*ЗА ПРАВА ЗАЁМЩИКОВ

ONF.RU/ZPZ
ЗАПРАВАЗАЕМЩИКОВ.РФ

ОБЩЕРОССИЙСКИЙ НАРОДНЫЙ ФРОНТ

Схемы финансового мошенничества: предупрежден, значит защищен

План лекции:

1. Определение мошенничества в Российском законодательстве
2. Схемы мошенничества
3. Как обезопасить себя от мошенничества

1. Определение мошенничества в Российском законодательстве

Финансовое мошенничество – это совершение противоправных действий в финансовой сфере путем обмана, злоупотребления доверием, введения в заблуждение и других манипуляций с целью незаконного обогащения.

В Российском законодательстве предусмотрена уголовная ответственность за финансовое мошенничество. Ответственность прописана в статье 159 УК РФ «Мошенничество». Согласно статье 159 УК РФ, мошенничество определяется как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

В зависимости от обстоятельств и участников схемы мошенничества, российское законодательство подразделяет его на совершенное одним участником или группой лиц, а также в зависимости от суммы ущерба - на мошенничество, совершенное в крупном или особо крупном размере.

В случае, если вина мошенников доказана в суде, то в зависимости от обстоятельств дела, наказание может быть назначено от штрафа в несколько сотен тысяч рублей до лишения свободы на срок до 5-ти лет (это максимально возможное наказание по 159 статье УК РФ). В связи с активным развитием новых технологий и усложнением финансовых продуктов и услуг, современное мошенничество приобрело интеллектуальный и психологический характер, вплоть до приемов нейролингвистического программирования и методов гипноза. Схемы мошенничества постоянно адаптируются к новым условиям и целью мошенников становятся не только физические лица, но и компании, банки, государственные органы власти.

Современные финансовые мошенничества многообразны и сложны. Для целей нашей лекции ограничимся основными типами мошенничества, с которым чаще всего сталкиваются российские потребители.

- **Финансовые пирамиды. Их признак: отсутствие какой-либо реальной деятельности, кроме сбора средств с участников пирамиды.**
- **Мошенничества с использованием банковских карт. Известно множество различных видом этого мошенничества, но цель у них, как правило, одна - воспользоваться средствами с вашей банковской карты.**
- **Интернет-мошенничества. Мошенники применяют как психологические приемы, так и технические средства с целью несанкционированного доступа к средствам на банковских счетах, картах.**
- **Мобильные мошенничества. Аналогично интернет-мошенничеству, мошенники могут использовать как психологические приемы, так и технические средства. Мошенники могут попытаться списать средства с Вашего мобильного счета, либо получить несанкционированный доступ к мобильному банку.**

Если Вы столкнулись с финансовым мошенничеством, то Ваши действия должны быть быстро направлены на пресечение возможности увеличения убытков.

Так, если Вы обнаружили, что у Вас украли банковскую карту, надо немедленно позвонить в банк и заблокировать ее. Если Вам пришло смс-сообщение о списании какой-то суммы с Вашего счета, или запрос на подтверждение операции, которую Вы не совершали – следует немедленно позвонить в банк и выяснить, не происходит ли прямо сейчас попытка кражи средств с Вашего счета.

Интернет-гигиену надо соблюдать наравне с физиологической: не открывать подозрительные письма и сайты, не скачивать, не открывать и не устанавливать подозрительные программы, не переходить по ссылкам, указанным в подозрительных письмах и сообщениях.

Чтобы не вложить свои деньги в финансовую пирамиду, надо перед заключением каких-либо сделок изучить всю доступную информацию об этой компании:

- **Официальные реквизиты и дату регистрации,**
- **Наличие необходимых разрешений и/или лицензий на осуществляемую деятельность,**
- **Наличие компании в государственных реестрах,**
- **Проверить отзывы других клиентов о ее деятельности.**

Но несмотря на эти не слишком сложные правила, ежегодно тысячи людей в России и миллионы по всему миру теряют деньги от финансового мошенничества. Почему так происходит?

Потому, что большинство людей весьма доверчивы и верят в то, что им обещают или говорят. А сделать второй шаг – проверить, является ли предоставленная информация правдивой – успевают далеко не все.

2. Распространенные схемы мошенничества.

* **Нелегальные банки**. Только за 2016 год в российском сегменте Интернета были обнаружены несколько нелегальных банков, которые предлагали банковские услуги, не имея банковской лицензии. Если Вы решили воспользоваться услугами банка в Интернете, то для начала проверьте его по номеру лицензии на официальном сайте Банка России:

  cbr.ru
  Информация по кредитным организациям / Справочник по кредитным организациям

  Регулярно обнаруживаются сайты-фальшивки, которые копируют сайт легального банка и таким образом вводит в заблуждение его клиентов. Поэтому всегда проверяйте адрес банка в строке браузера при входе в Интернет-банк. На мошеннических сайтах в адресной строке могут отображаться цифры или другие доменные имена, не соответствующие официально зарегистрированному доменному имени системы интернет-банка (например, вместо сбербанк.ру в адресной строке может быть написано сбер.ру или 1234.ру и т.д.).
  Внимательно относитесь к поступающим на Ваши электронный адреса и аккаунты в соц.сетях письмам и сообщениям. Не спешите переходить по предлагаемым ссылкам. Лучше самостоятельно вводить веб-адрес в адресную строку.
  Если Вы перешли по ссылке в подозрительном письме и Вам предлагается ввести фамилию, имя, отчество, номер карты, CVV или ПИН код – никогда не делайте этого.

* **Управляющая / инвестиционная компания, микрофинансовая организация**.
  Финансовые пирамиды могут маскироваться под управляющие компании и МФО, предлагая своим клиентам зарабатывать на инвестициях в какие-либо проекты, на кредитовании других граждан, или на фондовом / валютном рынках. Такие компании не скупятся на щедрые обещания прибыли, но фактически кроме сбора средств с клиентов никаких других действий не производят.

  Следует помнить, что легальные управляющие компании имеют специальную лицензию на инвестиционную деятельность, состоят в реестре Банка России, а также раскрывают информацию о своей бухгалтерской отчетности на своих официальных сайтах. Кроме того, законодательство обязывает управляющие компании информировать клиентах о всех возможных рисках, связанных с инвестициями.
  Микрофинансовым организациям не требуется специальная лицензия на деятельность, однако, все легальные МФО состоят в едином реестре, который ведет Банк России, соответственно, они должны раскрывать дату включения в реестр и номер, по которому их можно найти.
  Рекомендуется записать адрес Справочника Банка России, где можно найти все легальные компании, оказывающие финансовые услуги на российском рынке:

  cbr.ru
  Финансовые рынки / Справочник участников финансового рынка

- **Потребительские кооперативы.** Потребительский кооператив, в соответствии с законодательством, представляет собой объединение людей и организаций, основанное на желании удовлетворить какие-либо схожие материальные и иные цели. Участники потребительского кооператива делают вступительные и паевые взносы своим имуществом.

  Потребительским кооперативам не требуется специальная лицензия на деятельность. Чтобы отличить реальный потребительский кооператив от финансовой пирамиды, надо выяснить, официально ли зарегистрирована компания, как долго работает на рынке и каковы результаты ее деятельности, нет ли у нее задолженности перед налоговыми органами, изучить отзывы клиентов о данной компании.

- **Общества взаимопомощи, клубы, партнерства.** Нередко финансовые пирамиды маскируются под такие организации, заявляя благие цели и обещая всяческие выгодны новым членам. Также могут использоваться наименование и логотип / дизайн очень похожие на аналогичные бренды легальных компаний. Все это делается ради того, чтобы у будущих жертв обмана максимально снизилась здоровая подозрительность и критическое мышление.

  Методы работы с клиентами, как правило, отличаются настойчивостью, навязчивостью. Произносится много красивых слов и профессиональных терминов, чтобы внушить клиентам доверие.

  Помните, что Вы вкладываете свои средства и имеете право знать, в какую организацию Вы их отдаете и на какие цели. Компания, с которой Вы решили работать, должна иметь как минимум официальную регистрацию, Устав, официальное местонахождение – юридический адрес.

- **«Нигерийские письма».** Это интернет-мошенничество, основанное на массовой спам-рассылке электронных писем. Свое название оно получило в связи с особо широким распространением именно в Нигерии. Суть мошеннической схемы сводится к тому, чтобы убедить жертву сделать перевод средств / пожертвование по указанным в письме реквизитам. В письме некто представляется представителем знатной семьи, нигерийской или кенийской, ливийской и других. Легенда гласит, что из-за репрессий, военных действий и других форс-мажорных обстоятельств, данный человек лишился доступа к крупной сумме своих средств. Жертве предлагается помочь в доступе к этим средствам за солидное вознаграждение (как правило это сумма от 50 до 100 тысяч долларов). Правда сначала надо перечислить совсем небольшую сумму (100-300 долларов или евро) для оплаты услуг юриста по оформлению документов.

  По статистике, 1% от всех пользователей, получивших «нигерийские письма», все же попадаются на уловки мошенников и успевают перечислить средства мошенникам до того, как осознают, что их обманули.

  Сейчас появились новые сюжеты «нигерийских писем». Например, юная наследница богатой семьи, пострадавшей от репрессий диктатора, просит помощи для законного возврата своих богатств, и обещает вознаграждение за оказанную помощь. Или юрист, сообщающий, что Ваш

далекий родственник оставил Вам большое наследство, и за небольшое вознаграждение он совершит все юридические действия по его получению и передаче Вам. Пишут от имени бухгалтеров, обнаруживших тайный счет умершего босса, от имени детей и других бесчисленных родственников свергнутых президентов / министров / королей, от имени богачей-чудаков, мечтающих передать свое наследство именно Вам.
Рекомендация: если Вы получили «нигерийское письмо», не отвечайте на него.

* **Блокировка компьютера / аккаунта.** В результате посещения сайта, открытия письма или сообщения из соц.сети, зараженного вредоносной программой, происходит блокирование интернет-браузера или компьютера.

  Пользователь получает сообщение следующего содержания "Для возобновления работы отправьте SMS на указанный номер, и Вы получите код для разблокировки". При отправке SMS происходит списание всех денег со счета абонента.

  Меры электронной гигиены: будьте внимательны к ресурсам, которые Вы посещаете или которые Вам предлагают посетить путем рассылок e-mail, сообщений и смс.
  Установите и регулярно обновляйте антивирусное программное обеспечение своих электронных девайсов.

  Если произошла так называемая «блокировка» – не паникуйте! Перезагрузите компьютер, осуществите проверку компьютера на вирусы. Если указанные меры не помогли - обратитесь к профессиональным специалистам технической поддержки.

3. Как обезопасить себя от мошенничества.

Универсальное правило для защиты от всех видов мошенничества:
Не верьте - проверьте!

- **Если Вы рассматриваете предложения от банков или финансовых компаний, проверьте, имеет ли данный банк или компания официальный сайт, реквизиты (включая ОГРН, ИНН, юридический адрес), проверьте данную компанию в Справочнике финансовых организаций на сайте Банка России, найдите отзывы клиентов о данной организации.**
- **Полагайтесь на интуицию. Если у Вас возникли подозрения относительно сделки, которую Вам предлагают - не спешите подписывать документы. Возьмите паузу для более детального изучения условий сделки и компании, которая эту сделку Вам предлагает. В идеале получить консультацию юриста или финансиста по предлагаемому договору.**
- **Внимательно относитесь к поступающим на Ваши электронный адреса и аккаунты в соц.сетях письмам и сообщениям. Не спешите переходить по предлагаемым ссылкам, особенно если эти ссылки должны вести на сайты платежных систем, интернет-банков и т.п. В этом случае лучше самостоятельно вводить веб-адрес в адресную строку. Если Вы перешли по ссылке в подозрительном письме и Вам предлагается ввести фамилию, имя, отчество, номер карты, CVV или ПИН код – никогда не делайте этого.**
- **Если Вы заподозрили, что Вас уже втянули в мошенническую схему - помните, что время здесь работает против Вас. Обратитесь с жалобой в государственные органы (Роспотребнадзор, Банк России, МВД, Прокуратура), правозащитные организации (финансовый омбудсмен Павел Медведев, проект "За права заемщиков" и другие правозащитные организации). Помните, Ваше обращение должно быть обосновано и подтверждено фактами.**
- **Будьте бдительны, когда Вам звонят с неизвестных номеров телефонов. Никогда не раскрывайте звонящему Ваши персональные данные (ФИО, дату рождения, паспортные данные, номера карт и тем более пин-коды или коды подтверждения из смс-сообщений).**

Не спешите действовать, если Вам позвонили (или прислали смс) с сообщением о том, что Вы выиграли приз в лотерее или, например, что Ваша карта заблокирована. Такие смс-сообщения обычно рассылают мошенники. Их цель – заставить Вас позвонить по указанному номеру, а потом к делу подключаются профессиональные психологи, которые постараются выманить у Вас конфиденциальную информацию.

Также Вам могут позвонить, представится сотрудником банка и сообщить о просрочке по кредиту. Вы возмутитесь, особенно если Вы не брали никаких кредитов. Тогда Вам предложат сверить номер карты, заставив его назвать, а также подтвердить CVV-код.

Аналогичный звонки могут поступать от якобы сотрудников интернет-магазинов, которые сообщают что платеж не прошел и просят сверить номер карты и CVV-код.
Помните, все что нужно мошенникам - получить номер Вашей карты и CVV-код. Если такое мошенничество сработает, то вскоре Вы обнаружите, что Вашей картой расплатились где-то в интернет-магазине или сделали с нее перевод на другой счет.

6. Используйте смс-информирование обо всех операциях, произведенных по Вашим карточным счетам. При появлении малейших подозрений о неправомерном списании денег со счета, незамедлительно обращайтесь в банк. У держателя карточки есть 24 часа, чтобы оспорить неправомерное списание денег с карточного счета, заблокировать карту и получить подтверждение банка о блокировке. Банк в соответствии с законом несет обязанность в полном объеме возместить заемщику убытки, возникшие вследствие неправомерного (несанкционированного) списания денежных средств. Бремя доказывания обстоятельств, освобождающих банк от ответственности, лежит на банке как исполнителе услуг.

*ЗА ПРАВА ЗАЁМЩИКОВ

«При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 05.04.2016 № 68-рп и на основании конкурса, проведенного Общероссийской общественной организацией «Российский союз ректоров».