ПО ЗАКАЗУ МИНИСТЕРСТВА ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации»

Просветительские и информационные материалы по административным и финансовым проблемам инвалидов и лиц с инвалидизирующими заболеваниями

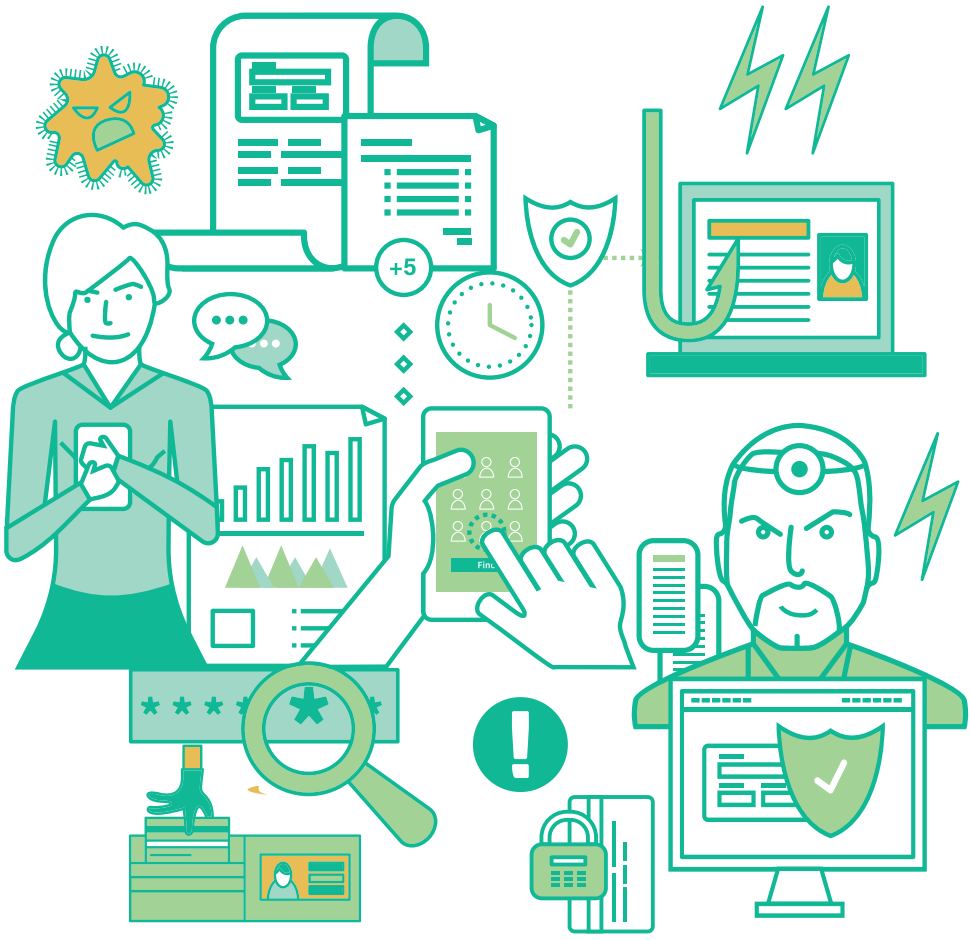
Финансовая безопасность

Дружи с финансами

НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН

Москва, 2018

СОДЕРЖАНИЕ



ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

Большая проблема, с которой сталкиваются семьи, где есть инвалиды I, II, III группы или ребенок-инвалид, – как сохранить собранные на лечение средства в безопасности. К сожалению, очень часто люди, стремящиеся спасти жизни своих близких, становятся жертвами финансовых мошенников, что значительно ухудшает их и без того нелегкую жизненную ситуацию.

Можно выделить следующие основные виды финансовых угроз.

1. Мошенничества с банковскими картами:
   - при использовании банкомата;
   - при оплате покупок и услуг;
   - при оплате через интернет.
2. Мобильные и интернет-мошенники.
3. Финансовые пирамиды.

1. МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Сегодня трудно найти человека, у которого нет банковской карты. На карты государство перечисляет пенсии, пособия и компенсации, с использованием банковских карт заметно упрощается сбор денег на дорогостоящее лечение.

Картами удобно оплачивать покупки в аптеках, лечение в больницах и клиниках, в том числе в других регионах и даже за границей. Карточки избавляют нас от необходимости носить с собой много наличных денег, подвергая себя ненужному риску.

Но и на карте деньги тоже можно потерять. Мошенники проявляют большую изобретательность, пытаясь заполучить доступ к вашему электронному кошельку. Хорошая новость заключается в том, что ваши интересы защищает банк, постоянно совершенствуя методы охраны денежных средств клиентов от электронных грабителей. Однако статистика показывает, что зачастую в исчезновении средств виноваты мы сами – наша невнимательность, доверчивость или беспечность.

Чтобы избежать неприятностей, необходимо знать, как могут украсть деньги с вашей карты, и соблюдать определенные меры безопасности.

Помните, что использование банковских карт, как и наличных средств, требует от вас внимательности, аккуратности и бдительности.

Банковская карта. Внешний вид

Большинство банковских карт выпускаются в соответствии с унифицированным стандартом. Это пластиковый прямоугольник размером 85,6 х 53,98 миллиметра.

ЛИЦЕВАЯ СТОРОНА

Электронный чип
(на некоторых картах может отсутствовать). Традиционно карты с чипами считаются более надежными за счет дополнительного уровня защиты

Имя и фамилия
владельца карты на английском языке

Наименование банка-эмитента

Номер карты
Чаще всего состоит из 16 цифр. Иногда встречаются варианты с 18 цифрами. Реже – другое количество

Срок действия карты

Название платежной системы
Наибольшее распространение получили Visa и MasterCard. Также встречаются Maestro, American Express, «Мир», ПРО100 и ряд других

ОБРАТНАЯ СТОРОНА

Телефон службы поддержки банка-эмитента
(его надо переписать и всегда иметь при себе)

Образец подписи владельца
Обратите внимание, что карты без автографа считаются недействительными и в их приеме может быть отказано

Код проверки подлинности карты
Английская аббревиатура CVV2 для платежной системы Visa и CVC2 для MasterCard. Необходим для подтверждения платежей без физического предъявления банковской карты, как правило, при транзакциях через интернет. Отсутствует на некоторых банковских картах, имеющих ограничения в использовании

ВАЖНО

Для того чтобы совершить платеж по вашей карте, обычно требуется указать следующие реквизиты:

- **номер банковской карты (обычно выгравирован на лицевой стороне). Это не является секретной информацией, так как она необходима для совершения перевода денег на карту;**
- **CVV/CVC-код (указан на обратной стороне карты). Необходим для подтверждения платежей без физического предъявления банковской карты, как правило, при транзакциях через интернет. Отсутствует на некоторых банковских картах, имеющих ограничения в использовании;**
- **срок действия карты. Обычно он не превышает два-три года (в редких случаях – до пяти лет) – таким образом, его можно достаточно легко подобрать простым перебором;**
- **имя и фамилия держателя карты. Обычно эта информация также не является секретной (зачастую при сборе средств указывается не только номер карты, на которую собираются средства, но и на чье имя она открыта). Кроме того, ряд банковских карт являются неименными, то есть вообще можно указать совершенно любое имя.**

Таким образом, для того чтобы украсть ваши деньги, злоумышленнику достаточно знать лишь номер карты (что обычно указано на страничках сбора средств в интернете) и код проверки подлинности карты (CVV/CVC). Никому не сообщайте эти данные!

1.1. ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ

Для того чтобы защитить деньги на вашей карте, необходимо соблюдать основные правила безопасного использования банковских карт:

1. Никому не сообщайте код проверки подлинности карты (CVV2 или CVC2) и ПИН-код. Помните, ни одно лицо (включая работников банка, выдавшего карту) и ни при каких обстоятельствах не вправе их запрашивать.
2. Ни при каких условиях никому (даже представителю банка!) не сообщайте пароль для доступа к своему счету через интернет. Только мошенники запрашивают пароли.
3. При утере или хищении карты немедленно позвоните в службу поддержки банка и попросите заблокировать вашу карту. Чем быстрее вы это сделаете, тем больше вероятность того, что мошенники не успеют ею воспользоваться.
4. Необходимо всегда иметь при себе (в записной книжке или в мобильном телефоне) контактные телефоны банка и номер банковской карты.
5. Постоянно контролируйте операции, которые вы осуществляете с помощью банковской карты. Движение денежных средств можно контролировать просто – подключите СМС-информирование на ваш номер телефона. Каждый раз при снятии или переводе денег вам придет уведомление о характере операции и сумме списания. Это позволит вам оперативно заметить списание средств, которое произошло без вашего согласия. Чем скорее клиент уведомит банк о несанкционированном списании средств, тем больше у него шансов получить свои деньги обратно.
6. При решении всех проблемных ситуаций обращайтесь только по официальным номерам телефонов банка. Если вам предлагают позвонить по другому номеру, то это, скорее всего, мошенники, которые пытаются узнать у вас информацию о вас и вашей карте, чтобы украсть деньги.
7. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте ее механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
8. Услугу по предоставлению овердрафта лучше заключать отдельным договором с банком – в таком случае меньше вероятность просмотреть те условия, которые обычно пишутся мелким шрифтом.
9. Установленный лимит суточного снятия наличных по карте убережет от снятия мошенниками суммы сверх этого лимита.

ВАЖНО

Если вам звонят по телефону (неважно кто: работники банка, полиция, служба безопасности или благотворители, выражающие желание перечислить вам деньги) и начинают подробно расспрашивать о реквизитах вашей карты, ПИН-коде, логине и пароле в системе интернет-банкинга – скорее всего, это мошенники.

Спросите Ф. И. О. «сотрудника», разговаривающего с вами.

Попросите внятно сформулировать цель звонка. После чего прервите разговор и самостоятельно перезвоните в клиентскую службу вашего банка. Сообщите обстоятельства беседы.

Это поможет службе безопасности предпринять необходимые меры и убережет других, более беспечных клиентов от пропажи средств.

1.2. МОШЕННИЧЕСТВА ПРИ ИСПОЛЬЗОВАНИИ БАНКОМАТА

Как бы ни была удобна банковская карта, наличные деньги по-прежнему необходимы. Например, при покупке лекарств или других товаров в аптеках/магазинах, где нет возможности оплаты картой, или их заказе с доставкой на дом. В случае срочной необходимости люди зачастую обращаются в ближайший банкомат, где их могут ждать мошенники.

Основная их цель – считать данные с карты и ПИН-код. Полученных сведений достаточно для изготовления клона карты, с которой впоследствии можно будет снять все деньги или даже получить доступ к другим картам или сберегательным счетам, открытым на имя владельца карты.

Самыми распространенными способами мошенничества с банковской картой при пользовании банкоматом являются следующие.

1. **Использование специальных считывающих устройств в картоприемнике (скиммеров)**, которые позволяют скопировать информацию с магнитной полосы банковской карты.

Примерно вот так обычно выглядит щель банкомата

Так может выглядеть банкомат со скиммером

ВАЖНО

Скиммер способен украсть информацию только с магнитной полосы, но не с чипа. По этой причине (и не только) чиповые карты считаются более защищенными.

2. **Использование на клавиатуре специальных накладок, способных считывать ПИН-коды**. Они могут выглядеть примерно так:

3. Вместо накладки на клавиатуру также **может использоваться и скрытая видеокамера**, которая может выглядеть примерно так:

4. **Установка банкоматов-имитаторов (фантомов)**, которые ничем не отличаются от настоящих. После установки клиентом карты и ввода ПИН-кода банкомат выводит сообщение об ошибке и возвращает карту. Клиент, думая, что банкомат просто неисправен, уходит, а мошенники получают дамп с данными карты и ПИН-кодом.

Как защитить карту при использовании банкомата

1. **Осматривайте банкомат** перед его использованием на предмет обнаружения устройств, которые ранее вами не наблюдались. Необходимо всегда обращать внимание, в каком состоянии банкомат, осмотреть клавиатуру и устройство для приема карты на предмет посторонних вставок, приспособлений, накладок, устройств.
2. Старайтесь пользоваться только банкоматами, установленными **в безопасных местах**.
3. Если у вас кредитная карта, то старайтесь **без острой необходимости не снимать с нее деньги в банкоматах**. Получение наличных практически все банки облагают большой комиссией, и в большинстве случаев такие операции не попадают под главное преимущество кредитки – льготный беспроцентный период.
4. Перед началом работы с банкоматом убедитесь, что **он обслуживает вашу карту**. В банкомате другого банка помимо подлежащей выдаче суммы может быть списана также оплата услуг обналичивания (обычно около 1% от снимаемой суммы, но не менее 100–200 рублей).
5. **Не прилагайте чрезмерных усилий при установке карты в картоприемник банкомата и не допускайте задержек при изъятии денег и карты.** Помните: если вы не производите в течение 30 секунд никаких действий (не нажимаете на клавиши выбора операции, не забираете карточку после ее выхода из картоприемника, не забираете деньги после их выхода из щели выдачи купюр), то банкомат в целях безопасности может захватить карточку и деньги, которые не были востребованы.
6. **При вводе ПИН-кода не стесняйтесь закрывать клавиатуру**.
7. Помните: **в случае трех неправильных последовательных попыток набора ПИН-кода ваша карта блокируется**.
8. **При захвате карточки банкоматом или невыдаче денег либо несоответствии выданной и запрошенной суммы позвоните по телефону, указанному на информационной наклейке банкомата**, а также запишите все доступные данные об этом аппарате, дату и точное время совершения операции и запрошенную сумму. Обратитесь с письменным заявлением в банк, указав все эти данные.

ВАЖНО
Если у вас возникли хоть какие-то сомнения – лучше не пользуйтесь этим аппаратом.

1.3. МОШЕННИЧЕСТВА ПРИ БЕЗНАЛИЧНОЙ ОПЛАТЕ ТОВАРОВ И УСЛУГ

Стать жертвой мошенника можно, просто расплачиваясь картой в аптеке, магазине или на заправке. Большинство даже не задумываются о том, что выпускать карту из собственного поля зрения очень рискованно и наличие ПИН-кода, на который многие ссылаются как на самый лучший способ защиты данных, далеко не всегда эффективно.

Существуют так называемые ручные скиммеры, которые мгновенно считывают данные, которые хранятся на магнитной полосе любой банковской карты. Таким образом мошенники получают своеобразный оттиск карты, которым впоследствии могут воспользоваться для хищения денег. Известны случаи, когда при оплате услуг в кафе в течение всего лишь пары минут, пока карта находилась вне поля зрения владельца, с магнитной полосы карты считывалась конфиденциальная информация о ее держателе и сумме средств на карточном счете.

Кроме того, злоумышленник может просто переписать, сфотографировать или запомнить номер карты и CVV/CVC-код и потом воспользоваться ими, например при покупке в интернете.

Как защитить карту при безналичной оплате товаров и услуг

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.

2. Требуйте проведения операций с картой только в вашем присутствии, не позволяйте уносить карту из поля зрения.
3. Не позволяйте вставлять карту в посторонние устройства, кроме терминала, через который происходит оплата по карте.
4. Не подписывайте чек (слип), в котором не указаны (или указаны неверно) сумма, валюта, дата и тип операции, название продавца.
5. Потребуйте возврата денег и получите чек на списание и возврат в случае, если с вас ошибочно списали деньги (например, кассир при ручном наборе суммы на терминале ввел неверное значение).
6. Сохраняйте чеки (слипы) после оплаты покупок по карте до тех пор, пока указанные суммы не будут списаны со счета (это обычно происходит через один – три дня с момента, как пришло СМС-сообщение о списании денег).
7. Сохраните чек с отказом от транзакции, если кассир сообщил вам, что операция по вашей карте не может быть совершена.

ВАЖНО

- **Внимательно смотрите, что делают с вашей картой.**
- **Не расплачивайтесь картой в сомнительных заведениях и обязательно храните у себя копии чеков.**

1.4. МОШЕННИЧЕСТВА ПРИ ОПЛАТЕ ПОКУПОК ЧЕРЕЗ ИНТЕРНЕТ

С современным развитием технологий практически любую покупку можно совершить, не вставая с дивана. Это особенно актуально, если в семье есть лежачий больной. При этом неважно, что конкретно вам понадобилось – лекарства, пеленки или авиабилет для консультации со специалистом в другой клинике, – если у вас есть банковская карта, по которой можно совершать платежи в сети Интернет, то оплатить покупку можно в любое удобное для вас время.

Но при этом нельзя забывать об осторожности, ведь оплата банковской картой через интернет связана с серьезным риском потери средств.

Обманывать вас могут по-разному. Например, один из самых распространенных способов обмана – фиктивный сайт интернет-магазина или интернет-аптеки, в котором товары (чаще всего это дорогостоящие лекарства, техника или авиабилеты, например на лечение или консультацию к специалисту в другом регионе/стране) стоят намного дешевле, чем в других магазинах. При оплате покупатель вводит данные карты, оплачивает (как он думает) товар или услугу, ждет покупку – ее все нет. В случае с авиабилетами иногда мошенники присылают точную копию брони билета, однако ее нельзя проверить на сайте авиакомпании. Если покупатель через какое-то время попробует зайти на сайт, с которого проводился платеж, то, как правило, его уже не существует.

Еще один способ использования чужой банковской карты – заражение компьютеров вирусными программами. Эти программы нацелены на хищение информации о карте пользователя при ее введении (номер, срок действия и т. д.). Программа сохраняет и пересылает эту информацию мошенникам. А далее можно попрощаться с деньгами.

Признаки, которые помогут определить, что перед вами сайт мошенников:

1. Стоимость товара/услуги заметно ниже, чем в аналогичных интернет-магазинах.
2. Сайт, через который осуществляется продажа, малоизвестен. Имеет небрежный дизайн, не соответствующий уровню товара/услуги.
3. Адрес страницы оплаты начинается не с **https://www...**, а с **http://www...**.
4. Покупателю открыто предлагается оплатить товар переводом по номеру карты.
5. В СМС-сообщении от банка с кодом для подтверждения операции содержится слово «перевод» вместо «оплата» («подтвердите перевод» вместо «подтвердите оплату»).

Как защитить карту при оплате через интернет

1. Заведите отдельную виртуальную карту для оплаты покупок через интернет и переводите на нее столько средств, сколько необходимо для оплаты конкретного товара или услуги. Это защитит данные о вашей основной карте, на которую открыт сбор средств, от несанкционированного использования.
2. Совершайте покупки на сайтах, соответствующих стандартам безопасного проведения операций. Обращайте особое внимание на доменные имена сайтов, которые вы посещаете. Адрес платежной страницы сайта должен начинаться с https (s означает secure, то есть безопасный).
3. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, так как могут использоваться похожие адреса.
4. Совершая покупку в интернет-магазине, помните, что вы проводите именно оплату картой (не путайте с банковским переводом средств со своего счета на счет продавца, например через интернет-банк). Если вам предлагают совершить перевод при помощи карты на другую карту и указывают номер карты получателя, воздержитесь от покупки.
5. Не вводите и не сообщайте ваш ПИН-код при работе в интернете.
6. Не используйте общественный Wi-Fi для проведения платежей по карте. Покупки в интернет-магазинах, любые виды онлайн-платежей, да даже просто вход в банковское приложение через общественный Wi-Fi – это большой риск того, что мошенники перехватят ваш код безопасности.
7. Используйте онлайн-защиту. Обязательно установите антивирусную программу не только на компьютер, но также на смартфон и планшет.

ВАЖНО

Когда вы вводите данные своей карты на сайте, вы предоставляете неизвестному вам человеку все сведения о своем счете. Эту информацию преступники могут использовать для того, чтобы снять деньги с вашей карты.

Прежде чем оплачивать покупку в интернете, убедитесь, что на сайте есть информация о текущем провайдере платежей, который сопровождает платежные операции (логотипы, сертификаты безопасности и т. д.).

2. МОБИЛЬНЫЕ И ИНТЕРНЕТ-МОШЕННИКИ

В России зафиксирован небывалый всплеск телефонных и интернет-афер. Тысячи людей ежедневно становятся жертвами сетевых аферистов, которые изобретают все новые и новые способы отъема денег у населения. По статистике, наиболее частой причиной преступлений в интернете становится банальная невнимательность пользователей либо недостаток знаний о правилах безопасности. Особенно это актуально для людей в тяжелой ситуации, когда все внимание и усилия направлены на сбор средств и лечение себя или своих близких.

Стремясь привлечь внимание к своей проблеме и собрать необходимые средства на лечение (свое или своих родственников), люди стремятся максимально подробно изложить ее суть. Выкладывают фотографии, диагноз, выписки, номер банковской карты и расчетного счета, контактные данные организатора сбора средств. К сожалению, очень часто преступники пользуются доверчивостью граждан, особенно в стрессовых ситуациях, и выманивают информацию, которая позволит им украсть деньги, в том числе те, которые собирались на лечение.

Рассмотрим наиболее распространенные механизмы сетевого мошенничества. Конечно, способов, которые используют аферисты, значительно больше, но, ознакомившись с этими примерами, а также соблюдая правила безопасности, вы наверняка сможете распознать расставленную ловушку и не угодить в нее.

Предупрежден – значит вооружен.

СХЕМА 1

Ситуация: вы хотите скачать какой-нибудь файл из интернета (например, на форуме неизвестный сообщил, что разработали новую методику лечения болезни) или в какой-то новейшей клинике, о которой мало кто знает, но где вам гарантируют излечение, при заполнении анкеты на сайте просят написать ваш номер мобильного телефона и код, который вам пришлют на указанный номер. Причины могут называться самые разнообразные:

- подтвердить, что вы реальный человек;
- подтвердить свое согласие с условиями лечения;
- подтвердить, что вам уже исполнилось 18 лет (хотя как это можно подтвердить с помощью СМС и мобильного телефона?);
- и другие.

Если вы соглашаетесь с указанными условиями и указываете присланный код, то в результате может оказаться, что вас подписали на платную рассылку или подписку стоимостью до нескольких сотен рублей. В худшем случае вы можете предоставить мошенникам код доступа к вашему банковскому счету, что грозит потерей всех денег, хранящихся на карте.

Ваши действия: не доверяйте непроверенной информации. Понятно, что утопающий хватается и за соломинку, но проверьте информацию, прежде чем скачивать файл по непонятной ссылке.

Если в интернете просят указать ваш номер мобильного телефона – это уже повод насторожиться. Если все же решились предоставить ваш номер телефона, прочитайте внимательно СМС, что там написано. Если оно пришло с короткого номера – пробейте его в интернете. Это позволит узнать стоимость такого сообщения или понять, что это обыкновенные мошенники.

СХЕМА 2

Ситуация: вам приходит сообщение, например что:

- ваш аккаунт заблокирован или будет заблокирован в ближайшее время;
- зарегистрирована заявка на восстановление доступа к странице, к которой привязан данный почтовый адрес;
- и т. п.

Это может быть письмо от службы поддержки почтового сервера (yandex, rambler, mail, gmail и др.), социальной сети или даже службы поддержки операционной системы (например, Windows).

Для того чтобы разблокировать аккаунт или отменить запрос на восстановление пароля, вам предлагают зайти по ссылке или отправить СМС на предложенный короткий номер.

Если к указанному аккаунту привязана вся информация, относящаяся к сбору денег, или просто представлена вся информация о больном, то мошенникам не составит труда завладеть ею, так как в состоянии стресса люди могут пройти по ссылке, чего и добивались злоумышленники.

Ваши действия: ни в коем случае не переходите по ссылке! Удаляйте письмо не раздумывая. Злоумышленники создали сайт-фальшивку, копирующий реальную страницу социальной сети или почтового сервера. После того как вы введете пароль от своего аккаунта, контроль над вашей учетной записью перейдет в руки мошенников. Они могут подставить свои данные в платежные реквизиты для сбора средств и даже получить доступ к вашему счету.

Чтобы этого не допустить, самостоятельно (а не по ссылке из письма!) наберите адрес сайта в интернет-браузере. Введите логин и пароль, для большей уверенности можете их сменить. В случае возникновения проблем с доступом обратитесь в службу поддержки по контактам, указанным на оригинальном сайте.

СХЕМА 3

Ситуация: вам приходит сообщение, что ваша карта заблокирована или, например, что заявка на списание денег принята. За дополнительной информацией предлагают обратиться по указанному телефону или пройти по ссылке.

Ваши действия: ни в коем случае не перезванивайте и не переходите по предлагаемой ссылке. Зайдите на официальный сайт вашего банка, в ваш личный мобильный банк или позвоните по официальным номерам телефонов банка, указанным на карте. На всякий случай банк может вам предложить перевыпустить вашу карту – это будет дополнительной гарантией того, что мошенники не получат доступ к вашим деньгам.

СХЕМА 4

Ситуация: от хороших знакомых, которые у вас в друзьях в социальной сети или в адресной книге, вам приходит сообщение с предложением пройти по ссылке. Это необходимо сделать для того, чтобы посмотреть какие-нибудь интересные данные по болезни: «Смотри, что нашел по тому вопросу...» или просто «От тебя очень много спама приходит. Проверь свой комп по ссылке...».

Иногда «друзья» обращаются с конкретными просьбами одолжить денег или просят помочь обновить профиль («Я нечаянно изменила логин, мне нужно обновить профиль. Можно на твой номер отправлю код, чтобы обновить профиль?»). Указанный код может дать мошенникам доступ к вашей учетной записи или подписать вас на платную подписку.

Ваши действия: не спешите переходить по ссылке, одалживать деньги или слать в ответ код. Велика вероятность, что телефон взломан и аферисты рассылают сообщения без ведома настоящего владельца номера.

Всегда проверяйте, от кого поступают просьбы. Лично перезванивайте, задавайте вопросы, ответы на которые никто, кроме вашего знакомого, знать не может. Например: «До какого класса мы учились вместе?», особенно если с этим человеком вы вообще в школе не учились – чтобы отвечающему было труднее угадать ответ.

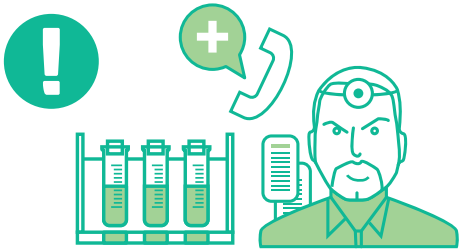


СХЕМА 5

Ситуация: к сожалению, иногда к преступникам попадают данные о пациентах с их контактной информацией и диагнозом. Мошенники звонят пациенту (чаще всего пожилым людям) от имени врача и сообщают ему о неудовлетворительных результатах сдачи анализов (к примеру, что анализ крови показал наличие рака в запущенной стадии). Затем поясняют, что мест для госпитализации очень мало, операция предстоит дорогая, и поэтому нужно внести предоплату – доктор сам заедет домой к пациенту и заберет деньги. Иногда «доктор» вместо операции уговаривает пожилого человека приобрести альтернативу проведению операции – лекарство (обычную БАД) за огромную сумму денег.

Ваши действия: часто жертвы мошенников поддаются панике, вместо того чтобы трезво оценить ситуацию. Они забывают даже, что, к примеру, могли вовсе не сдавать анализы на указанное заболевание, и откуда бы тогда взяться страшному диагнозу? А даже если и сдавали, то при плохом анализе врачи всегда советуют пересдать его, а уж потом делают выводы – и конечно, не по телефону.

Ни в коем случае не впадайте в панику. Помните, что звонок никак не связан с вашим походом к врачу – это в 99 процентах случаев совпадение, вы лишь очередная жертва в списке. Начинайте задавать конкретные вопросы: из какой поликлиники звонок, от какого врача звонят и так далее. Мошенники

пугаются таких подготовленных пациентов, и обычно происходит «случайный» сбой сети. Обязательно обратитесь в то медучреждение, на которое, может быть, ссылаются обманщики или где вы последний раз были у врача. Сообщите туда о подозрительных звонках, спросите, являются ли звонившие представителями этого медучреждения. Конечно, вы получите ответ, что звонок был не из поликлиники, не от врача, – врачи, как мы уже говорили, не имеют права сообщать подобные диагнозы по телефону.

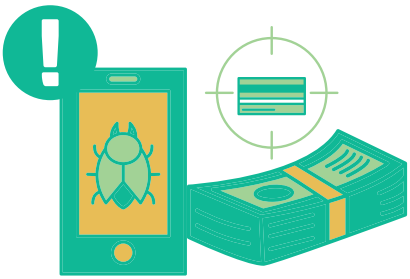


СХЕМА 6

Ситуация: вам приходит сообщение с просьбой: «Мама, срочно положи на номер XXX хотя бы 800 рублей. Потом все объясню».

Ваши действия: пополняйте только те номера телефонов, которые вам хорошо известны и внесены в вашу адресную книгу. Попробуйте перезвонить тому, от чьего имени пришло такое сообщение, – скорее всего, он ничего не знает о такой просьбе и будет очень удивлен.

СХЕМА 7

Ситуация: вам приходит сообщение с просьбой перезвонить на незнакомый номер или вы видите пропущенный звонок с незнакомого номера. Чаще всего звонок на указанный номер будет платным и с вас удержат приличную сумму денег.

Ваши действия: прежде чем перезванивать на незнакомый номер, проверьте его в интернете, где накоплено достаточно много подобной информации.

СХЕМА 8

Ситуация: вам приходит сообщение, что зачислен платеж, с незнакомого стандартного или короткого номера. Через некоторое время вам перезванивают или отправляют еще одно сообщение с просьбой вернуть якобы ошибочно переведенные деньги.

Ваши действия: прежде всего проверьте, изменился ли баланс. Если он и правда увеличился, то предложите собеседнику самостоятельно обратиться к своему оператору сотовой связи, и он поможет вернуть ошибочный платеж. Если баланс не изменился – игнорируйте подобное сообщение, а номер, с которого оно пришло, передайте в службу безопасности своего сотового оператора (она его достаточно оперативно заблокирует).

СХЕМА 9

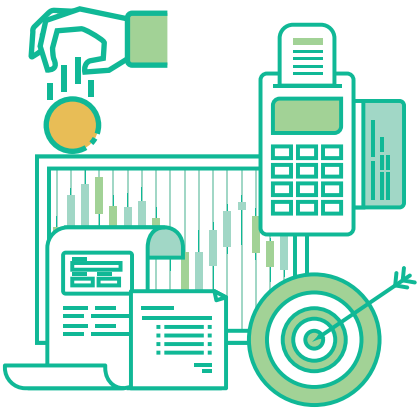
Ситуация: вы открыли сбор денег на очередную дорогостоящую процедуру или, например, что-то продаете на популярном сайте бесплатных объявлений. Находится благотворитель или покупатель, готовый сразу же перечислить вам деньги, только для этого вам нужно всего лишь сообщить ему номер своей банковской карты, срок ее действия, CVV-код или пароль для подтверждения платежа, который пришел вам в СМС-сообщении. Иначе его банк ну никак не хочет осуществлять

перевод. Как только вы сообщите конфиденциальную информацию, мошенники моментально ею воспользуются и опустошат ваш банковский счет.

Ваши действия: никогда не разглашайте свои персональные данные! Только мошенники запрашивают коды доступа. Помните, банк требует подтверждения паролем только при списании средств с вашей карты, а не при перечислении на нее! Если вы все же сообщили эту информацию мошенникам, немедленно обратитесь в банк и заблокируйте карту. Чем раньше вы это сделаете, тем больше шансов сохранить свои деньги.

2.1. ПРАВИЛА БЕЗОПАСНОСТИ: КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

1. Не воспринимайте интернет как нечто виртуальное и оторванное от настоящей жизни. Грань между цифровым миром и вашей повседневностью чрезвычайно тонка. Вы же не будете рассказывать первому встреченному на улице человеку ваши секреты или, скажем, комбинацию цифр от сейфа? Вот и в интернете делать этого не следует ни в коем случае.
2. Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой адрес (https://www....) указан в браузере. Помните, что в интернете много мошеннических сайтов, копирующих до мелочей легальные ресурсы. Сравните два адреса: **www.primer.ru** (настоящий сайт) – **www.prymer.ru** (сайт-фальшивка).
3. Никогда и никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных систем, страницах социальных сетей и т. д. Не ленитесь придумывать сложные комбинации для доступа к различным сервисам и храните их в надежных местах. Самый частый способ взлома личных данных – это элементарный подбор пароля типа 12345 или password. Возьмите за правило использовать разные пароли для захода на разные интернет-ресурсы. Вы же не пользуетесь в жизни одним ключом и для квартиры, и для машины, и для дачи.
4. Выходя в интернет с общественного компьютера или подключая свой смартфон к публичным сетям (например, в поликлинике, парке или кафе), избегайте совершать онлайн-покупки и по возможности не заходите на сайты под своим логином и паролем. А если это все-таки необходимо, обязательно по окончании нажимайте кнопку «Выход», которая есть на каждом сайте, требующем регистрации
5. Не оставляйте ваш телефон без присмотра в общественных местах. Его могут украсть вместе со всей информацией, содержащейся в телефоне, которая подчас стоит в десятки и сотни раз дороже, чем сам аппарат.
6. Обязательно установите на телефон пароль для разблокировки и доступа к данным.
7. Ценную информацию никогда не храните только в телефоне, дублируйте ее в блокноте, на компьютере.
8. Игнорируйте просьбы одолжить денег, если не уверены на 100%, что к вам обращается знакомый человек.



9. Не открывайте ссылки, не скачивайте прикрепленные файлы, пришедшие от неизвестных вам отправителей.
10. Никогда и никому не сообщайте присылаемые вам пароли и коды подтверждения. Зная номер вашей банковской карты и телефон, злоумышленники могут попытаться украсть деньги.

ВАЖНО

Если вы поняли, что разговариваете с мошенниками и к тому же передали им пароль от банковской карты:

- **прервите разговор, положите трубку;**
- **немедленно позвоните в контактный центр своего банка. Такие клиентские службы работают круглосуточно, звонки на них с мобильных телефонов, как правило, бесплатны. С помощью оператора совершите блокировку карты и входа в личный кабинет;**
- **оставьте заявку на перевыпуск карты банком;**
- **ознакомьтесь с правилами защиты от мошенничества на сайте банка.**

Если вы среагируете молниеносно, то преступники не успеют перевести деньги, даже если получили от вас пароль.

2.2. КУДА ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ

Борьбой с преступлениями в сфере высоких технологий занимается специально созданное для этих целей управление К, входящее в структуру Министерства внутренних дел РФ.

Не стоит думать, что раз вы не знаете мошенника в лицо, то дело безнадежно. Не отказывайтесь от подачи заявления и по причине небольшой суммы похищенного. Вполне возможно, что ваша жалоба окажется далеко не первой и сведения, сообщенные именно вами, помогут вывести злоумышленников на чистую воду.

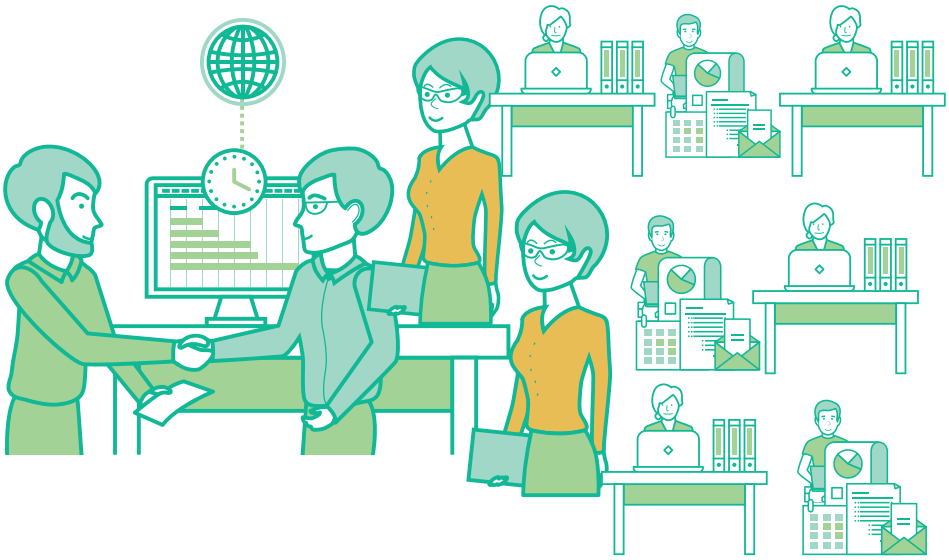
Кто поможет, кроме полиции

В случае если деньги были перечислены мошеннику через электронную платежную систему (например, WebMoney), стоит обратиться в службу поддержки клиентов. Есть шанс, что электронный счет аферист будет заблокирован. Это облегчит дальнейший возврат ваших денег.

На мошеннический сайт можно пожаловаться и на специальных сервисах, предназначенных для блокирования вредоносных сайтов. В частности, такие жалобы рассматриваются Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (http://rkn.gov.ru/).

Пожаловаться на вредоносные сайты можно и в службу поддержки крупных поисковых систем, таких как «Яндекс» (https://webmaster.yandex.ru/delspam.xml?ncrnd=1383) или Mail.ru (https://help.mail.ru/mail-help/security/fraud). Аналогичные сервисы есть и на сайтах социальных сетей.

Помощь в противодействии мобильным мошенникам оказывают и операторы сотовой связи. Они стараются поддерживать высокий уровень безопасности предоставляемых услуг, а также заинтересованы сохранять лояльность своих клиентов, поэтому стараются оперативно принять меры для защиты ваших денег и персональных данных.



3. ФИНАНСОВЫЕ ПИРАМИДЫ

Иногда сбор денег на лечение и процедуры идет не так быстро, как хотелось бы. В таких ситуациях некоторые решают рискнуть уже собранными средствами и попытаться с их помощью заработать на финансовом рынке необходимую сумму, поддавшись на обещания большой прибыли с минимальными вложениями. К сожалению, в большинстве случаев риск не оправдывает себя и люди теряют даже те деньги, которые им первоначально удалось собрать. В итоге потеряно время, потраченное на новый сбор средств, и, возможно, подорвано доверие людей, помогавших вам. Ведь в итоге первоначально собранные деньги пошли не на лечение, а в финансовую пирамиду.

Чтобы не попасть в ловушки мошенников, необходимо знать, как распознать финансовые пирамиды.

3.1. ХАРАКТЕРНЫЕ ПРИЗНАКИ ФИНАНСОВЫХ ПИРАМИД

Прежде чем расстаться со своими деньгами, подумайте о том, кому вы их отдаете и на какие цели. Если в организации, которой вы хотите доверить свои денежные средства, вы обнаружите все или несколько из перечисленных ниже признаков, стоит задуматься, не пытаются ли вас втянуть в очередную финансовую пирамиду. Не потеряете ли вы столь тяжело накопленные или собранные деньги?

- **Вознаграждение за приведенных вами клиентов**

Если вам обещают доплачивать за каждого приведенного в компанию клиента – это само по себе достаточное основание, чтобы не нести туда деньги и отговорить всех знакомых от такого рискованного мероприятия.

- **Гарантирование высокой доходности, в несколько раз превышающей рыночный уровень**

Официально гарантировать проценты по вкладам и возвратность средств могут только банки. Они находятся под строгим контролем ЦБ РФ и назначают ставку только в оговоренных законом рамках.

Помните: 100%-ную гарантию не дает никто, даже небесная канцелярия. Гарантирование доходности запрещено на рынке ценных бумаг.

- **Отсутствие необходимых лицензий**

Если лицензий нет, трижды подумайте, стоит ли связываться с этой фирмой. Вы же не обратитесь к врачу, которому «людей лечить надо, а не штаны просиживать, дипломы получая»!

- **Агрессивная реклама с некорректной информацией**

Такая реклама рассчитана на быстрое привлечение большого числа клиентов и содержит только ту информацию, оглашение которой выгодно самим основателям пирамид. Напротив, о рисках, с которыми может столкнуться клиент такой компании, рекламодатели по понятным причинам стараются не упоминать.

- **Отсутствие собственных основных средств, других дорогостоящих активов**

Имеющееся имущество и активы компании при неблагоприятном исходе можно будет продать и хотя бы частично вернуть вложенные деньги.

- **Отсутствие точного определения деятельности организации**

У пирамиды нет других клиентов, кроме самих вкладчиков. Вам никогда не покажут ее покупателей, поставщиков, посредников.

- **Наличие вступительного взноса: на оформление, обучение, за акции и т. п.**

Как правило, этот взнос и является основным доходом организаторов пирамиды.

- **Платежи принимают только наличными деньгами**

Если вам предлагают оплатить услуги, взнос, акции не через банковский счет, то есть все основания не доверять этой организации, поскольку она избегает контроля за движением денежных средств.

- **Консультации только при личной встрече**

При личной встрече проще применить различные психологические приемы и уловки, чтобы втереться в доверие клиента и убедить его вложить деньги.

- **Призывают не раздумывать и вкладывать быстро**

Попросите образец договора на руки и изучите его дома в спокойной обстановке. Если отдельные его положения вызовут у вас затруднения, постарайтесь проконсультироваться со специалистом. Не принимайте поспешных решений!

- **Договор не защищает ваши права**

Посмотрите, что за документ остается у вас взамен отданных денег. Можно ли назвать его финансовым документом, на основании которого очевидно, что фирма должна вернуть ваши деньги?

Внимательно читайте все документы. Ничего не подписывайте, не разобравшись.

Потом может выясниться, что деньги – благотворительное пожертвование или вступительный взнос, благодаря которому вы стали членом сомнительного клуба.

Если вам не нравится договор или отдельные его положения – не подписывайте его.

- **Анонимность организаторов и непрозрачность работы**

Узнайте о компании как можно больше. Изучите отзывы о компании, но взвешенно, так как их могут оставлять заинтересованные лица (сами сотрудники компании или, наоборот, конкуренты). Прочитайте все документы компании.

Узнайте, чем конкретно занимается фирма и куда будут вложены ваши деньги. Спросите, где это можно подтвердить. Проверьте эти сведения самостоятельно. Сравните условия с другими фирмами, предлагающими аналогичные услуги. Если имеют место более выгодные условия размещения ваших средств, поинтересуйтесь у сотрудника компании, за счет чего прибыль его компании в разы выше, чем у аналогичных структур, работающих в этой сфере, и получите внятные ответы на свои вопросы.

Если компания под любым предлогом отказывает в возможности получить информацию, а тем более ознакомиться с документами, подумайте, что получить вложенные деньги будет еще труднее.

3.2. ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ФИНАНСОВОЙ ПИРАМИДЫ?

1. Не паникуйте.
2. Соберите документы, подтверждающие передачу денег.

3. Незамедлительно обращайтесь в правоохранительные органы по месту жительства (полиция, прокуратура) и другие организации. Кроме того, в настоящее время сложилась достаточно успешная судебная практика борьбы с организаторами финансовых пирамид.
4. Максимально распространите информацию о мошенничестве. Не надейтесь на то, что если вы будете молчать, то организация привлечет средства других граждан, за счет которых расплатится с вами. Опыт показывает, что это совсем не так. Владельцы пирамид не спешат расплачиваться со своими кредиторами, но при этом очень искусно начинают прятать свои активы.

ВАЖНО

С 2016 года предусмотрена как административная ответственность за привлечение денежных средств в финансовые пирамиды, а также за их рекламу (ст. 14.62 КоАП), так и уголовная ответственность за организацию финансовых пирамид (ст. 172.2 УК РФ).

Куда обращаться

- Служба по защите прав потребителей финансовых услуг и миноритарных акционеров при Банке России.
- Правоохранительные органы по месту жительства (полиция, прокуратура).
- Общественные организации, например:

– «За права заемщиков»;
– Союз защиты прав потребителей финансовых услуг (ФинПотребСоюз);
– Конфедерация обществ потребителей (КонфОП);
– и другие организации.

ВАЖНО

Государство не отвечает за ваши индивидуальные финансовые решения и принятие финансовых рисков при инвестировании. Вы всегда самостоятельно несете ответственность за безопасность ваших денег на финансовом рынке. Подчас попытка заработать легкие деньги может привести к потере всех сбережений и накоплений. Помните, что ценой такого риска может стать здоровье, а подчас и жизнь близкого человека.

Чтобы не стать жертвой финансовой пирамиды, необходимо сохранять элементарную бдительность, не доверять обещаниям высокой гарантированной доходности, проверять всю информацию, предоставленную компанией, советоваться со специалистами.

- Изучите репутацию компании и достоверность предоставляемой ею информации.
- Опасайтесь щедрых вознаграждений за привлечение дополнительных вкладчиков.
- Не верьте обещаниям о гарантированной доходности инвестиций.
- Относитесь со здравым скептицизмом к различным приглашениям поучаствовать в розыгрыше всевозможных призов, подарков, путевок и т. п.
- Обратите внимание на то, как компания принимает деньги вкладчиков.
- Изучите информацию о руководстве компании, узнайте, где зарегистрирована компания.
- Проявляйте элементарную осторожность и будьте бдительны.

Предотвратить, а не бороться с последствиями

Контроль и надзор на финансовом рынке осуществляется единым органом – Центральным банком Российской Федерации. Поэтому обо всех подозрительных предложениях по совершению сделок сообщайте в полицию и Службу по защите прав потребителей финансовых услуг и миноритарных акционеров при Банке России.

АДРЕС ДЛЯ НАПРАВЛЕНИЯ КОРРЕСПОНДЕНЦИИ:
107016, г. Москва, ул. Неглинная, д. 12.

ТЕЛЕФОНЫ КОНТАКТНОГО ЦЕНТРА БАНКА РОССИИ:
8 (800) 250-40-72
(для бесплатных звонков из регионов России);
8 (495) 771-91-00
(круглосуточно по рабочим дням).

КОНТАКТЫ

Пресс-центр проекта:
117105, Россия, Москва,
Варшавское шоссе, дом 9, стр. 1

+7 (495) 640-80-91
press@vashifinancy.ru
www.вашифинансы.рф

Подготовлено по заказу Министерства финансов Российской Федерации в ходе реализации совместного проекта Российской Федерации и Международного банка реконструкции и развития «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации» в рамках конкурсной поддержки инициатив в области развития финансовой грамотности и защиты прав потребителей

Москва, 2018. – 20 с.
Тираж 3000 экз.