то при дистанционном проведении операций используются данные платежной карты или другого бесконтактного устройства, в связи с чем возникают определенные риски, которых можно избежать или существенно снизить, если следовать правилам безопасности.

Для того чтобы лучше разобраться в них, ответим на вопрос: какие данные платежных карт используются при дистанционной оплате?

Прежде всего это номер карты — от 16 до 19 цифр, срок окончания действия карты и проверочный код (CVC или CVV) — три цифры на обратной стороне карты, расположенные справа от поля для подписи. Как правило, этот код необходим для подтверждения платежа и именно поэтому мошенники пытаются всеми способами узнать его у вас. Причем если номер карты может сохраняться у продавца, то данный код — нет. Помните, что CVV или CVC-код никогда нельзя передавать/называть третьим лицам, никто не имеет права потребовать от вас назвать его, отправить письмом или сообщением. Если же это произошло, значит, вы имеете дело с мошенниками.

Кроме обозначенных реквизитов, многие интернет-магазины запрашивают имя держателя. Эта информация используется исключительно на стороне магазина и по каналам платежной системы от продавца к эмитенту карты не передается. Компания-продавец запрашивает ее в целях собственной безопасности на случай претензий со стороны покупателя. Если система запрашивает ввод имени держателя для оплаты покупки — напишите его, вам это ничем не грозит.

Рост мошенничества в виртуальной области вынудил платежные системы добавить еще одну степень защиты в процесс совершения платежей через интернет, а именно одноразовый пароль (так называемая технология 3DSecure). Такой пароль может быть получен различными способами:

- с помощью скретч-карты — специальной карты со счищаемым слоем;
- с помощью кода, рассчитанного специальным устройством;

- а в подавляющем большинстве случаев с помощью СМС или PUSH-сообщений — одноразовых паролей, направляемых вам банком-эмитентом карты.

Такой пароль необходимо ввести в специальном окне при покупке или совершении платежа через интернет. Так же как ПИН-код, CVV или CVC-код, его нельзя никому и никогда сообщать, поскольку при нормальной процедуре платежа он требуется только для проведения платежа через интернет. Никакие сотрудники банка, Банка России, полиции, любых других организаций и тем более частные лица не имеют права требовать от вас информацию об одноразовых кодах и паролях для подтверждения платежа.

Иногда совершенная вами транзакция может вызвать вопросы у сотрудников службы безопасности банка. В этом случае вам могут позвонить и попросить уточнить информацию о последних проведенных вами операциях по карте. Однако никогда и ни при каких обстоятельствах они не должны просить вас предоставить такую информацию, как номер карты, срок ее действия или тем более CVV или CVC-код и/или одноразовый пароль. Если кто-то под видом сотрудника банка пытается узнать у вас эти сведения, немедленно завершите разговор — вы имеете дело с мошенником.

Важно соблюдать главный принцип: все, что пришло по СМС, предназначено только для вас, и никакие люди по телефону не могут интересоваться этими цифрами. Если кто-то просит вас назвать код или другую секретную информацию, высылаемую вам банком в СМС-сообщении, такие люди — однозначно мошенники.

ФИШИНГ

Фишинг (англ. phishing, от сходного по звучанию английского слова fishing — рыбалка) — один из видов интернет-мошенничества, своеобразная «ловля на живца» с помощью массовых рассылок СМС-сообщений и сообщений по электронной почте якобы от имени популярных компаний или организаций, банков, Банка России и так далее, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих. Целью данного вида мошенничества является получение ваших конфиденциальных данных: логинов, паролей, данных лицевых счетов и банковских карт, ваших документов, одноразовых паролей, получаемых по СМС, ПИН-кодов к картам, CVV или CVC-кодов и другой информации, относящейся к вам и вашим финансам.

Обычно фишинговые рассылки маскируются под сообщения от имени вашего банка, популярных организаций или известных компаний. В текстах таких писем обычно содержится информация о блокировке карты, переводе или зачислении средств, выигрыше в лотерею, а также просьбы обновить или подтвердить верность персональных данных из-за каких-либо проблем

с ними. При письменном или устном общении злоумышленники запрашивают определенные данные либо предлагают пройти по ссылке на страницу фальшивого сайта, внешне неотличимого от настоящего, где просят жертву ввести необходимые им персональные данные. Получение подобной информации злоумышленниками может привести к краже персональных данных или списанию средств с карты.

Для того чтобы не стать жертвой фишинговой атаки, необходимо следовать принципам безопасного поведения в интернете:

- не переходить по ссылкам, присланным в подозрительных или непонятных СМС-сообщениях, сообщениях электронной почты, социальных сетей;
- не загружать вложенные файлы из сообщений, которых вы не ожидали;
- обеспечить надежной защитой свои пароли и никому их не передавать;
- не сообщать никому свои персональные данные — ни по телефону, ни лично, ни в каких-либо сообщениях;
- внимательно проанализировать адрес сайта (URL), на который осуществляется переадресация. Несмотря на то что сайт мошенников часто выглядит очень похожим на настоящий, его URL-адрес в большинстве случаев отличается от оригинального (например, заканчиваться на .com вместо .ru);
- не звонить по телефонам, указанным в подозрительном сообщении. Если у вас есть сомнения — перезвоните в свой банк по телефонам, которые приведены на вашей карте или на сайте банка;
- поддерживайте свой браузер обновленным и своевременно устанавливайте обновления безопасности и антивирусные программы.

ФИНАНСОВАЯ ПИРАМИДА

Финансовая или инвестиционная пирамида — это система обеспечения дохода более ранним инвесторам путем постоянного привлечения денежных средств новых участников. Основатели финансовой пирамиды обещают инвесторам сверхвысокую доходность, однако поддерживать такой уровень доходности длительное время невозможно, особенно при том, что реальной хозяйственно-инвестиционной деятельности пирамида, как правило, не ведет. Это означает, что погашение обязательств перед всеми участниками пирамиды заведомо невыполнимо.

Принципиальным отличием финансовой пирамиды от реального бизнес-проекта является источник выплаты дохода. Если сумма выплат дохода стабильно превышает размер добавленной стоимости, которую обеспечивает данный бизнес, то можно смело говорить о том, что проект является финансовой пирамидой.

Зачастую финансовые пирамиды регистрируются как некие организации, привлекающие средства для финансирования какого-нибудь проекта. В случае если его реальная доходность оказывается ниже обещанных инвесторам доходов или отсутствует вообще, то часть средств, поступивших от новых инвесторов, направляется на выплату дохода. Закономерным итогом такой ситуации является банкротство проекта и убытки последних инвесторов. Собранные средства направляются не на покупку ликвидных высокодоходных активов или развитие бизнеса, а сразу используются для выплат предыдущим участникам, оплату рекламы и дохода организаторов. Чем дольше функционирует пирамида, тем меньше процент возможного возврата средств при ее ликвидации.

МОШЕННИКИ НА ТОРГОВЫХ ОНЛАЙН-ПЛОЩАДКАХ

Сегодня все большей популярностью пользуются различные торговые онлайн-площадки, на которых в том числе и частные лица могут продать или купить как новые, так и бывшие в употреблении товары, а также различные услуги. Такие площадки представляют особый интерес для мошенников. Популярность мошенничества в этой системе объясняется большим количеством пользователей, которые размещают свои объявления.

На этих площадках мошенники работают в основном по нескольким схемам, среди которых можно выделить следующие:

- **Пересылка товара с предоплатой.** Зачастую процесс купли-продажи на сайте проходит между лицами из разных городов. Перед отправкой товара покупатель и продавец договариваются об условиях пересылки необходимого товара. Мошенники же действуют следующим образом: продавец отказывается встречаться с покупателем на удобной территории и требует предоплату за пересылку товара или говорит, что у него есть несколько покупателей и он отдаст товар в случае немедленной предоплаты в размере, например, 10% от суммы на его карту. Покупатель переводит необходимую сумму и остается ни с чем, так как мошенник пропадает и перестает выходить на связь. Поэтому если продавец начинает требовать заплатить ему частичную или полную стоимость товара, игнорируйте это требование, а при настойчивом вымогательстве прекращайте любые контакты. Подобные ситуации легко узнаваемы и, к сожалению, возникают часто. Старайтесь в них не попадать, так как те, кто все же совершит предоплату и не получит обещанный товар, потеряет деньги навсегда.
- **Требование ответить по СМС.** Очень часто мошенники отправляют с неизвестного номера СМС-сообщения различного содержания.

Например, о блокировке объявления за нарушение правил, о наличии откликов на размещенное объявление, просьбы прислать СМС с кодом для отмены блокировки и другие. Таким образом, злоумышленники вынуждают отправить СМС, за которое с вас могут списать крупную сумму. Для уверенности в правомерности подобных требований необходимо обратиться в службу поддержки используемого сайта. Обратите внимание, что некоторые мобильные операторы предоставляют услугу открытия отдельного счета для оплаты различных сервисов, подключение которых снижает риск потерь.

- **Работа с предоплатой.** Одним из распространенных случаев мошенничества является просьба о предоплате за услуги по устройству на работу. Мошенники просят внести определенный взнос за заключение договора, оформление документации, пропуск на территорию, обучающие материалы и так далее. Получив деньги, злоумышленники, естественно, исчезают. Помните! Ни одна организация не берет денег у будущих работников ни до их устройства на работу, ни после. Если вы столкнулись с такими просьбами — скорее всего, вы имеете дело с мошенниками.
- **Передача персональных данных.** Недобросовестные продавцы/покупатели под различными предлогами могут пытаться узнать у вас личные данные, например номер банковской карты и ее ПИН-код, CVV или CVC-код, даже одноразовый СМС-пароль для подтверждения оплаты. Разглашение данной информации третьим лицам может угрожать вашей личной и финансовой безопасности. Если вы хотите быть уверены в защите личных данных и денежных средств, держите сведения о них при себе.

«НИГЕРИЙСКИЕ» ПИСЬМА

«Нигерийские» письма — особый вид высокоорганизованного мошенничества, появившийся почти 40 лет назад и получивший наибольшее распространение с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что широкое распространение данный вид мошенничества получил в Нигерии, причем еще до появления интернета — в то время мошенники действовали с помощью обычной почты. Сегодня «нигерийские» письма можно получить и из других африканских стран, а также из Англии, Голландии, Испании, ОАЭ, США и даже России. Мошенники, как правило, просят у получателя письма помощи в совершении многомиллионных денежных операций, обещая за нее солидные проценты. Это могут быть, например, различные дела по получению адресатом наследства, или просьбы помочь с банковским переводом за границу, или предложения о получении денег с банковского счета умершего клиента, который

по какому-то чудесному совпадению является однофамильцем адресата. Если получатель письма соглашается помочь, у него постепенно выманиваются крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, а потом и штрафы.

Проблема состоит в том, что в данном случае у мошенников все продумано до мелочей: у них есть офисы, работающий факс, собственные сайты, связи с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде.

Несмотря на то что на протяжении многих лет в средствах массовой информации подробно рассказывается о данном виде мошенничества, массовость рассылки приводит к тому, что злоумышленники находят все новые и новые жертвы, которые отдают им крупные суммы денег.

В целом можно выделить общие особенности «нигерийских» писем и любого мошенничества, связанного с выманиванием денег. Во-первых, почти в каждом случае есть ощущение, что все надо делать «срочнейшим образом». Упоминаются форс-мажорные обстоятельства, а в теме письма пишут «срочно, очень срочно». Во-вторых, в большинстве случаев корреспонденция отправляется по факсу или через электронную почту. В-третьих, злоумышленники используют различные ссылки на разного рода документы, печатные издания, законодательные акты, призванные вызвать доверие жертвы. В-четвертых, всячески подчеркивается элитарность, эксклюзивность предлагаемой схемы. Предложение исходит якобы от высокопоставленных чиновников, вдов политических лидеров, различных наследников и так далее. Говорится, что вас как человека очень надежного и честного рекомендовал один ваш знакомый, пожелавший остаться неизвестным. В письмах практически всегда фигурируют большие суммы денег: от 10 до 80 млн $ США. Получателю предлагается сотрудничать за крупный процент (до 30% от общей суммы). Наконец, мошенники акцентируют внимание жертвы на конфиденциальном характере сделки, не скрывая ее нелегитимности. Все это нужно для того, чтобы после успешной аферы пострадавший не побежал жаловаться в полицию из-за страха быть уличенным в незаконных операциях.

Лучший способ избежать неприятностей, связанных с последствиями общения и взаимодействия с подобными мошенниками, — игнорировать их письма, немедленно удаляя без ответа.

ПСЕВДОБРОКЕРЫ И ПСЕВДОДИЛЕРЫ

Мошенники регулярно предлагают клиентам брокерские или дилерские услуги, с помощью которых якобы можно приумножить свой капитал и осуществить высокодоходные инвестиции, не имея при этом никакого отноше-

ния к реальным брокерам и дилерам, а также лицензии на осуществление такой деятельности. Их цель — вынудить клиента перевести им денежные средства.

К основным приемам мошенников можно отнести:

- **Вывод денег через повышение торгового статуса**. Например, клиент зарегистрировался на сайте торговой площадки по бинарным опционам, пополнил свой баланс и получил уведомление о получении «бонусных доходов». Однако для вывода этих денег к нему предъявляют требование о повышении своего торгового статуса, а именно просят внести дополнительную сумму. В итоге клиент вносит все больше и больше средств, но так и не получает возможности вывести свои деньги. Из реальной же брокерской или дилерской компании клиент всегда может вывести свои свободные денежные средства без каких-либо дополнительных вложений.
- **Просьба перевести деньги на карту (или электронный кошелек) третьему лицу.** Запомните, что реальные брокерские или дилерские компании не просят перевести средства на карту третьего лица. Если вы выполните такой перевод, отозвать средства будет уже невозможно.
- **Договор участия в лотерее или договор-пари.** Клиент невнимательно читает договор, который подписывает с якобы брокерской компанией, и когда он пытается получить свои деньги, компания отказывается их вернуть, ссылаясь на договор, где указано, что клиент участвовал в лотерее или пари, причем чаще всего эта информация прописывается мелким шрифтом. Получается, что клиенту «просто не повезло» и он проиграл свои деньги. Для того чтобы избежать такой ситуации, внимательно читайте договоры, которые вы подписываете. При любых сомнениях берите время на более детальное изучение документов и по возможности знакомьтесь с ними в спокойной домашней обстановке, прибегая при необходимости к консультации юриста.

Помните, если деньги переведены в компанию, зарегистрированную на территории другого государства, то споры придется решать в его правовом поле, то есть в другой стране, так как российские законы на эти компании не распространяются. Если случалось так, что вы все-таки перевели деньги на счет компании злоумышленников, банк сможет вернуть их только в случае согласия компании, на что рассчитывать не приходится.

Для того чтобы избежать встречи с мошенниками подобного типа, убедитесь, что у выбранной вами компании есть лицензия на осуществление брокерской или дилерской деятельности. Перечень российских компаний, у которых есть соответствующая лицензия, представлен в Справочнике участников финансового рынка на сайте Банка России. Кроме того, постарайтесь найти отзывы на профильных сайтах/форумах о нужной вам компании и разузнать о реальном опыте взаимодействия с ней.

ОПРОСЫ, КОНКУРСЫ, РАСПРОДАЖИ

Довольно часто в СМС-сообщениях, электронных письмах можно получить предложения пройти опрос/анкетирование с обещанием получить за это гарантированный приз. При ответе на такое сообщение или даже звонок мошенники долго рассказывают о компании, опросе, награде, а потом предлагают клиенту подтвердить свою личность, гражданство, место жительства, предоставив для получения приза определенную личную информацию: чаще всего данные банковской карты. Подвох состоит в том, что злоумышленники под разными предлогами настаивают на списании с карты небольшой денежной суммы, похищая при этом все имеющиеся на ней средства. В другом варианте мошенники просят перевести денежные средства на другую карту в целях подтверждения ее наличия у жертвы или осуществить гарантированный платеж для резервирования товара.

Для того чтобы не стать жертвами таких псевдорозыгрышей, необходимо помнить о том, что настоящие компании, проводящие опросы, не просят перевести им предварительно денежные средства. Любой платеж незнакомой компании или человеку должен быть обоснован.

РАБОТА В СЕТИ И МОШЕННИЧЕСТВО С ДОСТАВКОЙ НА ДОМ

В интернете, а также в различных рассылках можно получить предложения удаленной работы с возможностью высокого заработка. Как правило, в описании вакансии особо подчеркивается, что соискателю не требуются специфические знания, он должен будет пройти обучение, для чего ему надо приобрести специальные материалы либо получить базу данных клиентов. Для этого необходимо немного заплатить за почтовые расходы, подготовку базы данных, обучение или что-то еще и только после этого приступать к работе. Естественно, что после перевода денежных средств мошенники исчезают.

Другой распространенный вариант такого мошенничества можно встретить офлайн. Например, известная фирма расширяет свою сеть и нанимает сотрудников (можно с инвалидностью) для работы на домашнем телефоне. К кандидату приезжает «представитель фирмы» и проводит экзамен, который проходят абсолютно все кандидаты. Перед отъездом он оставляет у соискателя какие-либо вещи: набор образцов продукции, инструкции для общения с клиентами, телефонные справочники и получает за них залог — обычно порядка 1000-5000 рублей. После чего исчезает навсегда.

Настоящие работодатели перед трудоустройством не требуют пройти платное обучение, купить их продукцию, оплатить трудоустройство.

Прежде чем начинать общение с любым работодателем, зайдите на сайт его компании, ознакомьтесь с отзывами о ней, соберите информацию о реальном опыте взаимодействия с этой компанией, используя профильные сайты и/или форумы.

Случается, что злоумышленники маскируются под социальных работников и, приходя под их видом в дом, начинают рассказывать о новом лекарстве для пенсионеров по льготной цене или приборе, улучшающем, скажем, работу сердца. Конечно, его можно приобрести в районном центре социальной защиты, но тогда придется долго ждать, а вам повезло, и вы сейчас же его получите со скидкой 90%, говорят они. Как правило, предлагаемый мошенниками товар не сто́ит запрашиваемых за него денег, зачастую человека склоняют к заключению кредитного договора или даже обворовывают.

Для того чтобы не стать жертвой подобных мошеннических схем, необходимо помнить, что быстрый заработок, легкие большие деньги, ставки по вкладам в 10 раз больше, чем у любого банка, работа без образования и навыков, опросы, лотереи, дешевые лекарства и товары, оказавшиеся внезапно на пороге вашего дома, — очень часто становятся приманками для доверчивых граждан. Не теряйте бдительности и не спешите расставаться с деньгами!

ЗАКЛЮЧЕНИЕ

В заключение, еще раз обратим внимание на правила финансовой безопасности, которые помогут вам защититься от действий мошенников на финансовом рынке.

При совершении любой операции с картой или денежными средствами продумывайте свои действия и учитывайте возможные действия мошенников. Не оставляйте карту без присмотра, не передавайте ее никому и тем более не сообщайте ПИН-код, одноразовые пароли и другую информацию, получаемую вами от банка по телефону, в СМС-сообщениях или по электронной почте, даже своим близким родственникам, не говоря уже о друзьях, знакомых и прочих третьих лицах. Помните, что сотрудник банка не имеет права спрашивать ни номер вашей карты, ни тем более ПИН-код или пароли, пришедшие в СМС-сообщениях. При любых проблемах с картой, сомнениях или подозрениях в ее компрометации срочно связывайтесь с банком-эмитентом по телефонам, указанным на обороте карты или на сайте нужной кредитной организации. Используйте банкоматы, установленные в безопасных местах. Не пренебрегайте компьютерной безопасностью: установите антивирус, не открывайте файлы, ссылки из незнакомых источников.

Осмотрительно используйте публичный Wi-Fi. Не передавайте конфиденциальную информацию (пароли, банковские данные и так далее), по возможности используйте виртуальные частные сети (VPN), подключайтесь только

к тем сайтам, которые используют безопасный протокол (это можно увидеть по наличию https в начале названия сайта в адресной строке браузера).

Обращайте внимание на сообщения браузера о безопасности. Скачивайте только необходимые приложения из известных источников. Официальные интернет-магазины принимают определенные меры для предотвращения распространения вредоносных программ (хотя и не всегда успешно), и вы можете проверить отзывы других пользователей, прежде чем решите установить приложение или если заметите что-то подозрительное. Если вы скачиваете приложение с неофициального сайта и устанавливаете его на свое устройство, вероятность того, что приложение может содержать вредоносные программы, значительно возрастает.

С осторожностью подходите к любым финансовым сервисам, требующим ввода данных вашей карты, счета, персональных данных, адресов, телефонов, особенно если это связано с каким-то выигрышем, промоакциями и прочим.

По вопросам финансовой грамотности:

fingramota@cbr.ru

Сайт Банка России по финансовой грамотности:

fincult.info

Контактный центр Банка России:

8 800 300-30-00

(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:

cbr.ru/reception

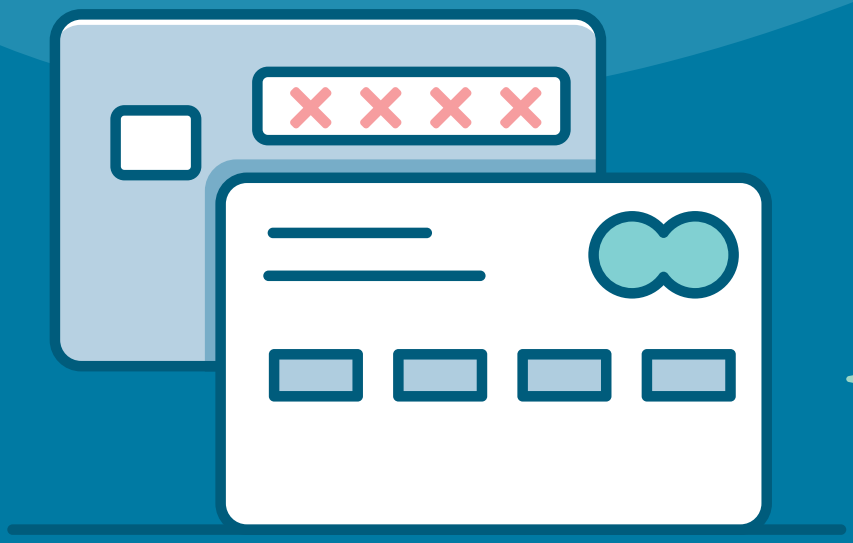
Банк России

BEST BUDDIES
ЛУЧШИЕ ДРУЗЬЯ

РООИ ПЕРСПЕКТИВА
ОТКРЫВАЕМ НОВЫЕ ВОЗМОЖНОСТИ

Как безопасно использовать банковскую карту

Пособие для людей с ментальными особенностями



Данный материал представляет собой описание банковских карт и безналичных переводов, а также базовых принципов их безопасного использования для людей с ментальными особенностями.

На примере этого текста можно понять принципы изложения в облегченном формате (Easy-to-read) информации о финансовых продуктах и услугах людям с легкими формами расстройств аутистического спектра, сниженным интеллектом, другими особенностями восприятия.

Материал адаптировали сотрудники РООИ «Перспектива», которые обладают многолетним опытом обучения людей с ментальными особенностями.

Банковская карта

Люди могут покупать и продавать разные вещи.

Например, продукты в магазине или билеты в кино.

Люди могут продавать и покупать с помощью денег.

Можно это делать несколькими способами.

Например, платить наличными деньгами
или с помощью банковской карты.

Наличные деньги можно потрогать.

Наличные деньги могут быть в виде купюр или монет.

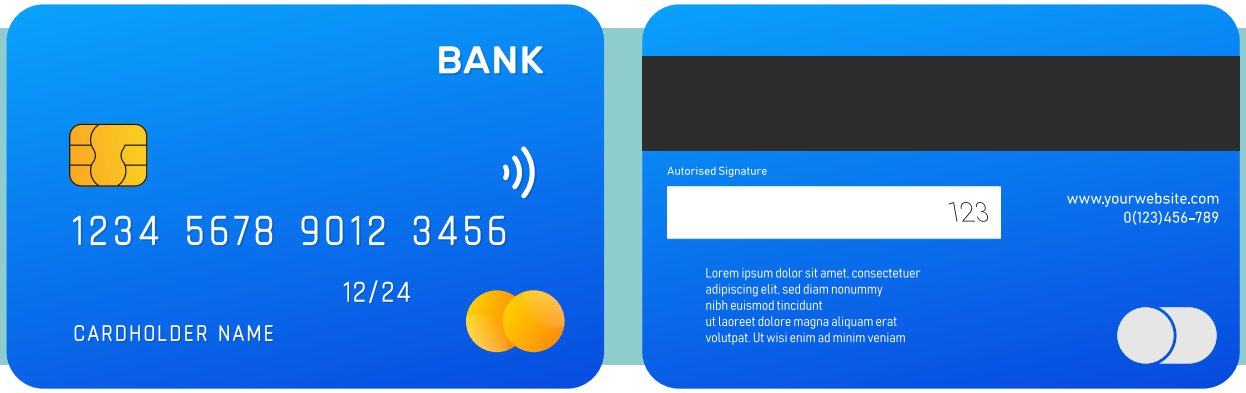
Лицевая сторона

Оборотная сторона

Так выглядит купюра в 100 рублей

Так выглядят монеты в 1, 2, 5 и 10 рублей

Деньги могут лежать на банковской карте.



Так выглядит банковская карта

На банковской карте написано название банка.

Номер телефона банка есть на обратной стороне карты.

Когда вы получаете новую банковскую карту, сразу запишите название и номер банка себе в телефон.

Номер банка может вам понадобиться.

✦ В этой главе вы узнаете про то, как безопасно пользоваться банковской картой

Важно знать, что происходит с деньгами на вашей карте

Для этого можно подключить SMS-оповещения.

SMS-оповещения — это услуга.

За эту услугу нужно платить деньги.

Услугу можно подключить в банке, банкомате или приложении.

Приложение — это специальная программа на телефоне.

SMS-оповещения — это сообщения, которые приходят на ваш мобильный телефон.

Сообщения могут называть «смсками».

Сообщения отправляет банк, где вы сделали вашу банковскую карту.

Банк отправляет сообщения:

- когда вы расплатились банковской картой
- когда вы сняли с карты наличные деньги
- когда вы перевели деньги с банковской карты
- когда вам пришли деньги на банковскую карту

Ещё в этих сообщениях пишут, сколько осталось денег на вашей банковской карте.

Безопасное пользование банкоматом

Банкомат — это специальное устройство

Так выглядит банкомат:

С помощью банкомата можно совершать разные операции.

Операции — это действия.

Примеры операций, которые можно совершать с помощью банкомата:

- снять наличные деньги с банковской карты
- положить наличные деньги на банковскую карту
- перевести деньги с банковской карты

Также с помощью банкомата можно совершить другие операции.

При пользовании банкоматом нужно соблюдать правила безопасности:

1. Старайтесь пользоваться банкоматами внутри отделения банка.
2. Прикрывайте рукой клавиатуру, когда вводите PIN-код.

PIN-код — это пароль для вашей карты.

Он состоит из 4 цифр.

PIN-код придумываете вы, когда получаете карту в банке.

PIN-код нельзя никому сообщать.

Обязательно запомните свой PIN-код.

Запишите PIN-код в месте, где его можете прочесть только Вы.

Никогда не пишите PIN-код на карте.

Без PIN-кода Вы не сможете снять деньги с карты или оплатить что-то с помощью карты.

3. Если вы снимаете наличные деньги, проверьте, что банкомат вернул банковскую карту.

4. Не пользуйтесь банкоматом, если он долго загружается.

Лучше отменить операцию.

Чтобы отменить операцию, нажмите кнопку «Отмена».

Не забудьте забрать карту.

Если во время пользования банкоматом вы увидели сообщение об ошибке, **не выбрасывайте чек,** который выдал вам банкомат.

5. Если у вас подключены SMS-оповещения, то проверьте телефон.

Вам должно прийти сообщение о том, что вы совершили операцию.

Например, сняли деньги с банковской карты.

Виды оплаты банковской картой

Оплачивать покупки банковской картой
можно двумя способами.

Обычный способ оплаты:

1. Вставить банковскую карту в терминал оплаты.

Терминал оплаты — это специальный банковский аппарат.

Так выглядит терминал.
В него вставлена банковская карта.

2. Ввести PIN-код на клавиатуре.

PIN-код — это пароль для вашей карты.
Он состоит из 4 цифр.
PIN-код придумываете вы,
когда получаете карту в банке.
PIN-код нельзя никому сообщать.

Есть способ бесконтактной оплаты.

Бесконтактная оплата — это оплата,
когда не нужно вставлять карту в терминал.

Способ бесконтактной оплаты:

1. Приложить карту к терминалу оплаты.

Вы так прикладываете проездной
в общественном транспорте.

Если ваша покупка стоит больше 1000 рублей,
то нужно ввести PIN-код.

Если ваша покупка стоит меньше 1000 рублей,
то PIN-код вводить не нужно.

2. Дождаться звукового сигнала от терминала.

Он будет обозначать,
что оплата прошла успешно.

Бесконтактная оплата есть не везде.

Это нужно уточнять у продавца.

Если терминал поддерживает бесконтактную оплату, то на нём будет значок в виде волн и рука с картой рядом.

Значок выглядит так:

У банковских карт не всегда есть функция бесконтактной оплаты.

Если бесконтактная оплата есть на карте, на ней тоже будет значок в виде волн.

Это значок бесконтактной оплаты:

Безопасное пользование банковской картой в кафе или магазине

Банковской картой можно оплатить покупки в магазине или кафе.

Чтобы оплатить покупку в магазине или кафе:

1. Вставьте карту в терминал для оплаты.
2. Введите PIN-код.

Следуйте правилам безопасности, когда расплачиваетесь в магазине или кафе:

- Смотрите, чтобы никто не увидел ваш PIN-код, когда вы пользуетесь терминалом.
- Если вам в кафе не принесли терминал для оплаты, не отдавайте карту официанту.
- Подойдите к терминалу на кассе сами.
- Не забудьте получить чек. Это доказательство того, что вы оплатили покупку.

Примеры небезопасной ситуации

Ситуация 1

Вы разрешили забрать вашу банковскую карту, чтобы расплатиться:

- Человек может сфотографировать вашу карту.
- На карте содержатся важные данные.
- С их помощью человек сможет оплатить покупки в интернете.
- Вы об этом не узнаете и потеряете деньги.

Ситуация 2

Вы решили расплатиться в кафе, но у вас нет SMS-оповещений.

Официант принёс вам терминал для оплаты.

Вы расплачиваетесь.

Вам говорят, что оплатить не получилось.

Вас просят еще раз набрать PIN-код.

Вы вводите PIN-код и платите два раза, хотя нужно было один раз.

Запомните!

Если оплатить не получилось, попросите чек из терминала.

В чеке должно быть написано, что оплата не прошла.

Сохраните этот чек.

CAFE&DONUTS.RU
Москва, ул. Центральная, д. 46
т. 47505503770

12.02.22 чек 0020
16:24 Оплата – ОТКАЗ

НЕДОСТ. СРЕДСТВ (51)

Терминал: 22214321
Мерчант: 78000036805
MIR A000000765410
Карта: (E) **********7768
Клиент: /
Сумма (Руб.):

534.00

Операция отклонена !
НЕДОСТ.СРЕДСТВ (51)

Если вы забыли карту в магазине или другом месте, срочно обратитесь в банк и попросите заблокировать карту:

- Обратитесь в банк, где вы делали вашу карту.
- Название и номер телефона банка написаны на карте.
- В банк можно позвонить или прийти лично.
- Если этого не сделать, банк не будет нести ответственность, если ваши деньги снимут с карты.

Мошенничество с банковскими картами

Мошенничество — это обман человека.

Мошенничество с банковскими картами — это обман человека с целью получить его деньги.

Человека, который занимается мошенничеством, называют **мошенником**.

Украсть деньги с банковской карты сложно.

Мошеннику нужно узнать много информации, чтобы сделать это:

- Чтобы расплатиться вашей картой в интернете, мошеннику нужно знать такую информацию:
  - номер вашей карты
  - имя и фамилия, которые написаны на карте
  - срок действия вашей карты
  - три цифры на обороте карты
- Чтобы снять все деньги с вашей карты, мошеннику нужно знать PIN-код вашей карты
- Чтобы получить доступ к вашим деньгам, мошеннику нужно знать одноразовый пароль

  Одноразовый пароль — это несколько цифр, которые присылает банк в SMS-оповещениях.

  Этот пароль нужен, чтобы:
  - оплатить покупки в интернете
  - перевести деньги
  - зайти в интернет-банк вашей карты

  Этот пароль действует только один раз, поэтому он одноразовый.

  Никогда не передавайте этот пароль другим людям!

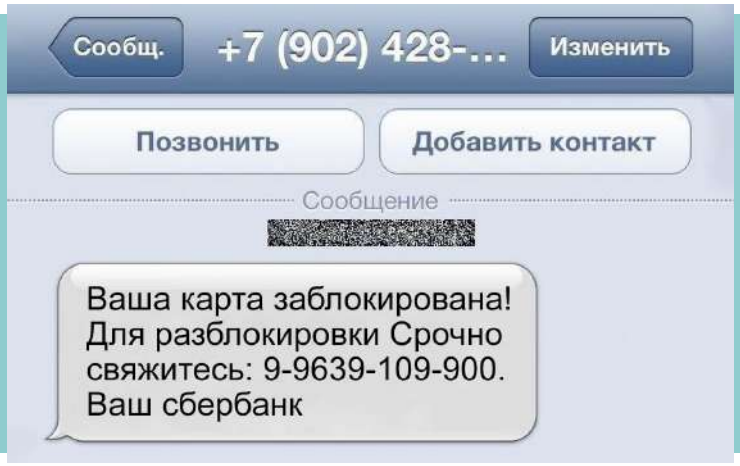
Примеры небезопасной ситуации

Ситуация 1

Вам пришло SMS-оповещение от банка (обычно SMS-оповещения от банка приходят
с одного и того же номера).

Сейчас же SMS-оповещение пришло **с незнакомого номера.**

Пример
SMS-сообщения
от мошенников



В сообщении написано, что ваша карта заблокирована.

В сообщении еще написано, что её можно разблокировать, если позвонить по номеру.

Номер указан в сообщении.

Скорее всего, вам написали мошенники.

Если вы позвоните, то вам ответят мошенники.

Мошенники будут представляться работниками банка.

Мошенники попросят данные вашей карты или попросят подойти к банкомату и сделать операции с картой.

Операции — это действия.

Например, снятие денег — это операция.

Если делать то, что просят эти люди,
вы потеряете деньги.

Правила безопасности в такой ситуации:

1. Не паникуйте и не торопитесь.
2. Не перезванивайте по незнакомому номеру.
3. Позвоните в банк и спросите, заблокировали ли вашу карту.
   Номер банка указан на банковской карте.
4. Либо обратитесь к работникам вашего банка в ближайшем отделении.

Ситуация 2

Вам позвонили люди.

Люди представились сотрудниками государственного учреждения.

Примеры государственных учреждений:

- Банк России
- прокуратура
- суд
- и другие

Люди из государственных учреждений говорят, что вам положены деньги.

Например, деньги за купленные медицинские товары. Это называется компенсация.

Скорее всего, это мошенники.

Мошенники попросят вас что-то оплатить.

Например, налоги.

Или мошенники попросят сказать данные карты или паспорта.

Если делать то, что просят эти люди, вы потеряете деньги.

Правила безопасности в такой ситуации:

1. Не паникуйте и не торопитесь.
2. Ничего не оплачивайте.
3. Не сообщайте данные карты или паспорта.
4. Обратитесь в государственное учреждение лично.
   Либо позвоните в него по телефону.
   Телефон можно найти на официальном сайте учреждения в интернете.

Ситуация 3

Вы получили письмо. Это письмо от Банка России.

В письме написано,что вам положены деньги.
Это решил суд.

Нужно связаться с определенным человеком,
чтобы получить эти деньги.

Связаться нужно очень быстро,
иначе деньги вернутся государству.

Пример письма от мошенников

Деньги

БАНК_РОССИИ@mail.ru
Кому: вам

Уважаемый клиент! Мы рады сообщить, что вам назначена выплата в размере 100 тысяч рублей. Этам сумма положена вам по решению суда по делу о наследстве.

Для получения денег вам нужно позвонить персональному менеджеру по телефону 8-949-292-29-92. Связаться нужно очень срочно!, иначе деньги вернутся государству.

Скорее всего, это мошенники!

Банк России не посылает такие письма!

Если делать то, что просят в письме,
вы потеряете деньги.

Правила безопасности в такой ситуации:

1. Не связывайтесь с человеком, контакты которого указаны в письме.
   То есть не нужно звонить и писать ему.
2. Обратитесь в полицию.

Общие правила безопасности

1. **Включите SMS-оповещения**
   Это нужно, чтобы вовремя заметить, что с вашей карты сняли деньги
2. **Не храните крупные суммы денег на карте, которую используете каждый день**
3. **Скажите сотрудникам банка, если вы собираетесь использовать карту только в России**
   Это нужно,чтобы снятие денег с карты из других стран было невозможно.
4. **Никогда и никому не сообщайте цифры PIN-кода**
   PIN-код — это пароль для вашей карты.
   Он состоит из 4 цифр.
   PIN-код придумываете вы, когда получаете карту в банке.
   Не записывайте PIN-код на карту.
5. **Расскажите друзьям и родственникам про эти правила**

Если из-за мошенников с вашей карты пропали деньги, нужно:

1. **Как можно скорее позвонить в банк.**
   Номер банка есть на обратной стороне карты.
   Скажите, что мошенники украли у вас деньги.
   Попросите заблокировать карту.

2. **Обратитесь в отделение банка, который обслуживает вашу карту.**
   Попросите выписку по счёту.
   Выписка по счёту — это документ.
   В выписке по счёту написаны суммы денег, когда на карту приходили деньги и когда с неё деньги тратились.

3. **Напишите в банке заявление о несогласии с операцией.**
   Это нужно для подтверждения того, что деньги сняли мошенники, а не вы.

4. **Сохраните экземпляр заявления.**
   На нем должна быть отметка банка, что заявление приняли.

5. **Обратитесь в полицию.**
   Напишите заявление о хищении.

Телефонное мошенничество

Ситуация 1

Вы получили с незнакомого номера тревожное SMS-сообщение от родственника или вам позвонил родственник.

Родственник просит срочно дать деньги, потому что он попал в беду.

Родственник поясняет, что времени объяснять ситуацию нет.

Родственник говорит, что за деньгами приедет курьер.

Голос может быть трудно узнать из-за плохой связи.

Скорее всего, это мошенники.
Они хотят вас обмануть.

- Они специально говорят от имени родственников, потому что думают, что вы захотите помочь.
- Они специально звонят в неудобное время, чтобы вы не думали и быстро согласились отдать деньги.

Правила безопасности в такой ситуации:

1. Не спешите отдавать деньги.
2. Попробуйте узнать больше информации.
   Обычно мошенники не хотят долго говорить и пояснять что-то.
3. Если вы не узнали достаточно информации, позвоните родственникам, которые якобы вам звонят.
   Если они не отвечают, позвоните друзьям и другим родственникам.
   Это нужно, чтобы узнать, нужна ли на самом деле помощь.

Ситуация 2

Вам позвонили и сказали, что вы выиграли в лотерею или в каком-то конкурсе.

Вас просят срочно перевести деньги, чтобы оплатить налог на приз.

Это точно мошенники. Переводить деньги нельзя.

Ситуация 3

Вам позвонил сотрудник поликлиники.

Вам говорят, что получены результаты анализов.

Анализы показали, что у вас серьезная болезнь.

Сотрудник поликлиники предлагает пройти лечение.

Лечение нужно проходить на дому, а не в поликлинике.

А еще нужно купить специальные лекарства или медицинские приборы.

Это мошенники. Не соглашайтесь с ними.

Ничего не оплачивайте.

Такого не может быть, потому что:

- Нельзя сообщать результаты анализов по телефону.
- Всегда лучше обратиться лично ко врачу в поликлинике.

Ситуация 4

Вам звонят и говорят, что вам на карту должны прийти деньги.

Эти деньги — ежегодная выплата.

Для перевода просят номер банковской карты и код доступа.

Это мошенники.

- Нельзя сообщать свои данные и данные карты по телефону.

Ситуация 5

Вам позвонили незнакомые люди и позвали на бесплатную консультацию или медицинскую процедуру.

Если вы пришли, вам предлагают что-то приобрести на большую сумму или пройти дорогостоящее лечение.

Если у вас нет денег, вам предлагают взять кредит.

Кредит — это когда человек берет деньги в долг у банка под процент.

То есть потом нужно выплатить банку не только сумму, которая вам была нужна, но и определенную часть от этой суммы за то, что вы пользовались деньгами банка, а не своими.

Это мошенники.

- Нельзя ходить на такие мероприятия.
- Нельзя на таких мероприятиях заключать договоры и брать кредиты.

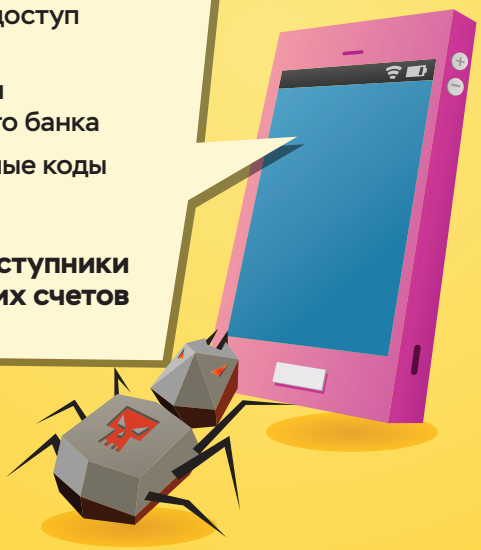
Банк России

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

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

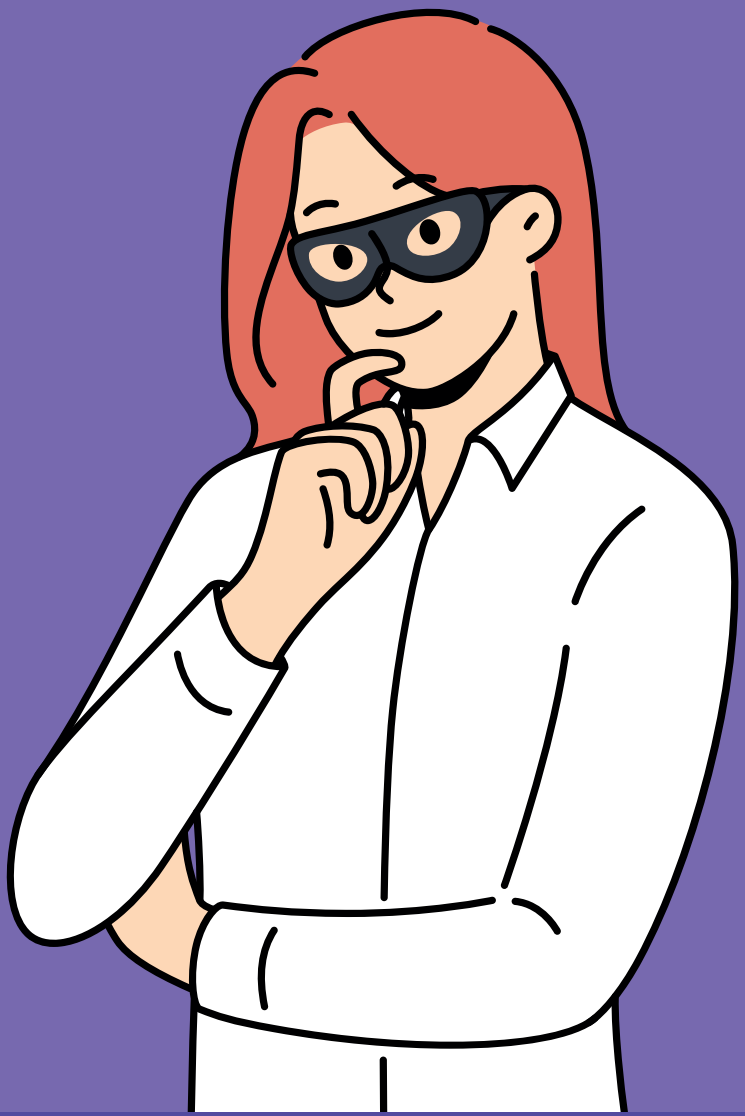
Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Как обманывают мошенники



2024

Содержание

Как обманывают мошенники

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенники придумывают
разные способы обмана.

Мошенник может представиться сотрудником государственной организации.

Вы должны знать, как обманывают мошенники.

Тогда вы сможете защититься
от мошенников.

Способ обмана 1. Мошенники предлагают увеличить вашу пенсию

Пенсия – это денежная помощь
от государства людям,
которым трудно работать.

ПРИМЕР

Вам звонит незнакомый человек.

Человек представляется сотрудником
Социального Фонда России.

Социальный Фонд России –
это государственная организация,
которая платит пенсии и пособия.

Человек говорит вам, что можно увеличить
вашу пенсию.

Человек предлагает вам оформить всё
по телефону.

Человек спрашивает у вас информацию вашей банковской карты.

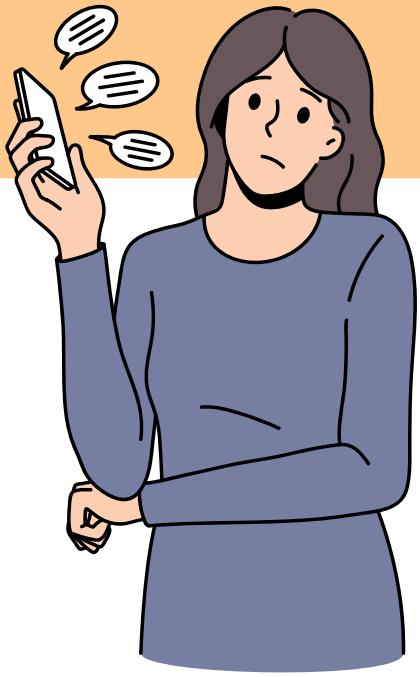
Банковская карта –
небольшая пластиковая карта,
на которой хранится информация
о вашем банковском счёте.

Потом вы получаете СМС-сообщение.

СМС-сообщение – текстовое сообщение
в мобильном телефоне.

Человек просит вас сказать код
из СМС-сообщения.

Не говорите ему ничего!
Вам звонит мошенник.
Он вас обманывает.



ЧТО ДЕЛАТЬ

Не сообщайте никому информацию вашей банковской карты.

Не говорите код из СМС-сообщения.

Прекратите разговор.

Чтобы увеличить вашу пенсию, вы должны прийти в Социальный Фонд.

Вы должны принести в Социальный Фонд нужные документы.

Сотрудник Социального Фонда может спросить:

- ваши документы
- куда перевести деньги

Сотрудник Социального Фонда:

- **не звонит** гражданам по телефону
- **не спрашивает** информацию о банковской карте
- **не спрашивает** секретный код

Секретную информацию спрашивают только мошенники.

Эта информация нужна мошенникам, чтобы украсть деньги с вашего банковского счёта.

ГДЕ ВЫ МОЖЕТЕ УЗНАТЬ ИНФОРМАЦИЮ О ВАШЕЙ ПЕНСИИ:

- Вы можете пойти в Центр «Мои документы».

В центре «Мои документы» вы можете оформить документы и государственные услуги.

- Вы можете пойти в Социальный Фонд России.
- Вы можете позвонить в Социальный Фонд России по телефону: 8-800-100-00-01

Способ обмана 2. Мошенники предлагают вам льготы

Льгота – частичная или полная оплата услуги государством.

Например: государство оплачивает проезд пенсионера в транспорте.

ПРИМЕР

Вам звонит незнакомый человек.

Человек говорит, что можно уменьшить вашу плату за электроэнергию.

Он говорит, что для этого надо записаться в Центр «Мои документы».

Человек предлагает записать вас.

Человек спрашивает у вас информацию
из ваших документов.

Не говорите ему ничего!

Потом вам приходит СМС-сообщение.

Человек просит вас назвать цифры
из СМС-сообщения.

Не говорите ему эти цифры!

ЧТО ДЕЛАТЬ

Не говорите никому информацию
из ваших документов.

Не говорите код из СМС-сообщения.

Прекратите разговор.

В СМС-сообщении может быть секретный код
из портала Госуслуг.

Портал Госуслуг – это место в интернете,
где вы можете оформить документы
и государственные услуги.

Если вы скажете секретный код,
мошенники могут войти
в ваш Личный кабинет на Портале Госуслуг.

Личный кабинет – это ваша личная
страница на сайте.

Если вы скажете мошенникам
код из СМС-сообщения:

- мошенники могут узнать вашу секретную информацию
- мошенники могут взять кредиты на ваше имя

Если вы все-таки сказали код, через две недели проверьте вашу кредитную историю.

Кредитная история – это информация обо всех ваших кредитах.

Вы можете заказать кредитную историю на портале Госуслуг.

Если мошенники взяли кредит на ваше имя, вы увидите это в кредитной истории.

ВЫ МОЖЕТЕ УЗНАТЬ ИНФОРМАЦИЮ О ЛЬГОТАХ:

- в Управлении социальной защиты населения
- в Центре «Мои документы»

Способ обмана 3. Мошенники предлагают большие скидки на товары

Скидка – это уменьшение цены товара.

Мошенники могут продавать ненужные товары по высоким ценам.

Мошенники обманывают людей, чтобы продать свои товары.

ПРИМЕР 1

Незнакомый человек предлагает вам купить очень хорошее лекарство.

Человек говорит, что в других местах лекарство стоит дороже.

Человек предлагает вам купить лекарство со скидкой.

Врач не выписывал вам это лекарство. Нельзя покупать лекарство, если его вам не выписал врач.

ЧТО ДЕЛАТЬ

Не покупайте лекарства
у незнакомых людей.

Лекарства нужно покупать в аптеке.

Нужно покупать только то лекарство,
которое вам выписал врач.

Подумайте спокойно.

Посоветуйтесь с врачом.

Это лекарство может навредить вам.

ПРИМЕР 2

Незнакомый человек говорит,
что вы выиграли приз.

Чтобы получить приз, вы должны купить
другой товар.

ЧТО ДЕЛАТЬ

Не спешите платить деньги.

Подумайте спокойно.

Посоветуйтесь с близким человеком.

Покупайте только нужные товары.

Если вы хотите купить товар, узнайте о нём больше.

Узнайте цену товара в других местах.

ПРИМЕР 3

К вам домой приходит незнакомый человек.

Человек говорит, что он сотрудник газовой службы.

Газовая служба – организация, которая следит за газовым оборудованием в домах.

Газовое оборудование – приборы, в которых используется природный газ. Например:
— газовая плита для приготовления пищи
— газовая колонка для нагревания воды

Незнакомый человек говорит, что у вас нет датчика утечки газа.

Датчик утечки газа – прибор, который проверяет воздух в квартире.

Если в воздухе содержится много природного газа, звучит сигнал.

Человек говорит, что вы должны заплатить штраф.

Человек предлагает вам установить датчик утечки газа, **чтобы не платить штраф.**

ЧТО ДЕЛАТЬ

Не спешите платить деньги.

Вы **не должны** платить штраф, если у вас нет датчика утечки газа.

Вы можете установить такой датчик, только если захотите.

Посоветуйтесь с близким человеком.

Узнайте цену датчика в других местах.

Узнайте стоимость установки датчика.

Датчик утечки газа может установить только сотрудник газовой службы.

Мошенники могут повредить ваше газовое оборудование.

Мошенники могут представиться сотрудниками разных коммунальных служб.

Примеры коммунальных служб:

- организация, которая даёт воду
- организация, которая даёт электричество
- организация, которая даёт газ

Мошенники могут надеть специальную одежду.

Мошенники могут сделать фальшивые документы.

Не пускайте к себе домой незнакомых людей.

Узнайте телефоны коммунальных служб.

Узнайте телефон вашей управляющей компании.

Управляющая компания – это организация, которая обслуживает дома с квартирами.

Вы можете найти телефон управляющей компании в квитанции на оплату коммунальных услуг.

Если незнакомый человек представляется сотрудником коммунальной службы, **не пускайте его в дом.**

Позвоните в эту организацию.

Проверьте информацию.

Способ обмана 4. Мошенники говорят людям о тяжёлой болезни

У многих людей есть проблемы со здоровьем. Мошенники могут сказать, что они сотрудники медицинской организации.

Мошенники могут сообщить человеку, что он тяжело болен.

Человек пугается, потому что боится умереть. Когда человек испуган, его легко обмануть. Мошенники говорят, что нужно заплатить за лечение.

Человек отдаёт мошенникам деньги.

ПРИМЕР 1

Незнакомый человек сообщает вам о вашей болезни по телефону.

Незнакомый человек может сказать, что он врач.

Незнакомый человек говорит, что вы должны заплатить деньги за лечение.

Незнакомый человек торопит вас и **не даёт** подумать.

ЧТО ДЕЛАТЬ

Не спешите платить деньги.

Посоветуйтесь с близким человеком.

Позвоните в поликлинику по телефону.
Спросите про этого врача.
Если такого врача нет,
то вам звонил мошенник.

Если такой врач есть, попросите записать вас к нему на приём.

Вы можете обсудить ваше лечение с врачом во время приёма.

Попросите близкого человека пойти на приём с вами.

Способ обмана 5. Мошенники предлагают вам выгодно вложить деньги

МОШЕННИКИ ПРЕДЛАГАЮТ ВАМ ВЫГОДНО ВЛОЖИТЬ ДЕНЬГИ

Мошенники предлагают вам перевести ваши деньги на другой банковский счёт.

Мошенники говорят, что вы получите много денег.

Мошенники говорят, что нет никаких рисков.

- **Не верьте** таким обещаниям!
- Вы **не получите** много денег.
- Мошенники заберут ваши деньги.

Вы можете открыть вклад в вашем банке.

Если вы хотите открыть вклад в банке, посоветуйтесь с близким человеком.

МОШЕННИКИ ПРЕДЛАГАЮТ ВАМ ТОРГОВАТЬ НА БИРЖЕ

Биржа – это место, где продают и покупают:
— ценные бумаги
— валюту – деньги других стран
— драгоценные металлы

Мошенники могут предложить вам торговать на бирже.

Мошенники обещают научить вас бесплатно.

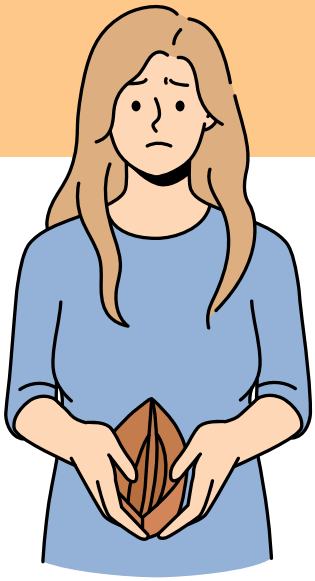
Мошенники говорят, что вы заработаете много денег.

Не верьте таким обещаниям!

Вы ничего **не заработаете**.

Мошенники заберут ваши деньги.

У вас могут появиться долги по кредитам.



Способ обмана 6. Мошенники предлагают перевести ваши деньги на безопасный счёт

ПРИМЕР

Незнакомый человек звонит вам по телефону.

Человек говорит, что он сотрудник вашего банка.

Человек говорит, что мошенники могут украсть деньги с вашего банковского счёта.

Человек предлагает вам перевести ваши деньги на безопасный счёт.

ЧТО ДЕЛАТЬ

Прекратите разговор.
Мошенники хотят забрать ваши деньги.

Не переводите никуда деньги,
если кто-то говорит вам это сделать.

С вашим банковским счётом
всё в порядке.

В банках нет специальных безопасных счетов.

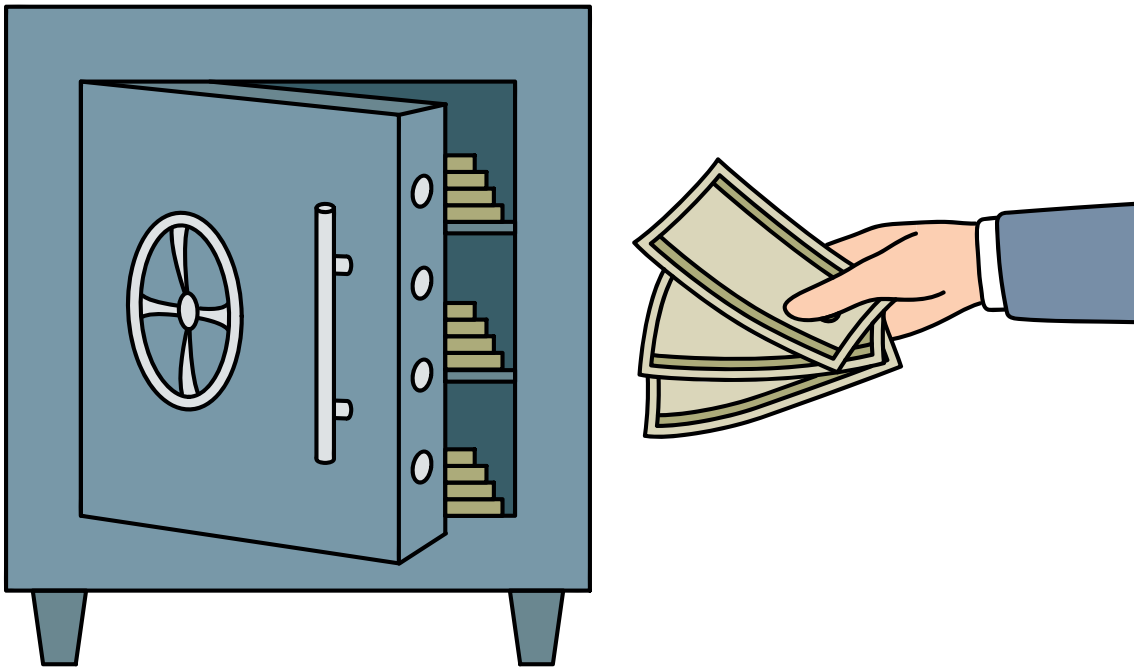
Все банковские счета должны быть безопасными.

Не говорите, не пишите, не показывайте никому информацию вашего банковского счёта.

Не говорите, не пишите, не показывайте никому информацию вашей банковской карты.

Не говорите, не пишите, не показывайте никому код из СМС-сообщения.

Тогда ваши деньги будут в безопасности.



Способ обмана 7. Мошенники предлагают помочь вернуть украденные деньги

Если мошенники украли деньги у человека, они могут сделать это ещё раз.

Другие мошенники звонят этому человеку.

Они предлагают помочь вернуть украденные деньги.

Мошенники требуют:

- заплатить им за помощь
- сообщить информацию банковской карты

Человек может потерять ещё больше денег.

Незнакомые люди **не могут** помочь вернуть деньги.

Чтобы вернуть деньги, нужно обращаться только в полицию.

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ

Мошенники придумывают новые способы обмана.

Чтобы вас не обманули, соблюдайте простые правила:

Не разговаривайте о деньгах с чужими людьми.

Мошенник может сказать, что он сотрудник банка.

Мошенник может сказать, что он сотрудник государственной организации.

Найдите в интернете телефон этой организации.

Позвоните по этому телефону.

Проверьте информацию, которую вам сказал незнакомый человек.

Никому не сообщайте то, что написано на вашей банковской карте.

Не вводите эту информацию на неизвестных сайтах.

Никому не сообщайте код из СМС-сообщений.

ЕСЛИ МОШЕННИКИ УКРАЛИ ДЕНЬГИ С ВАШЕГО БАНКОВСКОГО СЧЁТА

1 **Позвоните в ваш банк.**

- → Вы можете найти телефон банка на вашей банковской карте.
- → Вы можете найти телефон банка на официальном сайте банка.

2 **Сообщите** сотруднику банка, что у вас **украли деньги**.

- → Сотрудник банка скажет вам, что делать.

3 **Напишите** заявление в полицию.

- → Если вам трудно, попросите близкого человека помочь вам.

ЕСЛИ ВЫ ПЕРЕВЕЛИ ДЕНЬГИ МОШЕННИКАМ

1 **Позвоните в ваш банк.**

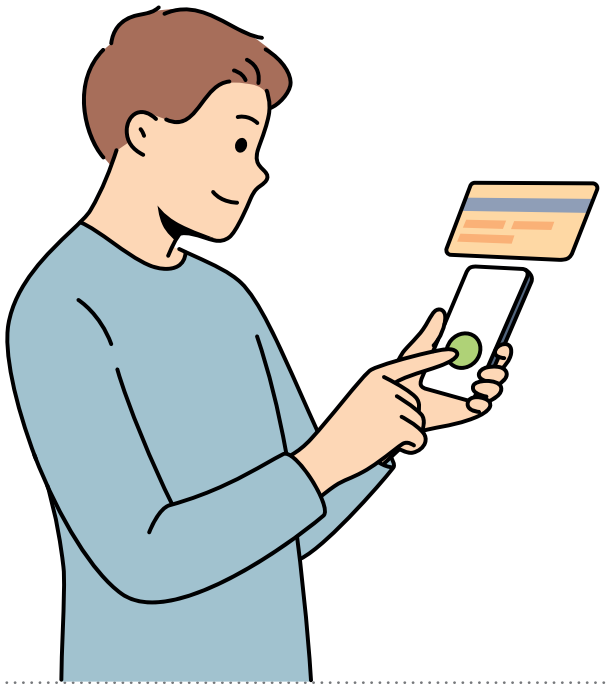
- → Вы можете найти телефон банка на вашей банковской карте.
- → Вы можете найти телефон банка на официальном сайте банка.

2 **Сообщите** сотруднику банка, что вы **перевели деньги** мошенникам.

- → Сотрудник банка скажет вам, что делать.

3 **Напишите** заявление в полицию.

- → Если вам трудно, попросите близкого человека помочь вам.



Словарь

Банковская карта – небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Банковский вклад – деньги, которые хранятся в банке определённое время. Банк прибавляет деньги к деньгам вашего банковского вклада.

Биржа – это место, где продают и покупают ценные бумаги, валюту, драгоценные металлы.

Валюта – деньги других стран.

Газовое оборудование – приборы, в которых используется природный газ. Газовая служба следит за газовым оборудованием в домах.

Датчик утечки газа – прибор, который проверяет воздух в квартире. Если в воздухе содержится много природного газа, звучит сигнал.

Кредитная история – это информация обо всех ваших кредитах.

Личный кабинет – это ваша личная страница на сайте.

Льгота – частичная или полная оплата услуги государством.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Пенсия – это денежная помощь от государства людям, которым трудно работать.

Портал Госуслуг – это место в интернете, где вы можете оформить документы и государственные услуги.

Скидка – это уменьшение цены товара.

СМС-сообщение – текстовое сообщение в мобильном телефоне.

Социальный Фонд России – это государственная организация, которая платит пенсии и пособия.

Управляющая компания – это организация, которая обслуживает дома с квартирами.

Центр «Мои документы» – это организация, где вы можете оформить документы и государственные услуги.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Как понять, что с вами говорит мошенник

2024

Содержание

Как понять, что с вами говорит мошенник

Мошенник – человек, который пытается обмануть вас и украсть ваши деньги.

Мошенники всё время придумывают новые способы обмана.

Как вы можете понять, что с вами говорит мошенник?

1. Мошенники всегда сами звонят или пишут вам

Мошенники могут:

- позвонить вам по телефону
- прислать вам СМС-сообщение – текстовое сообщение в мобильном телефоне
- прислать вам электронное письмо
- прислать вам ссылку на сайт

Мошенник может сказать, что он:

- сотрудник банка
- сотрудник полиции
- ваш богатый родственник

Если незнакомый человек звонит
или пишет вам, будьте осторожны.

Этот человек хочет что-то получить от вас.

Вы **не можете** сразу узнать, кто этот человек.

Этот человек может обмануть вас.

Мошенники могут подменить номер телефона.

На экране телефона в момент вызова
вы увидите другой номер.

Например, номер телефона вашего банка.

Вы подумаете, что звонит сотрудник
вашего банка.

Мошенники могут создавать поддельные сайты организаций.

Поддельные сайты очень похожи на настоящие сайты.

Мошенники могут создавать поддельные страницы на сайтах.

Внимание!

Незнакомый человек может обмануть вас.

Проверяйте информацию от незнакомых людей.

Попросите помощи у близкого человека.

2. Мошенники всегда говорят с вами о деньгах

Мошенники хотят украсть ваши деньги.

Поэтому мошенники всегда говорят о деньгах.

Мошенники обычно говорят:

- ➜ что вы можете потерять деньги

или

- ➜ что вы можете получить деньги

Если незнакомый человек говорит с вами о ваших деньгах, будьте осторожны.

3. Мошенники просят сообщить вашу секретную информацию

Мошенники могут спросить у вас информацию вашей банковской карты.

Банковская карта –
небольшая пластиковая карта,
на которой хранится информация
о вашем банковском счёте.

На вашем банковском счёте хранятся ваши деньги.

Не говорите никому информацию вашей банковской карты!

Мошенники могут спросить логин и пароль вашего Личного кабинета на сайте банка.

Личный кабинет – это ваша
личная страница на сайте банка.

Логин и пароль нужны, чтобы войти в ваш Личный кабинет на сайте.

Мошенники часто спрашивают код из СМС-сообщения от вашего банка.

Не говорите никому код из СМС-сообщения!

Настоящий сотрудник банка **не спрашивает** секретную информацию:

- информацию банковской карты
- логин и пароль Личного кабинета
- код из СМС-сообщения от банка

Секретную информацию спрашивают только мошенники.

4. Мошенники хотят напугать или обрадовать вас

Мошенники стараются вас напугать
или сильно обрадовать.

Тогда вы начнёте волноваться
и можете совершить ошибку.

Не верьте им!

ПРИМЕР 1

Мошенник говорит человеку, что преступники
вошли в его Личный кабинет на сайте банка.

Человек пугается, потому что преступники
могут украсть его деньги

Человек думает только о том,
как спасти свои деньги.

Человек в таком состоянии сделает всё,
что скажет мошенник.

Человек может сказать мошеннику
любую информацию.

Не делайте то, что говорит вам незнакомый человек.

Не говорите ничего незнакомому человеку.

ПРИМЕР 2

Незнакомый человек говорит вам, что вы выиграли много денег.

Человек говорит, что вы можете их получить.

Для этого нужно заплатить небольшую сумму на сайте.

На сайте вы должны ввести информацию вашей банковской карты.

Внимание!

Это сайт мошенников.

Мошенники могут узнать информацию о вашей банковской карте.

Мошенники могут украсть деньги с вашего банковского счёта.

Никогда не вводите информацию на таких сайтах.

ЧТО ДЕЛАТЬ

Если вы волнуетесь,
постарайтесь успокоиться.

Не торопитесь делать всё, что говорят незнакомые люди.

Посоветуйтесь с близким человеком.

Если незнакомый человек хочет узнать информацию о вас, прекратите разговор.

Если незнакомый человек что-то требует от вас, прекратите разговор.

5. Мошенники торопят вас

Мошенники торопят вас
и мешают спокойно подумать.

Мошенники говорят, что вам нужно сделать.

Мошенники говорят, что сделать это нужно прямо сейчас.

Не слушайте их!

Если незнакомый человек пугает вас, прекратите разговор.

Если незнакомый человек что-то требует от вас, прекратите разговор

ЧТО ДЕЛАТЬ

Не спешите.

Спокойно подумайте.

Посоветуйтесь с близким человеком.

Всегда проверяйте информацию.

Если незнакомый человек что-то требует от вас, прекратите разговор.

ПРИМЕР

Вы получили электронное письмо.

В этом письме написано, что вы можете получить выплату от государства.

ЧТО ДЕЛАТЬ

Найдите в интернете информацию об этой выплате.

Найдите закон об этой выплате.

Вы можете прочитать в законе, кто может получить эту выплату.

Если вы **не нашли** закон об этой выплате, **не верьте** информации из письма.

Удалите это электронное письмо.

Внимание!
Признаки мошенника

- **Незнакомый человек сам пишет или звонит вам.**
- **Незнакомый человек говорит или пишет вам о деньгах.**
- **Незнакомый человек просит вашу секретную информацию.**
- **Незнакомый человек пугает вас.**
- **Незнакомый человек торопит вас.**

Словарь

Банковская карта –
небольшая пластиковая карта,
на которой хранится информация
о вашем банковском счёте.

Банковский счёт – это место в банке,
где хранятся ваши деньги.

Личный кабинет – это ваша личная страница
на сайте.

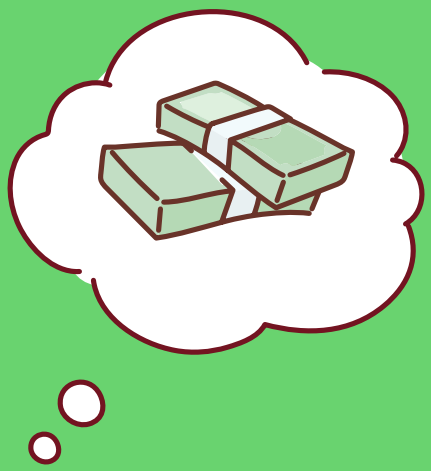
Логин и пароль нужны, чтобы войти
в ваш Личный кабинет на сайте.

Мошенник – человек, который пытается
обмануть вас и украсть ваши деньги.

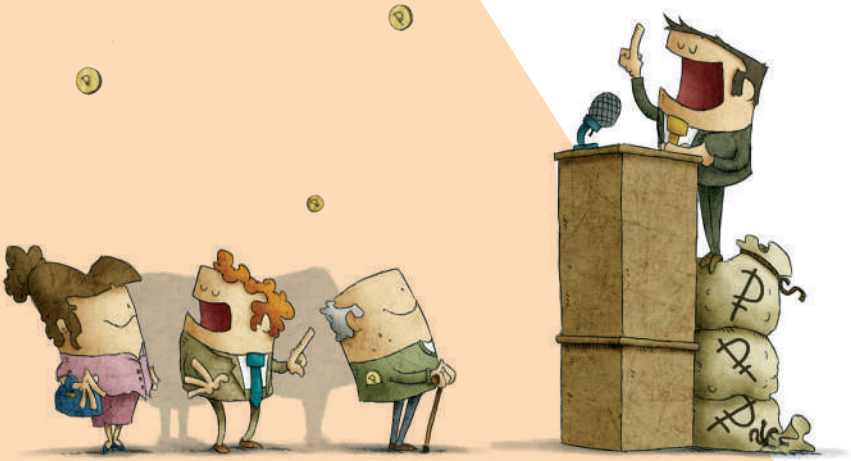
СМС-сообщение – текстовое сообщение
в мобильном телефоне.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК



КАК РАСПОЗНАТЬ ФИНАНСОВУЮ ПИРАМИДУ



Финансовая пирамида — это мошеннический проект, который имитирует выгодные инвестиции.

Вас призывают вложить деньги в фиктивный бизнес и агитируют приводить друзей и родственников. В результате можно потерять не только деньги, но и доверие своих близких.

КАКИМИ БЫВАЮТ ФИНАНСОВЫЕ ПИРАМИДЫ?

Пирамиды могут маскироваться под любые компании: кредитные потребительские кооперативы (КПК), микрофинансовые организации (МФО) и просто интернет-проекты.

Фантазия обманщиков безгранична. Они предлагают вложиться в сельское хозяйство или криптовалюты, открыть бизнес по франшизе.

Ключевое отличие от реального бизнеса — организаторы ничего производят и ни во что не инвестируют деньги вкладчиков. Мошенники просто собирают их в свой карман.

ПРИЗНАКИ ФИНАНСОВОЙ ПИРАМИДЫ

Обещают высокий доход

Если вам «гарантируют» десятки или даже сотни процентов в год без всякого риска, это точно аферисты.

Вас просят приводить новых клиентов

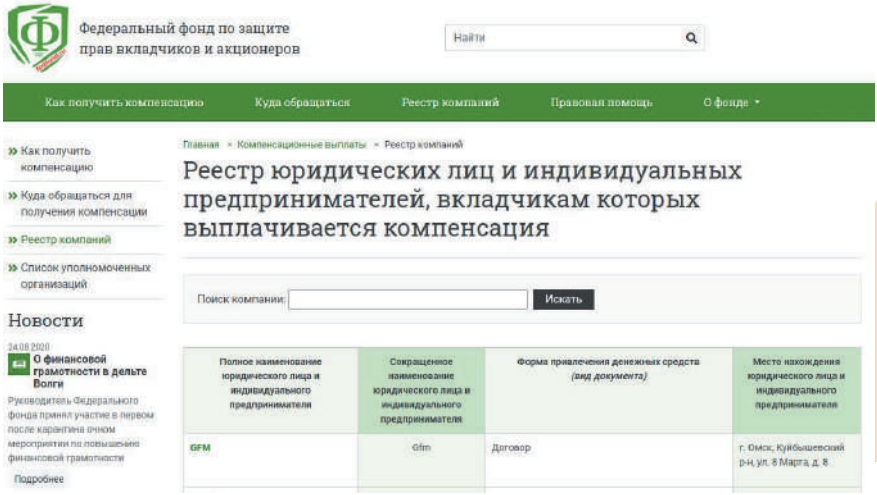
И обещают начислить процент от их взноса. Так преступники пытаются побыстрее вовлечь как можно больше людей в свою аферу, собрать с них деньги и скрыться.

Нет подтверждения инвестиций

Вам показывают только красивые презентации и не дают взглянуть на финансовые документы, бухгалтерскую отчетность. Деньги просят перевести на чей-то персональный счет либо электронный кошелек или же внести наличными, при этом не выдают никаких чеков

МОЖНО ЛИ ВЕРНУТЬ ДЕНЬГИ, ЕСЛИ ПИРАМИДА РУХНУЛА?

Можно, но при условии, что пирамида попала в реестр **Федерального фонда по защите прав вкладчиков и акционеров**. Только он выплачивает компенсации обманутым клиентам некоторых компаний. На сайте Фонда **fedfond.ru** можно посмотреть список пирамид, по которым идут выплаты.



МАКСИМАЛЬНЫЙ РАЗМЕР КОМПЕНСАЦИИ:

- для ветеранов и инвалидов Великой Отечественной войны — **250 000 рублей**
- для всех остальных граждан — максимум **35 000 рублей**

Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Мошенники просят вас сказать код из СМС-сообщения

2024

Содержание

Мошенники просят вас сказать код из СМС-сообщения

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

СМС-сообщение – текстовое сообщение в мобильном телефоне.

Никому **не говорите** код из СМС-сообщения!

Код у вас могут спрашивать только мошенники.

Мобильный оператор –
это организация, которая оказывает
услуги мобильной связи.

Примеры мобильных операторов России:

- Билайн
- Мегафон
- МТС
- Т2

ПРИМЕР

Незнакомый человек звонит вам по телефону.

Человек говорит вам, что он сотрудник
вашего мобильного оператора.

Человек говорит, что заканчивается
срок действия вашей СИМ-карты.

СИМ-карта – это маленькая пластина в мобильном телефоне.
СИМ-карта нужна, чтобы пользоваться мобильной связью.

Человек говорит, что ваш телефон **не будет работать.**

Человек говорит, что вы должны продлить срок действия вашей СИМ-карты.

Тогда ваш телефон будет работать.

Человек предлагает продлить срок действия СИМ-карты по телефону.

Вы получаете СМС-сообщение.

СМС-сообщение – это текстовое сообщение в мобильном телефоне.

Человек просит вас сказать цифры из СМС-сообщения.

Не говорите ему ничего!
Вам звонит мошенник.
Он вас обманывает.
У СИМ-карт нет срока действия.
СИМ-карты не нужно продлевать.

ЧТО ДЕЛАТЬ

1 **Прекратите** разговор.

2 **Не называйте** никому цифры из СМС-сообщения.

Если вы скажете код, мошенники смогут совершать действия от вашего имени.

ПРИМЕР

Мошенники смогут войти в ваш Личный кабинет на сайте мобильного оператора.

> Личный кабинет – это ваша личная страница на сайте.

Мошенники могут перевести ваши звонки и сообщения на свой номер.

Тогда мошенники смогут узнать вашу секретную информацию.

Мошенники смогут узнавать все коды из ваших СМС-сообщений.

Мошенники могут украсть деньги
с вашего банковского счёта.

Банковский счёт – место в банке,
где хранятся ваши деньги.

Мошенники могут взять кредит на ваше имя.

Кредит – это деньги, которые вы берёте
в долг у банка.

**Нельзя никому говорить код
из СМС-сообщения.**

Что делать, если вы уже сказали код

1 **Заблокируйте** ваши банковские карты.

> Банковская карта – небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Вы можете заблокировать банковскую карту в Личном кабинете на сайте вашего банка.

2 **Позвоните** в ваш банк.

> Телефон банка вы можете найти на вашей банковской карте.

Расскажите сотруднику банка, что случилось.

3 **Зайдите** в ваш Личный кабинет
на сайте мобильного оператора.

Проверьте услуги на вашем телефоне.

Отмените все лишние услуги.

Отмените переадресацию,
если она установлена.

4 **Проверьте** вашу кредитную историю.

Кредитная история –
это информация
обо всех ваших кредитах.

Вы можете заказать кредитную историю
на Портале Госуслуг.

Портал Госуслуг – это место в интернете,
где вы можете оформить документы
и государственные услуги.

Если мошенники взяли кредит
на ваше имя, вы увидите это
в кредитной истории.

Правила безопасности

Не говорите секретный код чужим людям.

Если незнакомый человек торопит вас, прекратите разговор.

Если незнакомый человек пугает вас, прекратите разговор.

Не спешите.

Спокойно подумайте.

Посоветуйтесь с близким человеком.

Не верьте, что вам звонит сотрудник мобильного оператора.

Позвоните по телефону мобильного оператора.

Вы можете найти телефон на официальном сайте мобильногооператора.

Расскажите сотруднику мобильного оператора, что случилось.

Словарь

Банковская карта – небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Банковский счёт – место в банке, где хранятся ваши деньги.

Кредит – это деньги, которые вы берёте в долг у банка.

Кредитная история – это информация обо всех ваших кредитах.

Личный кабинет – это ваша личная страница на сайте.

Мобильный оператор – это организация, которая оказывает услуги мобильной связи.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Портал госуслуг – это место в интернете, где вы можете оформить документы и государственные услуги.

СИМ-карта – это маленькая пластина в мобильном телефоне.
СИМ-карта нужна, чтобы пользоваться мобильной связью.

СМС-сообщение – это текстовое сообщение в мобильном телефоне.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Мошенничество

2022

Содержание

Мошенничество – это обман людей с целью украсть их деньги.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенники пытаются узнать вашу секретную информацию.

Мошенники пытаются узнать ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники хотят узнать информацию о ваших банковских счетах.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Мошенники хотят узнать информацию о ваших банковских картах.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Мошенники хотят узнать ПИН-код вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль вашей банковской карты.

ПИН-код – это 4 цифры.

ПИН-код нужен, чтобы пользоваться вашей банковской картой.

ПИН-код вашей банковской карты должны знать только вы.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Мошенники хотят узнать защитный код вашей банковской карты.

Защитный код (CVV/CVC-код) – 3 цифры на оборотной стороне вашей банковской карты.

Защитный код нужен для подтверждения платежа с вашей банковской карты.

Не говорите, **не показывайте** и **не пишите** защитный код вашей банковской карты чужим людям.

Мошенники хотят узнать одноразовый пароль из СМС-сообщения от банка.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на телефон.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Мошенники обманывают людей разными способами.

Вы должны знать, как обманывают мошенники.

Тогда вы сможете защититься от мошенников.

Где мошенники могут быть опасны?

1 Мошенники могут быть опасны при использовании банкомата

Банкомат – аппарат для приёма и выдачи наличных денег.

Для использования банкомата вам нужна ваша банковская карта.

Вам нужно набрать ПИН-код вашей банковской карты.

ПИН-код – это секретный пароль вашей банковской карты.

ПИН-код — это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Другие люди **не должны** видеть ПИН-код вашей банковской карты.

Мошенники могут пытаться узнать ваш ПИН-код.

Мошенники могут:

- установить на банкомат специальное устройство
- установить видеокамеру над клавиатурой банкомата

Если мошенники получат информацию о вашей банковской карте, они могут украсть ваши деньги.

Если вы хотите снять деньги, внимательно осмотрите банкомат.

Если на банкомате есть лишние предметы, найдите другой банкомат.

Если клавиатура банкомата шатается, найдите другой банкомат.

Мошенники могут попытаться подсмотреть ваш ПИН-код.

Пользуйтесь банкоматом, когда рядом нет других людей.

Когда вы вводите ПИН-код вашей банковской карты, прикрывайте клавиатуру рукой.

Если вам трудно пользоваться банкоматом, попросите близкого человека помочь вам.

Если кто-то предлагает вам помощь у банкомата без вашей просьбы, откажитесь от помощи.

Если вы обращаетесь за помощью к чужим людям, будьте осторожны.

Не передавайте вашу банковскую карту чужим людям.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Лучше пользоваться банкоматом в офисе банка.

Если вам нужна помощь, сотрудник банка поможет вам.

2 Мошенники могут быть опасны при оплате товаров и услуг в интернете

При оплате в интернете вы вводите секретную информацию:

- номер вашей банковской карты
- срок окончания действия вашей банковской карты
- ваши имя и фамилию
- защитный код (CVV/CVC-код) вашей банковской карты

Для оплаты в интернете банки присылают вам одноразовый пароль.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на мобильный телефон.

Одноразовый пароль нужно ввести на странице оплаты.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Чтобы получать СМС-сообщения от банка, вам нужно подключить мобильный банк.

Мобильный банк – это система, которая позволяет управлять вашими деньгами в банке с помощью СМС-сообщений.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Никто **не должен** спрашивать у вас одноразовый пароль.

Одноразовый пароль спрашивают только мошенники.

СМС-сообщения из банка – это ваша секретная информация.

Никто **не должен** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

Иногда вам может позвонить сотрудник банка.

Он может спросить про последние платежи с вашей банковской карты.

Сотрудник банка **не должен** спрашивать у вас информацию вашей банковской карты.

Информацию банковской карты спрашивают только мошенники.

Если у вас спрашивают информацию вашей банковской карты, сразу завершите разговор.

3 Мошенники могут быть опасны в интернете

Чтобы узнать вашу секретную информацию, мошенники создают поддельные сайты.

Мошенники копируют сайты известных организаций.

Поддельный сайт очень похож на настоящий сайт организации.

Поддельный сайт имеет другой адрес в интернете.

Пример

Вы попали на поддельный сайт интернет-магазина.

Вы хотите оплатить покупку на этом сайте.

Вы вводите информацию вашей банковской карты.

Ваша секретная информация попадает к мошенникам.

Мошенники могут украсть ваши деньги.

Будьте внимательны!

Адреса поддельных сайтов очень похожи на адреса настоящих сайтов.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Мошенники могут прислать вам сообщение со ссылкой на поддельный сайт.

Не нажимайте на эту ссылку!

Сообщение вы можете получить:

- в телефоне
- по электронной почте
- в социальной сети

Мошенники пишут ложные сообщения.

Примеры ложных сообщений:

- ваша карта заблокирована
- с вашего банковского счёта переведены деньги
- на ваш банковский счёт зачислены деньги
- вы выиграли в лотерею
- вам нужно обновить ваши личные данные
- вам нужно подтвердить ваши личные данные

Мошенники пишут ложные сообщения, чтобы вы нажали ссылку.

Если вы нажмёте ссылку, вы попадёте на поддельный сайт.

Не нажимайте на эту ссылку!

Поддельный сайт внешне очень похож на настоящий сайт.

На поддельном сайте вас попросят ввести ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники могут украсть ваши личные данные.

Мошенники могут украсть ваши деньги.

Пример 1

Вам приходит сообщение от вашего друга.

В сообщении есть ссылка.

В сообщении говорится, что нужно нажать ссылку.

Что делать

- **не нажимайте** ссылку в сообщении
- позвоните вашему другу
- расскажите вашему другу о сообщении

Мошенники украли секретную информацию вашего друга.

Мошенники хотят украсть вашу секретную информацию.

Пример 2

Вам приходит сообщение от известного магазина.

В сообщении вам предлагают большие скидки на товары.

Вам нужно перейти на сайт по ссылке.

Чтобы получить скидку, вам нужно ввести ваши личные данные на сайте.

Что делать

- **не нажимайте** ссылку в сообщении
- найдите в интернете сайт магазина
- узнайте на этом сайте информацию о скидках

Не вводите ваши личные данные на сайте.

Известные организации никогда **не спрашивают** личные данные.

Правила безопасности:

- **не нажимайте** ссылки в неизвестных сообщениях
- **не загружайте** вложенные файлы, которые вы **не ждете**

Вложенный файл – документ, который приходит в сообщении.

Обращайте внимание на интернет-адрес в ссылке.

Обращайте внимание на адресную строку.

Интернет-адрес поддельного сайта отличается от интернет-адреса настоящего сайта.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Если вы постоянно пользуетесь сайтом, сохраните его в закладках.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Обращайте внимание на содержание сообщения.

Мошенники часто делают много ошибок.

Не звоните по телефонам из сообщения.

Найдите в интернете сайт организации.

На сайте организации вы можете найти номер телефона.

Позвоните по этому номеру телефона.

Вы сможете узнать нужную информацию.

Вы будете уверены, что вас **не обманули**.

Надёжно защитите ваши пароли.

Никому **не говорите** ваши пароли.

Запишите пароли на бумаге и храните в надёжном месте.

Никому **не передавайте** ваши пароли.

Никому **не говорите** и **не пишите** ваши личные данные.

Установите антивирус на ваши устройства.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Регулярно обновляйте программы и приложения на ваших устройствах.

4 Мошенники создают финансовые пирамиды

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Например, мошенники предлагают людям вкладывать деньги в фонд.

Мошенники обещают очень высокий доход.

Если люди вкладывают деньги в такой фонд, мошенники украдут эти деньги.

Можно вкладывать деньги только в известные финансовые организации.

Как понять, что вас обманывают?

Как понять, что вас зовут в финансовую пирамиду?

Признаки финансовой пирамиды:

- вам обещают высокий доход
- вам говорят, что нет никаких рисков
- вас просят внести деньги сразу
- вас просят внести наличные деньги
- вас просят привести друга

На финансовых пирамидах заработать нельзя.

Мошенники заберут ваши деньги.

Вы **не сможете** вернуть ваши деньги.

5 Мошенники бывают на торговых сайтах

В интернете есть торговые сайты.

На этих сайтах вы можете сами продавать и покупать товары.

На торговых сайтах вы можете встретить мошенников.

Будьте внимательны.

Мошенники могут вас обмануть.

Пример 1

Вы хотите купить товар.

Продавец товара живёт в другом городе.

Товар нужно переслать в ваш город.

Продавец требует заранее оплатить пересылку товара.

Продавец просит перевести деньги на его банковскую карту.

Что делать

- **не переводите** деньги заранее
- вы **не получите** товар
- вы потеряете деньги

Платите деньги после того, как получите товар.

Если продавец требует заранее заплатить ему деньги, **не общайтесь** с ним.

Найдите другого продавца.

Пример 2

Вы хотите что-то продать.

Покупатель хочет перевести деньги на ваш банковский счёт.

Покупатель просит у вас номер вашей банковской карты.

Покупатель просит у вас защитный код (CVV/CVC-код) вашей банковской карты.

Что делать

Защитный код банковской карты (CVV/CVC-код) – это секретный код.

Никому **не говорите** и **не пишите** защитный код вашей банковской карты.

Чтобы перевести вам деньги, покупателю нужен только номер вашей банковской карты.

Если покупатель просит вашу секретную информацию, **не общайтесь** с ним.

Пример 3

Вы разместили объявление о продаже товара.

Вы получаете СМС-сообщение с неизвестного номера.

В сообщении вы можете прочитать ложную информацию:

- ваше объявление заблокировано за нарушение правил
- есть отклик на ваше объявление
- пришлите СМС с кодом для отмены блокировки

Что делать

Не отправляйте СМС-сообщение на неизвестный номер.

Вы можете потерять много денег.

Зайдите на сайт, где вы разместили объявление.

Найдите на сайте контакты службы поддержки.

Напишите или позвоните в службу поддержки сайта.

Расскажите о сообщении, которое вы получили.

Вам скажут, что нужно делать.

6 Мошенники могут присылать электронные письма

Мошенники могут присылать вам письма на электронную почту.

Мошенники могут предлагать вам:

- много денег за помощь
- пройти опрос
- получить приз

Не верьте тем, кто предлагает вам деньги и призы.

Не отвечайте на письма от незнакомых людей.

Пример 1

Вы получаете электронное письмо.

Незнакомый человек просит вас помочь получить наследство.

Человек обещает вам за помощь много денег.

Что делать

Сразу удалите письмо.

Не верьте тем, кто предлагает вам много денег.

Если вы согласитесь помогать, вы потеряете много денег.

Пример 2

Вы получаете электронное письмо.

В письме вам предлагают пройти опрос.

Вам обещают выдать приз.

Чтобы получить приз, нужно заплатить деньги.

Что делать

Не платите деньги.

Если опрос настоящий, вам **не нужно** платить деньги.

Только мошенники просят заранее платить деньги.

7 Мошенники могут предлагать вам работу

В интернете вам предлагают устроиться на работу.

Вам предлагают большую зарплату.

Вас просят заранее оплатить услуги по устройству на работу:

- вы должны оплатить оформление документов
- вы должны оплатить пропуск на территорию организации
- вы должны купить обучающие материалы
- вы должны заплатить за обучение

Не надо платить.

Вы потеряете ваши деньги.

Вы **не получите** работу.

Помните!

Организации **не берут** деньги у будущих работников.

Только мошенники просят заплатить при устройстве на работу.

Чтобы устроиться на настоящую работу:

- вам **не нужно** платить за обучение
- вам **не нужно** покупать продукцию
- вам **не нужно** платить за трудоустройство

8 Мошенники могут говорить, что они представители банков и государственных организаций

Мошенник может представиться сотрудником вашего банка.

Мошенник может представиться сотрудником государственной организации.

Мошенники могут позвонить вам по телефону.

Мошенники могут прийти к вам домой.

Мошенники подделывают официальные документы, чтобы вы им поверили.

Будьте внимательны!

Не верьте незнакомым людям, если они звонят вам и что-то спрашивают.

Не открывайте дверь незнакомым людям!

Пример 1

Вы получаете СМС-сообщение.

В сообщении написано, что ваша банковская карта заблокирована.

Если банковская карта заблокирована, она **не работает**.

В сообщении есть номер телефона.

Вам предлагают позвонить в банк по этому номеру телефона.

Вы звоните по этому номеру.

Вам отвечают мошенники.

Мошенники спрашивают у вас информацию вашей банковской карты.

Что делать

Никому **не говорите** информацию вашей банковской карты.

Не звоните по номеру телефона в сообщении.

Позвоните в банк.

Номер телефона банка есть на вашей банковской карте.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Сотрудник банка поможет вам.

Пример 2

К вам домой приходит человек.

Человек говорит, что он социальный работник.

Он рассказывает вам про новый прибор.

Человек говорит, что этот прибор дорого стоит.

Он предлагает вам купить прибор за небольшие деньги.

Что делать

Не покупайте ничего у чужих людей, которые пришли к вам домой.

Вы потеряете ваши деньги.

Не пускайте чужих людей в дом, если вы их **не приглашали**.

Чужие люди могут обмануть вас.

Чужие люди могут украсть у вас деньги и вещи.

Правила безопасности

Когда вы пользуетесь банковской картой:

- **не оставляйте** вашу банковскую карту без присмотра
- **не передавайте** никому вашу банковскую карту
- никому **не говорите**, **не показывайте** и **не пишите** ПИН-код вашей банковской карты
- никому **не сообщайте** информацию, которую вы получили от банка

Сотрудник банка **не имеет права** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

При любых проблемах с вашей банковской картой срочно звоните в банк.

Телефон банка есть на обороте вашей банковской карты.

Телефон банка вы можете найти на сайте вашего банка.

Используйте банкоматы в безопасных местах.

Не открывайте файлы и ссылки из незнакомых источников.

Установите антивирус на ваших устройствах.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Когда вы пользуетесь интернетом, **не пользуйтесь** публичным Wi-Fi.

Wi-Fi – это беспроводной интернет.

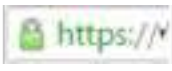
Публичный Wi-Fi – это беспроводной интернет в общественном месте.

Пользуйтесь только безопасными сайтами.

Адрес безопасного сайта начинается так:

https://

В адресной строке безопасного сайта вы увидите значок в виде замка:



Знак безопасного сайта

Загружайте приложения для смартфона только с официальных сайтов.

Приложение с другого сайта может содержать вредные программы.

Будьте внимательны, когда загружаете банковские приложения на смартфон.

Обращайте внимание, кто создал банковское приложение.

Официальные банковские приложения создаёт сам банк.

Не загружайте приложения от других организаций.

Оплачивайте покупки только на сайтах с защищённым соединением.

На этих сайтах должен быть значок платёжной системы вашей банковской карты.

Если на сайте нужно ввести ваши личные данные, будьте осторожны.

Если вам звонят незнакомые люди.

Будьте внимательны! Проверяйте информацию.

Позвоните в организацию по официальному номеру телефона.

Номер телефона вы можете найти на сайте организации.

Если вам сообщили о блокировке банковской карты, позвоните в ваш банк.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Телефон банка есть на обратной стороне вашей банковской карты.

Телефон банка вы можете найти на сайте банка.

Адрес сайта банка вы можете найти на сайте Банка России:
http://cbr.ru/banking_sector/credit/FullCoList

Никогда **не спешите** платить деньги.

Спокойно подумайте.

Посоветуйтесь с близким человеком.

Если вас обманули, сразу обратитесь в полицию.

Словарь

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Банковская карта позволяет вам пользоваться деньгами с вашего банковского счёта.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Банкомат – аппарат для приёма и выдачи наличных денег.

Вложенный файл – документ, который приходит в сообщении.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Защитный код (CVV/CVC-код) — 3 цифры на оборотной стороне вашей банковской карты.

Личные данные – это информация из ваших документов.

Мобильный банк – это способ управления вашим банковским счетом через СМС-сообщения.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенничество – обман людей с целью украсть их деньги.

Одноразовый пароль вы можете использовать только один раз.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль банковской карты.

ПИН-код нужен, чтобы пользоваться банковской картой.

ПИН-код – это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Поддельный сайт очень похож на настоящий сайт организации, но имеет другой адрес в интернете.

Поддельные сайты создают мошенники.

Публичный Wi-Fi – беспроводной интернет в общественном месте.

СМС-сообщение (СМС) – это текстовое сообщение в мобильном телефоне.

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Wi-Fi – это беспроводной интернет.

Запомните!

Не бойтесь просить помощи, если вы в чём-то не уверены.

Кто может помочь вам понять финансовые вопросы?

Куда вы можете обратиться за дополнительной информацией?

Вы можете получить помощь и узнать ответы на ваши вопросы здесь:

- **Ваша семья и ваши друзья**
- **Ваш банк**
  Вы можете написать свои вопросы на сайте банка.
  Вы можете позвонить в ваш банк по телефону. Контактные данные вы можете найти на сайте банка в интернете.
  Вы можете прийти в офис банка и задать вопросы сотруднику банка.

Банк России

Вы можете задать вопрос в чате мобильного приложения «ЦБ онлайн».

Вы можете позвонить по телефону:
8-800-300-30-00

АНО «Наш Солнечный Мир»

Вы можете прислать вопросы по электронной почте: info@solnechnymir.ru

Сайт «Финансовая культура»:
www.fincult.info/feedback

Вы можете найти ответ на ваш вопрос
на этом сайте.
Вы можете написать вопрос на этом сайте.

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

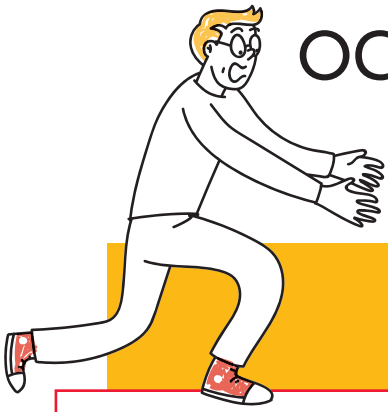
Как обезопасить свои деньги в интернете?

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

ОСТОРОЖНО: МОШЕННИКИ!



Вам звонят из банка и просят сообщить персональные данные или информацию о карте/счете — БУДЬТЕ БДИТЕЛЬНЫ, ЭТО МОГУТ БЫТЬ МОШЕННИКИ!

Злоумышленники с помощью специальных технологий могут сделать так, что на экране вашего телефона высветится официальный номер банка.

Они могут обратиться к вам по имени-отчеству и попросить секретные сведения о карте или счете. Например, чтобы остановить подозрительную операцию.

В ЧЕМ ОПАСНОСТЬ И ЧТО ДЕЛАТЬ?

Узнав нужную информацию, преступник может украсть ваши деньги.

- Не говорите и не вводите ПИН-код, трехзначный код с обратной стороны карты, или одноразовый пароль из СМС.
- Не набирайте на телефоне никаких комбинаций и не переходите по ссылкам.
- Положите трубку. Позвоните в банк по официальному номеру — он есть на сайте или обратной стороне карты.
- Самостоятельно наберите номер на клавиатуре телефона. Не перезванивайте обратным звонком, вы можете снова попасть к мошенникам.

ПРАВИЛА
ФИНАНСОВОЙ БЕЗОПАСНОСТИ

1 Звоните в банк сами

Набирайте номер вручную. Телефон горячей линии указан на обратной стороне карты и на официальном сайте банка.

Перезванивая на номер, с которого пришел звонок или сообщение, вы рискуете снова попасть к мошенникам.

2 Сосредоточьтесь

Если банк выявит подозрительную транзакцию, он приостановит ее на срок до двух суток.

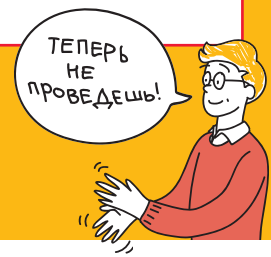
У вас есть 48 часов, чтобы спокойно принять решение: подтвердить или отменить операцию.

3 Не говорите никому секретные коды

Если вас убеждают продиктовать или ввести CVC/CVV-код на обратной стороне карты, пин-код или коды из СМС – это мошенники!

Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

Подробнее о том, как защититься от киберкраж и финансовых мошенников, читайте на сайте **fincult.info**



Банк России

Контактный центр Банка России:
8 800 300-30-00
(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:
www.cbr.ru/reception

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

СМС, МЕССЕНДЖЕРЫ, СОЦСЕТИ

Вам пришло СМС от банка с информацией:
- **о заблокированном платеже или карте;**
- **о выигрыше;**
- **об ошибочном переводе на ваш банковский счет или мобильный телефон с просьбой вернуть деньги.**

— Что делать?

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКЕ И НЕ ПЕРЕЗВАНИВАЙТЕ!

Проверьте информацию, позвонив в банк по номеру, который указан на вашей банковской карте.

Знакомый в соцсетях просит дать в долг или перевести деньги на лечение.

— Что делать?

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ СРАЗУ!

Перезвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страницу взломали.

Контактный центр Банка России

8 800 300-30-00
(бесплатно для звонков из регионов России)

+7 499 300-30-00
(в соответствии с тарифами вашего оператора)

300
(бесплатно для звонков с мобильных телефонов)

Все представленные номера доступны для звонков круглосуточно

Банк России не совершает исходящих звонков с указанных номеров

fincult.info
ПОРА УЗНАТЬ ПРО ДЕНЬГИ ВСЕ

Банк России

ОСТОРОЖНО: МОШЕННИКИ!

НИКОГДА
НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ ЛЮДЯМ ТРЕХЗНАЧНЫЙ КОД НА ОБОРОТЕ КАРТЫ, PIN-КОД И ПАРОЛИ ИЗ СМС

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Спрашивают данные карты.

— Что делать?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ — ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.

Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

— Что делать?

НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят совершить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.

Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

— Что делать?

ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

ИНТЕРНЕТ

Предлагают вложить деньги на очень выгодных условиях.

— Что делать?

ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.

На сайтах с объявлениями («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

— Что делать?

НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.

Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

— Что делать?

ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись **https://** и **«замочек»** в адресной строке браузера.

СМС, МЕССЕНДЖЕРЫ, СОЦСЕТИ

Вам пришло СМС от банка с информацией:
- **о заблокированном платеже или карте;**
- **о выигрыше;**
- **об ошибочном переводе на ваш банковский счет или мобильный телефон с просьбой вернуть деньги.**

— Что делать?

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКЕ И НЕ ПЕРЕЗВАНИВАЙТЕ!

Проверьте информацию, позвонив в банк по номеру, который указан на вашей банковской карте.

Знакомый в соцсетях просит дать в долг или перевести деньги на лечение.

— Что делать?

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ СРАЗУ!

Перезвоните своему знакомому, чтобы выяснить ситуацию, — возможно, его страницу взломали.

Контактный центр Банка России

8 800 300-30-00
(бесплатно для звонков из регионов России)

+7 499 300-30-00
(в соответствии с тарифами вашего оператора)

300
(бесплатно для звонков с мобильных телефонов)

Все представленные номера доступны для звонков круглосуточно

Банк России не совершает исходящих звонков с указанных номеров

fincult.info
ПОРА УЗНАТЬ ПРО ДЕНЬГИ ВСЕ

Банк России

ОСТОРОЖНО: МОШЕННИКИ!

НИКОГДА
НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ ЛЮДЯМ ТРЕХЗНАЧНЫЙ КОД НА ОБОРОТЕ КАРТЫ, PIN-КОД И ПАРОЛИ ИЗ СМС

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Спрашивают данные карты.

— Что делать?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ — ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.

Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

— Что делать?

НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят совершить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.

Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

— Что делать?

ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

ИНТЕРНЕТ

Предлагают вложить деньги на очень выгодных условиях.

— Что делать?

ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.

На сайтах с объявлениями («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

— Что делать?

НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.

Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

— Что делать?

ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись **https://** и **«замочек»** в адресной строке браузера.

ЧИТАЙТЕ ТАКЖЕ НА САЙТЕ FINCULT.INFO

Личные финансы:
С чего начать путь инвестора?
Как распознать финансовую пирамиду?
Для чего вести учет доходов и расходов?

Малый бизнес:
Как получить кредит на бизнес?
Как начать свое дело и преуспеть?
Как открыть ИП и не запутаться в документах?

Понятная экономика:
Почему растут цены?
Кто решает, сколько стоит валюта?
Почему нельзя напечатать денег, чтобы всем хватило?

Банк России

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЗАЩИТИТЕ СЕБЯ И СВОЮ СЕМЬЮ

Кто охотится за вашими деньгами?
Как распознать мошенников?
Что делать, если вас все-таки обманули?

Контактный центр Банка России

8 800 300-30-00

(для бесплатных звонков из регионов России)

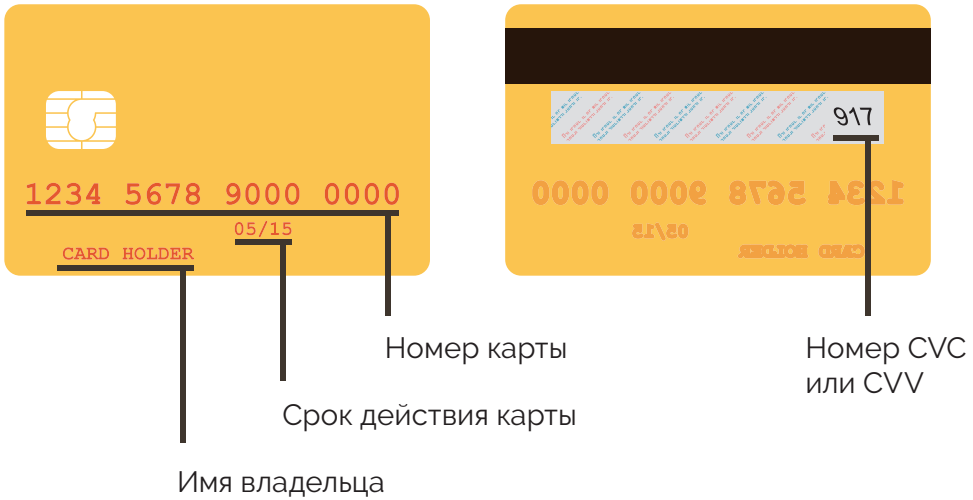
Интернет-приемная Банка России
cbr.ru/reception

fincult.info — сайт для тех, кто думает о будущем

Мошенники умеют выманивать деньги по телефону, в социальных сетях и офисах. Как они это делают?

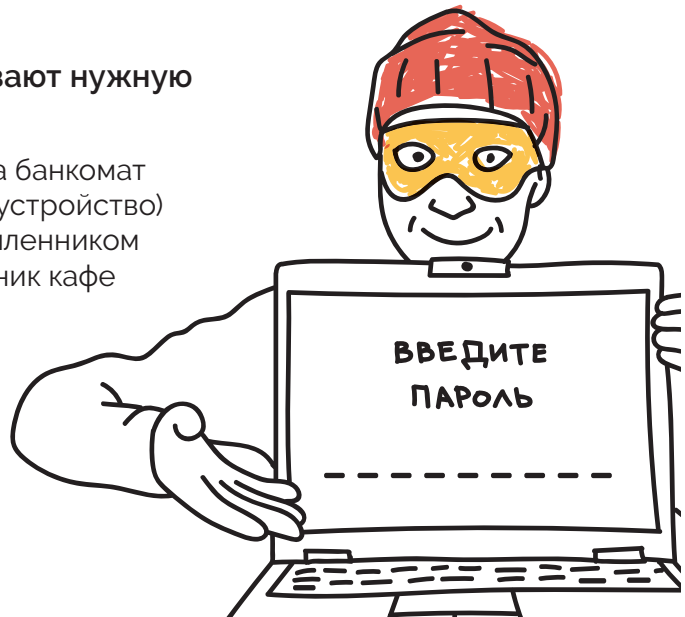
МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам нужны ваши данные:



Как мошенники добывают нужную информацию?

Они могут установить на банкомат скиммер (считывающее устройство) и видеокамеру. Злоумышленником может оказаться сотрудник кафе или магазина, который получит доступ к вашей карте хоть на пять секунд.



БИНАРНЫЕ ОПЦИОНЫ

Не связывайтесь с бинарными опционами. Кажется, все просто: нужно открыть счет и делать ставки на рост или падение стоимости валют. Если угадали, вы зарабатываете, если нет — теряете деньги.

Но сегодня в интернете нет площадок, на которых могут проводиться эти сделки, поэтому все обещания о легком заработке на бинарных опционах — мошенничество.

Вы просто потеряете деньги.

Если вы все же решили выйти на рынок Форекс, внимательно изучите закон и «Базовый стандарт совершения операций на финансовом рынке при осуществлении деятельности форекс-дилера».

У форекс-дилера обязательно должна быть лицензия. Уточнить, есть ли она, можно на сайте Банка России.

Компания должна быть зарегистрирована в России, а не в офшорных зонах.

Предупредите пожилых родственников, что агрессивная реклама быстрого заработка в интернете — мошенничество и на деле обернется потерей денег.

А еще лучше — не рискуйте, попробуйте начать путь инвестора на бирже.

Если вы стали жертвой мошенничества на финансовых рынках

Соберите все документы (договоры, заключенные с посредником, чеки на перевод денег), сделайте скриншоты с сайта — и обратитесь в полицию.

Сообщите в Банк России.

КАК УБЕРЕЧЬСЯ ОТ ОБМАНА

Финансовая организация должна иметь лицензию Банка России. Сверьтесь со Справочником участников финансового рынка на сайте cbr.ru.

Проверьте компанию в Едином государственном реестре юридических лиц ФНС России.

Запросите образцы договоров, копии документов. Проконсультируйтесь с юристом.

Я ВЛОЖИЛСЯ И ПРОГОРЕЛ. ЧТО ДЕЛАТЬ?

Составьте претензию и направьте ее в адрес компании.

Если компания отказывается вернуть деньги, соберите все документы и обратитесь в полицию.

Свяжитесь с юристом и попробуйте найти других жертв мошенничества.

МОШЕННИКИ НА РЫНКЕ ФОРЕКС

Торговля на рынке Форекс — риск, гарантий нет, больше шансов потерять все, чем сорвать куш. Но опасность кроется и в посредниках. Чтобы обычному человеку выйти на рынок Форекс, нужно заключить договор с посредником, форекс-дилером, и торговать через него. Можно нарваться на мошенников, которые возьмут у вас деньги и не вернут их.

КАК НЕ ПОПАСТЬСЯ

Осмотрите банкомат. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.

Набирая ПИН-код, прикрывайте клавиатуру рукой.

Подключите мобильный банк и СМС-уведомления.

Если совершаете покупки через интернет, никому не сообщайте секретный код из СМС.

Никогда не теряйте из виду вашу карту.

МЕНЯ ОБОКРАЛИ. ЧТО ДЕЛАТЬ?

Позвоните в банк (номер есть на обороте карты или на главной странице сайта банка) и заблокируйте карту.

Запросите выписку по счету и напишите заявление о несогласии с операцией.

Обратитесь с заявлением в полицию.

КИБЕРМОШЕННИЧЕСТВО

Вам приходит СМС или письмо «от банка» со ссылкой, просьбой перезвонить или уведомлением о крупном выигрыше. Или звонят «из банка» и просят сообщить личные данные. Или пишут в социальных сетях от имени родственников или друзей, которые попали в беду, и просят перевести деньги на неизвестный счет. Скорее всего, вы имеете дело с мошенниками.

КАК НЕ ПОПАСТЬСЯ

Главное правило — не торопитесь и всегда проверяйте информацию.

Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам.

Никому не сообщайте личные данные (из паспорта и других документов) и полные данные карты, включая три цифры с оборота и срок действия.

Не храните реквизиты карт и личные данные на компьютере или в смартфоне и не вводите их на подозрительных сайтах.

Скачивайте приложения только в официальных онлайн-магазинах.

Установите и регулярно обновляйте антивирусы на всех устройствах.

Не пользуйтесь непроверенными сетями Wi-Fi.

Расскажите про эти простые правила своим родственникам и знакомым.

С МОЕЙ КАРТЫ ОБМАНОМ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

Позвоните в банк (номер есть на обороте карты или на главной странице сайта банка) и заблокируйте карту.

Запросите в банке выписку по счету и напишите заявление о несогласии с операцией.

Обратитесь с заявлением в полицию.

ФИНАНСОВЫЕ ПИРАМИДЫ

Они маскируются под микрофинансовые организации, инвестиционные и управляющие предприятия, онлайн-казино. Заявляют о высоких процентах по вкладам и отсутствии рисков, гарантируют доход (что запрещено на рынке ценных бумаг), обещают помощь людям с плохой кредитной историей.

Заработать на пирамидах нельзя. Если вы вложите деньги, вы их потеряете.

ЧЕРНЫЕ КРЕДИТОРЫ

ВЫВОДИМ ЗЛОУМЫШЛЕННИКОВ НА ЧИСТУЮ ВОДУ

У кого есть право выдавать кредиты?
Как отличить нелегальных кредиторов от легальных?
Что делать, если ваш кредитор оказался черным?

КТО МОЖЕТ ВЫДАВАТЬ КРЕДИТЫ?

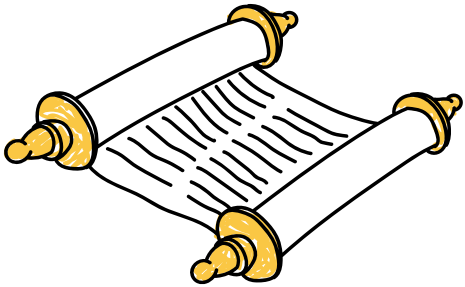
Быть профессиональным кредитором, то есть выдавать кредиты и займы в денежной форме, **могут только:**

банки

микрофинансовые организации (МФО)

кредитные потребительские кооперативы (КПК и СКПК)

ломбарды



Для этого у них должно быть специальное разрешение Банка России.

КТО ТАКИЕ ЧЕРНЫЕ КРЕДИТОРЫ?

Если у компании нет разрешения Банка России на выдачу кредитов (или лицензии у банка), а она все равно привлекает клиентов, выдает себя за лицензированную и кредитует потребителей, то перед вами нелегальный (или черный) кредитор.

Нелегальные кредиторы могут действовать по-разному. Например, выдавать кредиты под очень высокие проценты, но при этом не прибегать к откровенному криминалу. А могут использовать преступные схемы, чтобы обманом завладеть деньгами и имуществом клиентов.

БЕРИТЕ КРЕДИТ ИЛИ ЗАЕМ ТОЛЬКО У ЛЕГАЛЬНОГО КРЕДИТОРА

Деятельность легальных кредиторов регулируется законом. Также ограничены способы, которыми кредиторы могут взыскать долг. Черные кредиторы используют черные же методы взыскания: запугивание, угрозы, разговоры с вашими родственниками, коллегами, друзьями и соседями. А иногда долги выбивают — в прямом смысле этого слова.

ЕСЛИ КРЕДИТ НЕ ДАЮТ ЛЕГАЛЬНО

Случается, что люди сознательно идут к нелегальным кредиторам, потому что легально получить кредит им не удается. Этого делать нельзя.

Почему?

Финансовую проблему такой заем не решит, а усугубит, ведь проценты по черному кредиту очень высоки.

Есть риск потерять не только деньги, но и нервы, а в некоторых случаях и здоровье.

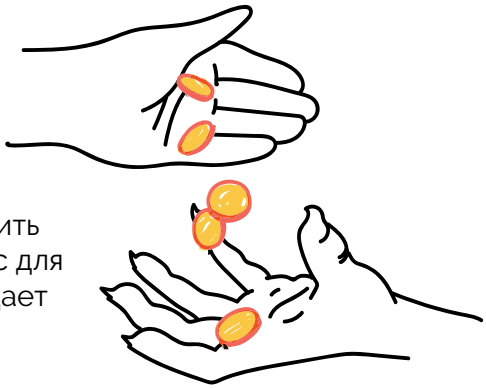
КАК ЧЕРНЫЕ КРЕДИТОРЫ ОБМАНЫВАЮТ КЛИЕНТОВ?

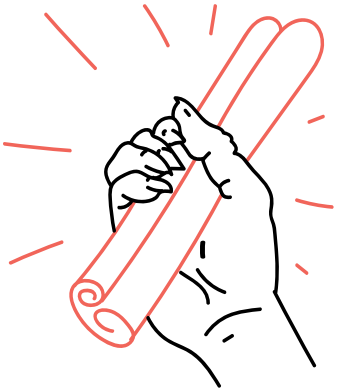
Часто заемщики не подозревают, что перед ними нелегальная организация. Вот три самые популярные схемы, по которым мошенники привлекают невнимательных клиентов.

1

Предоплата за кредит

Кредитор просит оплатить проверку кредитной истории или страховку, берет комиссию за выдачу кредита, предлагает оплатить услуги нотариуса или членский взнос для вступления в кооператив. Клиент отдает деньги — и «помощник» исчезает.





2

Использование данных

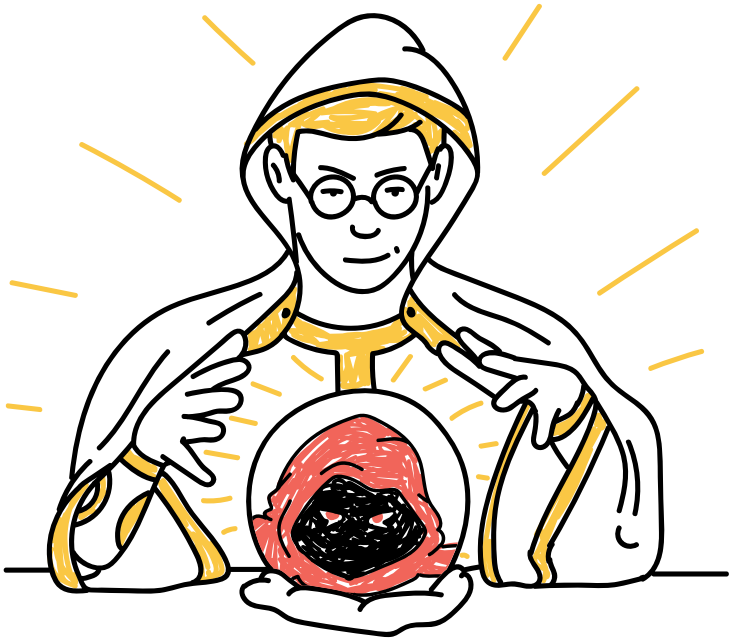
Клиент приносит в организацию полный пакет документов. Мошенники могут взять кредит от его имени или обнулить его счета.

3

Сомнительные бумаги

Мошенники могут подменить договор и дать клиенту на подпись другие условия, где, например, не указан срок возврата. Это позволит им запросить всю сумму с процентами уже на следующий день.

КАК РАСПОЗНАТЬ ЧЕРНОГО КРЕДИТОРА?



ПРОВЕРЬТЕ, ЕСТЬ ЛИ КОМПАНИЯ В РЕЕСТРЕ НА САЙТЕ БАНКА РОССИИ

Если компании нет в Справочнике по кредитным организациям или в Справочнике участников финансового рынка на сайте Банка России — это нелегальный кредитор. Но даже если вы нашли название компании в списке, будьте внимательны.

Мошенники могут подделать сайт, используя название легальной компании. Поэтому пользоваться финансовыми услугами онлайн следует особенно осмотрительно.

НЕ СОБЛАЗНЯЙТЕСЬ ЗАМАНЧИВЫМ ПРЕДЛОЖЕНИЕМ

Если вам предлагают подозрительно выгодные условия, убедитесь, что в договоре действительно прописаны все обещания, которые сулит реклама.

Не берите кредит, если формулировки двусмысленны или противоречат тому, что написано в рекламе.

Проконсультируйтесь с юристом, если вы не можете понять, что именно написано в документах.

ВНИМАТЕЛЬНО ЧИТАЙТЕ ДОГОВОР

В документах легального кредитора должны быть четко прописаны порядок заключения договора, выдачи кредита или займа, условия его возврата или использования. И по закону кредитор обязан выдать вам документы или хотя бы ознакомить вас с ними.

По закону можно взять документы домой и подумать в течение пяти дней. Условия договора за это время не поменяются.

Черному кредитору невыгодно давать время на раздумье. Он будет уговаривать вас подписать договор немедленно, убеждать, что это самое выгодное предложение и завтра его уже не будет.

Если вам чересчур настойчиво предлагают кредит или заем, это повод задуматься, стоит ли подписывать договор.

ЕСЛИ ВЫ СТОЛКНУЛИСЬ С ЧЕРНЫМ КРЕДИТОРОМ

Если кредитор не указан в реестре на сайте Банка России или указан, но нарушает правила — обратитесь в интернет-приемную Банка России и подайте заявление в правоохранительные органы.

Если черные кредиторы пытаются взыскать с вас просроченную задолженность, выдавая себя за коллекторов или поручив это им на самом деле, вы можете обратиться в Федеральную службу судебных приставов.

Черным кредиторам только на руку, если пострадавшие от их незаконных действий будут по тем или иным причинам умалчивать о случившемся.

Не верьте, когда вас убеждают, что обращаться за защитой ваших прав бесполезно.

ЧИТАЙТЕ ТАКЖЕ НА САЙТЕ FINCULT.INFO

Личные финансы:
Давать ли детям карманные деньги?
Что такое санация банка?
Как накопить на мечту?

Малый бизнес:
Зачем нужен факторинг?
Что можно взять в лизинг?
Как участвовать в госзакупках?

Понятная экономика:
Как считают инфляцию?
Что такое монетарная политика?
Чем занимается центробанк страны?

Банк России

Контактный центр Банка России

8 800 300-30-00

(для бесплатных звонков
из регионов России)

Интернет-приемная
Банка России
cbr.ru/reception

fincult.info — сайт
для тех, кто думает
о будущем

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

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

КОДОВОЕ СЛОВО
называйте только сотруднику банка, когда сами звоните на горячую линию

НЕ ПУБЛИКУЙТЕ
персональные данные в открытом доступе

УСТАНОВИТЕ
антивирусы на все устройства

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

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура