Личная финансовая безопасность

Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условий договоров, отсутствие финансовой дисциплины и - как следствие - неисполнение своих обязательств и неприятная финансовая ситуация.

Поговорим о финансовой безопасности и начнем с финансового мошенничества. **Что связывают с Финансовым мошенничеством** — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Рассмотрим несколько **видов мошенничества**:

- Мошенничества с использованием банковских карт
- Интернет-мошенничества
- Мобильные мошенничества
- Кредит в продаже медицинских услуг
- Финансовые пирамиды

На сегодняшний день Банковская карта удобный инструмент повседневных расчетов. Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение.

Если мы с Вами сталкиваемся с хакерскими атаками, то здесь мы скорее бессильны повлиять на ситуацию, с ними не справляются порой даже самые защищенные системы, в том числе банковской защиты. Но в нашей повседневной жизни мы можем столкнуться с такими видами мошенничества, когда в наших силах избежать негативных последствий, соблюдая простые меры безопасности, направленные на предупреждение возникновения таких последствий.

Основные приемы, которые используют злоумышленники:

•Скимминг или установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте. Это может быть накладная клавиатура, устройство для считывания карт и т.п.

•Существуют ручные скиммеры, с помощью которых, совершаются магазинные мошенничества. Это происходит во время оплаты покупки или услуги. Таким ручным скиммером могут быть считаны и зафиксированы данные Вашей карты.

•Траппинг - установка на банкомат устройства, которое блокирует карту и не выдает ее обратно, а «добрый» прохожий, якобы пытающийся помочь, подглядывает пин-код и после вашего ухода, забирает карту из банкомата и снимает с нее деньги.

•Фишинг - рассылка электронных писем, в которых от имени банка сообщается об изменениях, производимых в системе его безопасности. При этом пользователей просят возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код.

•Мошенничество с помощью телефона - когда клиенту поступают звонки с просьбой погасить задолженность по кредиту, который клиент не брал, и в ходе разговора уточняются данные карты. По похожей схеме может звонить «автоответчик» и собирать необходимые для мошенничества данные.

Таким образом, доказывая какой-то якобы кредитной организации Вашу непричастность к кредитным обязательствам, о которых Вам сообщает представитель этой организации, Вы тем самым, добровольно предоставляете мошенникам сведения о Вашей карте.

Рекомендации для избежания вероятности хищения средств с банковской карты.

В первую очередь по возможности пользоваться банкоматами, установленными непосредственно на территории отделений Банков. При использовании банкомата внимательно осматривать поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних прикрепленных предметов.

• Закрывать рукой клавиатуру при вводе ПИН-кода

• Не передавать банковскую карту посторонним: ее реквизиты могут быть использованы для чужих покупок.

• Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения.

• Никому никогда не сообщать ваш пин-код или код из смс-сообщения.

• Помните: Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов.

• Сообщать банку актуальные контактные данные (банк никогда не запрашивает пин код).

• Подключить услугу SMS- уведомлений, имея при себе телефон круглосуточной службы поддержки владельцев карт банка – Вы обеспечите эффективную профилактику риска несанкционированных операций по Вашей карте. (*в случае каких-либо подозрительных ситуаций, в том числе блокировка банкоматом, либо потеря карты, либо телефона, к которому она привязана незамедлительно набрать службу поддержки Банка и заблокировать Вашу карту*) *если банкомат не возвращает карту, не покидать место совершения финансовой операции до момента ее блокировки.*

• Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому. При его потере или краже немедленно заблокируйте карту

Уберегите себя от неприятных последствий собственной невнимательности:

• Своевременно оплачивайте кредит и не превышайте лимит кредитования – это обеспечит отличную кредитную историю и убережет от штрафов.

• Не теряйте карту - перевыпуск может стоить дополнительных средств.

• Не снимайте с карты деньги полностью – оставьте некоторую сумму для оплаты комиссий или автоматических платежей.

• В случае смены места работы обратитесь в банк и уточните актуальные для вас тарифы.

• При использовании карты зарубежом, помните о курсовой разнице во избежание нежелательного «технического овердрафта».

Технический овердрафт. Сегодня многие владеют кредитными картами, дающими возможность пользоваться определенным лимитом денежных средств, установленным банком. Как правило, банк доводит до клиентов информацию о правилах пользования такими картами, и все знают, как и что нужно делать, чтобы на карте не появилось непредвиденной задолженности. А вот владельцы дебетовых карт обычно уверены, что у них возникновение кредитной задолженности является в принципе невозможным, ведь на такие карты зачисляются только собственные средства клиента, которыми он и пользуется. Однако, такое мнение является ошибочным.

Даже на зарплатной или пенсионной карте может возникнуть задолженность, которая называется техническим овердрафтом. Хотя, для таких карт никакого лимита не устанавливается. По сути, технический овердрафт на дебетовой карте является несанкционированной задолженностью, возникающей исключительно по техническим причинам. И гасить ее необходимо в ближайший месяц.

В каких случаях может возникнуть технический овердрафт?

Случай первый. Владелец карты идет к банкомату с целью снятия наличности, при этом, он уверен, что на его счету есть 5 000 рублей. Когда он запрашивает эту сумму в банкомате, то видит сообщение, что, для проведения операции на его счету недостаточно денег. Озадаченный клиент вводит меньшую сумму, к примеру, 4 900 рублей. После получения денег на руки он вспоминает о том, что банком предусмотрена комиссия за обналичивание.

Если дело происходит в банкомате банка, выпустившего карту, то технического овердрафта возникнуть не должно, ведь оставшейся на счете суммы достаточно, чтобы оплатить комиссию. Однако, если речь идет о другом банке, то возникает необходимость оплаты дополнительной комиссии, которую клиент не учел при проведении операции. Впоследствии банком-эмитентом будет выставлен счет к оплате этой комиссии, что приведет к появлению на карте отрицательного остатка. О таком техническом овердрафте владелец карты узнает, только когда он захочет провести с этой картой другую операцию, или получит от банка уведомление о наличии задолженности и необходимости погасить ее в ближайшее время.

Случай второй. Владелец карты знает, что на карте находится сумма 3 000 рублей, и хочет ими рассчитаться, делая покупки в магазине. Однако, как это нередко случается, во время совершения транзакции в терминале возникает сбой, и операция проводится дважды. В результате на карте появится минус, о чем клиенту становится известно лишь через какое-то время. Тогда ему следует прийти в банк и написать заявление для рассмотрения данного вопроса. Если банк обнаружит ошибку в работе программы, то он вынесет решение в пользу клиента и снимет с него несанкционированный технический овердрафт. Решение по процентам, которые начисляются на просрочку, обычно принимается каждым банком индивидуально.

Случай третий. Вы расплачиваетесь рублевой картой за рубежом или просто оплачиваете покупку в иностранном интернет-магазине. Списание средств происходит лишь спустя несколько дней, а конвертация валют осуществляется на день списания, а не на день совершения покупки. Таким образом, если за эти дни курс рубля снизился по отношению к мировым валютам, с карты спишется большая сумма, чем ожидалось.

Перечень случаев, которые могут стать причиной появления кредитной задолженности на дебетовой карте, является весьма обширным. Самыми худшими вариантами являются ситуации, когда комиссия взимается не во время проведения платежа, а появляется на карточном счете позже, и клиент в течение определенного времени остается в неведении относительно наличия на его карточном счету задолженности.

Технический овердрафт может негативно отразиться на кредитной истории владельца карты, поэтому, следует взять за правило проводить проверку состояния счета после каждой проведенной в банкомате или магазине транзакции.

У некоторых банков есть практика установления для карты суммы возможного технического овердрафта, чтобы клиенты могли рассчитаться за покупку даже при нехватке собственных средств. В этом случае погашение овердрафта происходит автоматически при поступлении денег на карту. Обычно это практикуется для зарплатных и пенсионных карт, обслуживаемых банком.

Чем опасен технический овердрафт. Самым неприятным последствием технического овердрафта является увеличение в несколько раз процентов за пользование картой. Они являются самыми ощутимыми в линейке кредитных продуктов, предлагаемых банками.

При этом, клиент может даже не догадываться, что у него есть задолженность по кредитной карте, а она в это время растет буквально с каждым днем. Владелец дебетовой карты зачастую даже помыслить не может, что у него автоматически появился кредит. А когда это становится ему известно, то сумма начисленных процентов может быть уже в несколько больше суммы несанкционированного технического овердрафта.

Возникшая задолженность является обязательной для погашения, поэтому, даже при написании заявления не следует надеяться, что банк пойдет навстречу. Тарифы четко прописываются в договоре на открытие карточного счета, поэтому, отказ от выплаты долга невозможен. Здесь не лишне еще раз вспомнить золотое правило, запрещающее подписывать документ без тщательного изучения его содержания.

Чтобы защитить себя от появления технического овердрафта на дебетовой карте, следует:

- снимать деньги «под ноль» только в банкомате своего банка, чтобы минимизировать количество комиссий.

- всегда оставлять на счету определенный «запас», достаточный для покрытия небольших комиссий и предотвращения появления на карте отрицательного баланса.
- не пытаться провести операцию повторно, если при ее проведении программа дала сбой. Чтобы удостовериться, что платеж не был проведен, можно позвонить на круглосуточную «горячую линию» банка.

Выполняя эти простые правила, каждый владелец дебетовой карты обезопасит себя от несанкционированного технического овердрафта и связанных с ним неприятных последствий в виде уплаты непредвиденной задолженности, ухудшения кредитной истории и т. д.

Мошенничество в интернете. Оно включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Наиболее часто нас могут поджидать неприятности в следующих случаях:

- Покупки через интернет (особенно по предоплате и неоправданно низкой цене)
- При составлении всяческих «бесплатных» гороскопов
- При получении смс от якобы платежных систем. На самом деле часто вас поджидает вирус, задача которого - собрать данные о ваших аккаунтах в платежных системах, данные банковской карты, которые вы вводите на своем компьютере.

Как защититься:

- Не открывать сайты платежных систем по ссылке (например, в письмах), проверять, какой URL стоит в адресной строке.
- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах (потребителям, совершающим частые покупки в интернет магазинах следует взять за правило, завести для таких покупок отдельную карту, *присмотрели товар за определенную сумму, перевели на карту именно эту сумму, приобрели товар, даже если какие-то мошеннические действия захотят произвести с этой картой, денег на ней все равно нет.)*
- Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров.
- Если вам предлагают удаленную работу и при этом просят оплатить взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку.
- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, удаляйте.
- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

По данным международной статистики, совокупные потери операторов связи и абонентов от **мобильного мошенничества** ежегодно составляют примерно 25 млрд. долларов. Вариантов их огромное множество, но основных видов не так много:

- «Вы выиграли приз…». При этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код. Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.
- «Мама, я попал в аварию», когда мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета злоумышленников.
- «Блокировка карты». На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону…». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.

• Рассылка вирусов, который помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

Способы защиты:

• Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки.

• При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию.

• Не отправляйте СМС на короткие номера, заранее не узнав стоимости подобного сообщения.

• Никогда не сообщайте никаких персональных данных, даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации и перезвоните.

• Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу - не верьте! Позвоните вашему родственнику.

• Ценную информацию никогда не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

Еще одна схема финансового мошенничества Финансовая пирамида. Чаще всего работает по следующему принципу: организаторы пирамиды собирают у вкладчиков деньги (продают ценные бумаги пирамиды), но не вкладывают эти деньги в экономику, а оставляют у себя. Они объявляют о росте курса своих ценных бумаг и, когда старые вкладчики хотят снять свои деньги с процентами, с ними расплачиваются деньгами новых вкладчиков.

Пирамиды обычно обещают сверхвысокую доходность: 200—300 % в год. Так как поначалу число вкладчиков всё время растёт, организаторы пирамиды могут какое-то время поддерживать её платёжеспособность.

Опасность пирамиды заключается в том, что рано или поздно она рухнет. Слишком много вкладчиков одновременно захотят продать свои ценные бумаги. Организаторы поймут, что расплатиться со всеми не получится, приостановят выплаты, а потом скроются с оставшимися деньгами.

Как распознать пирамиду? Не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений. Обратите внимание на следующие **признаки,** которые могут характеризовать организацию как «финансовую пирамиду»:

✓ Вас призывают не раздумывать и вкладывать быстро

✓ Вам объясняют высокую доходность непрозрачными сверхприбыльными проектами, при этом не раскрывают информацию о потенциально возможных рисках. Проекты, как правило, находятся в другой стране, что затрудняет выяснение текущего положения дел.

✓ Организаторы скрывают информацию о себе, о наличии лицензий на ведение соответствующей деятельности и действуют через посредников. Часто компания зарегистрирована не в России, а в договоре отсутствует защита прав вкладчика

✓ Вам обещают высокое вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги.

Старайтесь принимать взвешенные финансовые решения, не поддавайтесь эмоциям жадности и страха. Перед тем как отдать деньги:

✓ Проверьте наличие лицензии Центрального банка на ведение деятельности (банковская, страховая, инвестиционная, такие данные размещает ЦБ на своем официальном сайте).

✓ Внимательно изучите договор на предмет условий инвестирования и возврата средств.

✓ Найдите в сети Интернет информацию о данной организации, ее историю, отзывы клиентов, рейтинги в соответствующей отрасли.

Если деньги уже вложены в сомнительные проекты, постарайтесь максимально оперативно изъять не только полученную прибыль, но и основные вложения. Не ждите, когда пирамида развалится, и не старайтесь компенсировать убытки, вкладывая новые средства.