МИНФИН РОССИИ 220 лет

Российский экономический университет имени Г. В. Плеханова

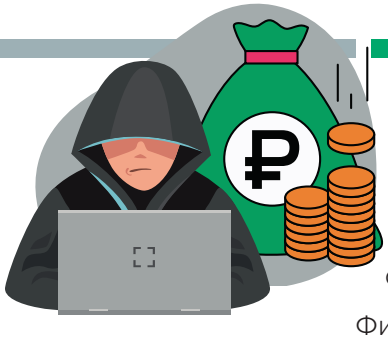
ПРЕДУПРЕЖДЕН – ЗНАЧИТ ВООРУЖЕН!

ЗАЩИТА ОТ МОШЕННИЧЕСТВА

У меня лично есть четыреста сравнительно честных способов отъема денег у населения.

Остап Бендер

(Ильф И., Петров Е. «Золотой телёнок»)



Каким бы ни было общество, всегда найдется кто-то, кто захочет присвоить себе чужое имущество вместо того, чтобы честно трудиться самостоятельно. Увы, с этим неприятным фактом можно только смириться, а точнее, принять его во внимание.

Финансовое мошенничество не является исключением: несмотря на все усилия правоохранительных органов, оно остается серьезной угрозой для финансового благополучия граждан и злоумышленникам нередко удается воплощать свои преступные планы, избегая законного наказания. Но есть и хорошие новости: в силу своих особенностей мошенничество относится к тем видам преступлений, от которых человек способен успешно защищаться самостоятельно. Руководствуясь простыми правилами, можно обезопасить себя практически от любых мошеннических посягательств на свое имущество и деньги.

Как же распознать злоумышленников и защитить себя от их действий?

Как действуют мошенники

Прежде всего мошенничество – это весьма специфический вид преступления. Нередко его считают родственным краже, однако между этими правонарушениями есть одно важное различие:

- кража происходит незаметно для жертвы, без ее ведома и участия;
- жертва мошенничества сама отдает свое имущество злоумышленнику, причем делает это добровольно и осознанно.

Чтобы добиться своих целей, мошенники используют обман, манипулирование и другие психологические приемы, при помощи которых они стараются усыпить бдительность своей жертвы и заставить ее добровольно расстаться со своим имуществом. То есть жертва мошеннических действий всегда так или иначе помогает злоумышленникам – в противном случае они не смогут добиться своих целей.

И это позволяет нам сделать два важных вывода (условно «плохой» и «хороший»):

1. Очень часто гражданин сам виноват в том, что стал жертвой мошенников.

2. Злоумышленников можно легко «оставить с носом», если правильно вести себя и не поддаваться на их уловки.

ВАЖНО!

Уголовный кодекс РФ устанавливает ответственность за мошенничество, однако необходимо помнить, что только суд может признать гражданина или организацию мошенником.

Существует огромное количество видов финансового мошенничества. Более того, злоумышленники продолжают изобретать все новые и новые мошеннические схемы. Однако в конечном итоге все их действия строятся на одних и тех же основных способах, которые часто комбинируются друг с другом.

Этих способов всего ТРИ:

1 Игра на определенных качествах личности и чертах характера потенциальных жертв.	Чаще всего мошенники делают ставку на жадность, тщеславие, страх, легкомыслие, доверчивость, недостаток ответственности, азарт, опасение упустить свой шанс. При этом злоумышленники умело манипулируют людьми с этими качествами.
2 Использование недостаточной финансовой грамотности потенциальных жертв, незнания ими законов существования финансового мира.	Многие мошеннические схемы построены на предложениях, заведомо невозможных в условиях современной экономики (например, очень высокие доходы от вложений, очень низкие ставки по кредитам и т. д.). Если потенциальная жертва этого не знает, она может попасть на удочку злоумышленников.
3 Применение сложных и современных технологических средств.	Мошенники могут не только подделать документы, но и создать фальшивый интернет-сайт компании или, к примеру, сделать так, чтобы при звонке жертве на ее телефоне отобразился настоящий телефонный номер того банка, от имени которого они совершают звонок.

Зная эти основные методы действия злоумышленников, можно вывести определенные модели поведения, соблюдение которых позволит вам надежно уберечь себя и своих близких от мошеннических действий.

Как вести себя, чтобы не стать жертвой мошенников?

Вот несколько несложных советов, которые помогут вам «оставить с носом» любых злоумышленников, пытающихся завладеть вашим имуществом при помощи мошеннических схем:

ВАЖНО!

Стоит помнить, что мошенничество может подстерегать нас практически везде, поэтому необходимо сохранять бдительность. Безопасности много не бывает, и лучше «подуть на холодное, чем обжечься на горячем».

1 Следует всегда быть готовыми к тому, что вы можете столкнуться с мошенниками.

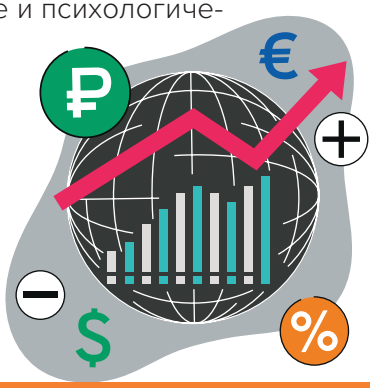
Большинство мошеннических схем построено на использовании эффекта неожиданности. Даже простая готовность к возможному появлению злоумышленников на вашем пути ощутимо снижает их шансы на успех.

2 Необходимо во всех ситуациях сохранять критическое мышление, хладнокровие и здравый смысл.

Чаще всего усилия злоумышленников направлены именно на то, чтобы сбить вас с толку, усыпить вашу бдительность и заставить принять необдуманное решение. Хладнокровие и здравый смысл – универсальное оружие против большинства злоумышленников, делающих ставку на обман, доверие и психологическое манипулирование.

ВАЖНО!

Если на вас оказывают психологическое давление, запугивают, настойчиво пытаются убедить в чем-то или заставить срочно что-то сделать, дать согласие, оплатить что-то и т. д., вы наверняка имеете дело с мошенниками!



3 Нужно знать основные законы и принципы экономики.

Многие мошеннические схемы на финансовом рынке построены на предложениях или требованиях, которые заведомо невозможны просто потому, что так устроен современный финансовый мир. Зная, как этот рынок функционирует, можно распознать множество преступных схем буквально с первого взгляда.

ВАЖНО!

Современная экономика не предполагает никаких законных способов быстрого получения большого дохода. Бесплатных кредитов не существует. Никакая организация не может гарантировать вам доход от вложения денег в ту или иную деятельность. Зная эти и подобные правила, можно легко «отсечь» множество злоумышленников.

4 Относитесь критически к любым особо «привлекательным» финансовым предложениям.

Бесплатный сыр бывает только в мышеловке, и никто не будет давать вам возможность заработать просто «по доброте душевной». Сталкиваясь с такими предложениями, самое лучшее – игнорировать их.

ВАЖНО!

Особо низкие ставки по кредитам, необычайно дешевые товары или услуги, сообщение о выигрыше в лотерею, в которой вы не участвовали, неожиданные предложения крупных выплат от каких-либо фирм или ведомств – все это и многое другое активно применяется злоумышленниками.

5 Некоторые личностные качества стоит всегда держать в узде. Злоумышленники ориентируются в первую очередь на людей, обладающих определенным складом мышления и определенными чертами характера.

Главным образом речь идет о жадности, зависти, доверчивости или азарте, но не ограничивается только ими.

ВАЖНО!

Помимо прочего, необходимо осознавать меру собственной ответственности за свои финансовые решения, а также свою роль в действиях злоумышленников. К примеру, банк не возместит вам деньги на счете, если вы потеряли их по собственной вине, добровольно назвав мошенникам секретные данные своей банковской карты, или сами, без принуждения, перевели их на счет злоумышленника.

6 **При возникновении любых подозрений всегда проверяйте человека или финансовую организацию, с которой вы общаетесь.**

Достаточным оружием для защиты от большого числа злоумышленников является следование принципу «доверяй, но проверяй».

ВАЖНО!

Все финансовые организации (банки, финансовые посредники, страховые компании, ломбарды и т. д.) должны иметь лицензию Банка России на ведение своей деятельности. Ее наличие можно проверить на интернет-сайте Банка России. Стоящий за дверью квартиры сотрудник ЖЭКа должен иметь удостоверение, но и оно может быть поддельным, поэтому лучше позвонить в ЖЭК и проверить. Никогда не стесняйтесь это делать!

7 **Берегите свои персональные данные.**

Учитывайте, что злоумышленники могут за ними охотиться. Знайте, кто и в каком объеме вправе требовать от вас ваши личные данные (серию и номер паспорта, данные вашего банковского счета, банковской карты и т. д.). При первых подозрениях на кражу этих данных немедленно обращайтесь в свой банк и правоохранительные органы.

ВАЖНО!

Никто (даже полиция и прокуратура) и никогда не имеет права требовать у вас секретные данные вашей банковской карты (PIN-код, CVC/CVV-код с обратной стороны карты или проверочный код из SMS-сообщения).

8 **Старайтесь быть в курсе новых методов финансового мошенничества.**

Например, нелишним будет регулярно просматривать новости в сети Интернет, посвященные данной теме. Предупрежден – значит вооружен.

Соблюдение этих правил является надежным средством защиты практически от любого вида мошенничества. Выработка привычки следовать им может занять время и потребовать определенного упорства, но результат – безопасность вашего имущества – определенно того стоит!

ВАЖНО!

Как только новый способ мошенничества становится известен правоохранителям или Банку России, они стараются как можно шире распространить эту информацию, чтобы злоумышленники не смогли использовать эффект неожиданности.

А чтобы научиться еще эффективнее противостоять злоумышленникам, давайте **рассмотрим несколько наиболее распространенных видов мошенничества и методы защиты от них.**

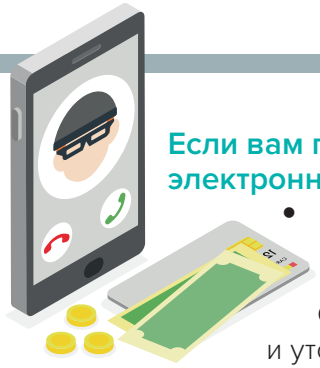
Мошенничество с банковскими картами

Если вы пользуетесь банкоматом

- Отдавайте предпочтение устройствам, установленным в отделениях банков или на закрытых территориях. Избегайте банкоматов в безлюдных местах.
- Сохраняйте внимание при работе с банкоматом. При любых сомнениях нажмите кнопку «Отмена».
- При возникновении технических проблем (к примеру, банкомат не отдает деньги или карту) не поддавайтесь на советы посторонних людей. Позвоните в банк по телефону горячей линии, указанному на банкомате; сообщите о своей проблеме и следуйте указаниям специалиста банка.

Если вы расплачиваетесь картой в магазине или ресторане

- Используя карту для оплаты, старайтесь не упускать ее из вида.
- PIN-код на терминале оплаты следует вводить так, чтобы он не был виден посторонним людям.
- Если произошел сбой оплаты или операция была отклонена, обязательно попросите соответствующий чек (он всегда печатается устройством оплаты).



Если вам поступают неожиданные SMS-сообщения, электронные письма или звонки

- **Вы получили сообщение якобы от родственника или друга, попавшего в беду, с просьбой о переводе денег.**

Свяжитесь с отправителем сообщения напрямую и уточните ситуацию.

- **Вы получили сообщение или письмо от имени вашего банка с информацией о том, что ваша карта заблокирована или перевыпущена.**

Позвоните в свой банк по телефонному номеру, указанному на обратной стороне вашей карты, и выясните, все ли в порядке.

- **Вам звонит «рассеянный человек», который говорит, что по ошибке указал при совершении интернет-платежа ваш номер телефона.**

Он просит сообщить ему код подтверждения, который придет (или только что пришел) на ваш телефон в SMS-сообщении. Игнорируйте этот звонок! В реальности ситуация, описанная этим «рассеянным человеком», невозможна.

Уточните имя и должность собеседника, положите трубку и перезвоните в банк самостоятельно, **НЕПРЕМЕННО набирая телефонный номер банка вручную** (перезванивая автоматическим способом, вы рискуете снова попасть на номер мошенников). Опишите специалисту сложившуюся ситуацию.

ВАЖНО!

- Злоумышленники могут говорить уверенным голосом, использовать психологическое давление, заявляя, что прямо сейчас по вашей карте проводятся подозрительные платежи на большие суммы денег, что к карте получили доступ мошенники и т. д. Кроме того, они могут обратиться к вам по фамилии, имени и отчеству, правильно назвать ваши паспортные данные и данные карты.
- Не поддавайтесь на провокации! Помните о том, что НИКТО и НИКОГДА не может требовать у вас назвать PIN-код карты, CVC/CVV-код или одноразовые пароли из SMS-сообщений. НИКОМУ, кроме злоумышленников, эта информация не может понадобиться!

- **Вам поступает звонок якобы из клиентской службы или службы безопасности вашего банка.**

При этом на вашем телефоне может отобразиться реальный телефон вашего банка, например, 900 для Сбербанка. В разговоре собеседник пытается заставить вас назвать секретные данные вашей банковской карты (PIN-код, CVC/CVV-код, одноразовые пароли из SMS-сообщений, кодовое слово карты).

Вам действительно могут позвонить из вашего банка, если совершенный вами платеж вызывает вопросы у сотрудников его службы безопасности.
У вас могут спросить, действительно ли вы проводили эту операцию, попросить назвать время и способ совершения операции, но никогда не будут спрашивать у вас данные вашей карты, данные паспорта или кодовое слово. Вся необходимая информация у настоящих сотрудников банка уже есть.

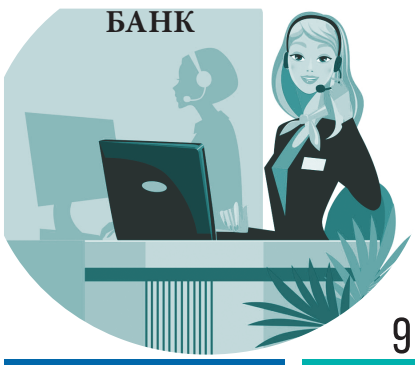
Если вы стали жертвой мошенников:

- обнаружив неожиданное списание денег со счета своей карты, немедленно позвоните в банк по телефону горячей линии (он указан на обороте карты);
- сообщите о случившемся и попросите заблокировать карту;
- затем обратитесь в отделение вашего банка и подайте заявление о несогласии с операцией;
- также обязательно обратитесь в правоохранительные органы с заявлением о хищении ваших средств.

Мошенничество от имени банков и организаций

Если вы получили письмо или телефонный звонок от имени какого-либо ведомства или организации с сообщением о причитающейся вам выплате (каких-либо компенсациях, выигрышах, возмещениях и т. д.), в абсолютном большинстве случаев вы имеете дело с мошенниками.

Позвоните по официальному телефонному номеру ведомства или организации (НЕ из полученного письма) и опишите ситуацию оператору. До этих пор не следуйте никаким указаниям и ничего не оплачивайте.



- Вы можете получить звонок якобы от сотрудников полиции, прокуратуры и других силовых ведомств с сообщением о правонарушениях в отношении вас, о преступлениях ваших родственников и т. п.

Сохраняйте спокойствие. Уточните фамилию и звание собеседника, положите трубку, перезвоните в ведомство по официальному номеру телефона и уточните ситуацию.

- Если в дверь вашей квартиры звонят люди, представляющиеся сотрудниками той или иной службы, и при этом вы их не ждете и не осведомлены о каких-либо плановых проверках, стоит позвонить в данную службу и убедиться, что это действительно «их люди».

Например, если человек представился сотрудником газовой службы, позвоните в диспетчерскую ЖЭКа. До этого ни в коем случае не открывайте дверь. Помимо собственно мошеннических действий, подобный визит может быть прикрытием для разбойного нападения.

ВАЖНО!

К рекламным агентам и продавцам, стучащимся в квартиры, также стоит относиться с осторожностью. Они могут предлагать дешевые товары или услуги по цене дорогих. Кроме того, нередко мошенники обмениваются между собой сведениями о легковерных жертвах и наведываются к ним под разными предлогами, сменяя друг друга.

Что делать, если вы стали жертвой мошенников?

Обратитесь в полицию и детально обрисуйте ситуацию.

Кибермошенничество

Это название носят действия злоумышленников, направленные на хищение личных данных граждан в сети Интернет. Мошенники пытаются выяснить логины и пароли своих жертв на сервисах электронной почты, в социальных сетях, личных кабинетах на сайтах банков и т. д. Используя эти данные, они могут попытаться получить доступ к сбережениям жертвы, взять кредит на ее имя или, к примеру, рассылать рекламу с ее страницы в социальной сети.

Одним из самых распространенных методов действия кибермошенников является фишинг – массовая рассылка электронных писем, сообщений в социальных сетях и мессенджерах.

Распознать фишинговое письмо можно по следующим признакам:

В письме описывается какая-то проблема или срочный вопрос, требующий решения, однако ранее вы ни о чем таком не слышали; еще вариант – вас просят подтвердить действия, которых вы не совершали (например, интернет-заказ или смену пароля).

Вы получили это письмо неожиданно.

Письмо содержит ссылку, по которой вам предлагается пройти, или файл со странным содержанием, который предлагается открыть.

- При получении сообщения, напоминающего фишинговое, имеет смысл связаться с компанией, от имени которой оно отправлено.
- Не используйте для связи телефоны из подозрительного сообщения!
- Не переходите ни по каким ссылкам и не загружайте вложенные файлы из подозрительных или неожиданных сообщений по электронной почте, в соцсетях и мессенджерах.
- Установите на компьютер надежный антивирус.
- Любые приложения и программы для компьютеров следует скачивать только с официальных сайтов разработчиков, а для смартфонов – в магазинах App Store и Google Play.

ВАЖНО!

Даже если вы получили неожиданное сообщение со ссылкой или файлом от знакомого человека, лучше перезвонить ему и проверить, действительно ли именно он отправил вам это сообщение. Есть риск, что от имени вашего знакомого действуют злоумышленники.

Что делать, если вы стали жертвой? При подозрениях на фишинговую атаку немедленно смените пароли своих учетных записей на сервисах, которыми вы пользуетесь. При обнаружении кражи средств с банковских счетов действуйте в соответствии с не раз упомянутой выше схемой: звонок в банк, блокировка банковских карт, заявление о несогласии с операцией, обращение в полицию.

Фальшивомонетничество

- **Изучите и запомните основные признаки подлинности денежных банкнот**, особенно крупных номиналов.

- **Не стесняйтесь проверять подлинность денег в присутствии того, кто передал их вам** (при покупке товара у вас или на сдачу).

Если деньги настоящие, они будут возвращены вам; если поддельные – банк передаст их в полицию, которая начнет расследование. Увы, в этом случае банк не сможет возместить ваши потери, поскольку это должен делать сам мошенник (после того, как он будет найден и осужден судом).

Если вы стали жертвой мошенников, то обратитесь в любой банк и сдайте подозрительные банкноты на проверку.

Финансовые пирамиды

Это особая мошенническая схема, действующая следующим образом: некая организация предлагает гражданам вложить деньги в ее деятельность, обещая большие прибыли; в реальности, однако, эта организация не ведет никакой деятельности, а прибыль своим вкладчикам выплачивает за счет того, что постоянно привлекает все новых и новых вкладчиков. Рано или поздно она обанкротится, а ее организаторы скроются с деньгами обманутых вкладчиков, которые остаются ни с чем.

ВАЖНО!

Финансовые пирамиды могут действовать под видом микрокредитных организаций («Вам отказали в банке? Мы поможем!») или предлагать рефинансирование кредита, взятого в другом месте («Избавим от долгов!»).
Будьте бдительны!

Связываться с финансовыми пирамидами нельзя ни в коем случае. Распознать такую организацию бывает непросто, но есть несколько признаков, указывающих на то, что организация может быть финансовой пирамидой.
Вот они:

Организация обещает (или даже гарантирует) вкладчику огромную прибыль, существенно выше обычной.

Организация ничего не производит и никуда не вкладывает средства (т. е. не ведет деятельности, приносящей доход). Нередко такие организации голословно утверждают, что вкладываются в какую-то современную и очень доходную деятельность, но проверить эти утверждения невозможно.

Организация крайне активно, навязчиво и агрессивно рекламирует себя.

ПРИЗНАКИ ФИНАНСОВОЙ ПИРАМИДЫ

В договорах много недосказанности, расплывчатые формулировки, приписки мелким шрифтом.

Сведений об организации мало или они «мутные».

При возникновении любых сомнений стоит проконсультироваться с квалифицированными людьми (а еще **лучше – посетить юридическую консультацию**).

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ?

- **Если финансовая пирамида еще действует, обратитесь к компании с письменной претензией и потребуйте вернуть ваши деньги** (укажите, что в противном случае вы будете обращаться в полицию).

- **Если организация не отвечает или уже обанкротилась, обратитесь в полицию** с заявлением о наличии в действиях компании признаков состава преступления.

- **Подайте на организацию гражданский иск «О взыскании вложенных денежных средств, неосновательного обогащения, процентов за пользование чужими денежными средствами и компенсации морального вреда».** По возможности стоит найти других жертв пирамиды и действовать сообща (подав коллективный иск).

ВАЖНО!

Любой договор нужно читать очень внимательно, даже если организация, с которой вы его подписываете, заслуживает доверия. Если договор пестрит сложными терминами и неясными формулировками, написанными мелким шрифтом, лучше проявить осторожность.

Кредитное мошенничество

Злоумышленники могут прикидываться легальными кредитными организациями и завлекать жертв, предлагая кредиты на очень выгодных условиях. В реальности, однако, такие кредиты содержат множество дополнительных условий и становятся для жертв долговой ямой. Особенно уязвимыми для этих мошенников становятся граждане, остро нуждающиеся в денежных средствах.

- Не поддавайтесь на излишне привлекательные предложения.
- Пользуйтесь услугами только легальных кредитных организаций (банков, микрокредитных организаций, ломбардов и т. д.). Всегда проверяйте наличие у организации действующей лицензии на ведение их деятельности. Это можно сделать с помощью справочников, которые доступны на сайте Банка России.
- Всегда внимательно читайте договор и другие документы, которые подписываете.

ВАЖНО!

Все кредитные организации должны иметь лицензию Банка России на ведение своей деятельности. Их деятельность жестко регулируется законами. Мошеннические организации такой лицензии не имеют.

Если вы стали жертвой мошенников, обратитесь в полицию.

Приложите к заявлению все имеющиеся у вас документы (чем их больше, тем лучше). Старайтесь не поддаваться психологическому давлению и запугиванию со стороны злоумышленников. Если вам кажется, что ваши права нарушила легальная кредитная организация, обращайтесь за помощью в Банк России (https://cbr.ru/).

cbr.ru

Страховое мошенничество

По возможности пользуйтесь услугами только проверенных страховых компаний.

Если страховая компания вам неизвестна, проверьте наличие у нее лицензии на ведение данной деятельности (это можно сделать на сайте Банка России **https://cbr.ru/**).

Если вам предлагает свои услуги страховой агент (к примеру, пришедший к вам на дачный участок), позвоните в страховую компанию, которую он представляет, и убедитесь, что это действительно их агент. Не стесняйтесь проверять агента в его присутствии!

МОИФИНАНСЫ.РФ

FINGRAM.REA.RU

РЭУ.РФ
ИМЕНИ Г. В. ПЛЕХАНОВА

БУДЬТЕ БДИТЕЛЬНЫ И БЕРЕГИТЕ СЕБЯ!