

3. Личная финансовая безопасность

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

Финансовое мошенничество — 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
- Финансовые пирамиды

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.

Основные приемы, которые используют злоумышленники:

Скимминг или установка специальных устройств на банкоматы (накладная клавиатура, устройство для считывания карт), с помощью которых преступники получают информацию о карте.

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.

Магазинные мошенничества, когда во время оплаты покупки или услуги данные карты могут быть считаны и зафиксированы ручным скиммером.

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.

Во избежание вероятности хищения средств с вашей карты соблюдайте следующие правила:

При использовании банкомата внимательно осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних прикрепленных предметов.

Закрывайте рукой клавиатуру при вводе ПИН-кода

Не передавайте 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 сообщайте 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.

Сообщайте банку актуальные контактные данные

Подключите услугу SMS- уведомлений, всегда имейте при себе телефон круглосуточной службы поддержки владельцев карт банка - обеспечите эффективную профилактику риска несанкционированных операций по ней.

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 также и от неприятных последствий собственной невнимательности:

Своевременно оплачивайте кредит и не превышайте лимит кредитования – это обеспечит отличную кредитную историю и уберезет 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».

Мошенничество в интернете. 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 «бесплатного» гороскопа

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.

Когда вы получаете письма от сильно нуждающихся «королевских особ», которые за солидный процент просят вас перевести крупную сумму для спасения страны.

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

Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров.

Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации.

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 отправляете 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.

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?

Во-первых, не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений.

Во-вторых, 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 высокие вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги.

В-третьих, 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).

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.

Статья подготовлена в рамках Всероссийской недели сбережения 2018, которая проходит в рамках Проекта Министерства финансов Российской Федерации «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации». Узнайте больше на портале вашифинансы.рф.