

Уважаемые студенты группы ДБ 9-22!

Вам необходимо выполнить задание:

1. Прочитать внимательно лекцию на тему: «Финансовое мошенничество».
2. Составить краткий конспект по основным понятиям.
3. Ответить на контрольные вопросы.
4. Выполненное задание предоставить на проверку в виде фотоотчета до 31.03.2023г. на email: margomtv1977@inbox.ru С Уважением Мелихова Татьяна Валерьевна.

!!! Если возникнут вопросы, обращаться по телефону: +7959-133-02-54 (ватсап, телеграмм).

ЛЕКЦИЯ 1.9 ФИНАНСОВОЕ МОШЕННИЧЕСТВО

СОДЕРЖАНИЕ

1. Виды мошеннических действий.
2. Способы защиты от мошенников на финансовом рынке.
3. Финансовые пирамиды.
4. Правовые нормы для защиты прав потребителей финансовых услуг.
5. Ответственность за мошенничество.

Мошенничество - хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотребления доверием (статья 159 УК РФ).

Финансовое мошенничество - совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Финансовое мошенничество распространяется на имущество и денежные средства граждан или организаций. Важным моментом является корыстный мотив со стороны злоумышленника, неважно какую из схем обмана он использует. В отличие от обычной кражи финансовое мошенничество характеризуется умышленным завладением чужими деньгами, но более «тайными» способами.

Все мошенничества в финансовой сфере объединяет одно: преступники без принуждения, с согласия самих людей получают их денежные средства. При этом потерпевшие думают, что передают эти деньги в обмен на какие-либо законные блага — недвижимое имущество, товары в интернет-магазинах, наследство и т.д. На самом деле же никаких «законных благ» нет, люди просто теряют свои деньги,

не получая ничего взамен. Злоумышленники же изначально знают, что они не имеют никаких правовых оснований для получения денег и другого имущества от потерпевших.

Наиболее распространенные виды мошенничества представлены на рисунке 1.



Рисунок 1 - Распространенные виды мошенничества

С каждым годом появляются всё новые и новые виды мошенничества. С активным развитием новых технологий финансовое мошенничество адаптируется к современным условиям. В наши дни мошенничество приобрело интеллектуальный характер. Мошенники применяют не только новые технологии, но и самые современные психологические методики.

1. Финансовые пирамиды - это мошеннические схемы по принципу обеспечения дохода через привлечение других участников «пирамиды» или вложения под проценты. Руководители таких афер часто выдумывают несуществующие продукты, а после сбора денег с участников попросту исчезают со всеми сбережениями. Банк России выделяет следующие внешние признаки, свидетельствующие о том, что организация или группа физических лиц является «финансовой пирамидой»:

- выплата денежных средств участникам из денежных средств, внесённых другими вкладчиками;
- отсутствие лицензии ФСФР России (ФКЦБ России) или Банка России на осуществление деятельности по привлечению денежных средств;
- обещание высокой доходности, в несколько раз превышающей рыночный уровень;
- гарантирование доходности (что запрещено на рынке ценных бумаг);
- массивная реклама в СМИ, сети Интернет с обещанием

высокой доходности;

- отсутствие какой-либо информации о финансовом положении организации;
- отсутствие собственных основных средств, других дорогостоящих активов;
- отсутствие точного определения деятельности организации.

а) offline: банкоматы и терминалы (в т.ч. скимминг), оплата в магазинах или ресторанах и т.д.

Скимминг — установка на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковской карты и вводимый пин-код) для последующего хищения денежных средств со счета банковской карты.

Способы минимизации рисков:

- пользоваться только банкоматами, установленными в безопасных местах;
- внимательно осматривать банкомат, перед его использованием;
- закрывать клавиатуру при вводе пин-кода;
- оформить услугу sms-оповещения о проведенных операциях по карте;
- не давать согласие на получение карты по почте и ее активации по телефону;
- не хранить пин-код вместе с картой;
- не сообщать по мобильным или стационарным телефонам реквизиты карты и ее пин-код;
- определить лимит суточного снятия наличных по карте;
- заблокировать карту немедленно в случае утери/хищения.

Способы минимизации рисков:

- установить программы защиты и обеспечения безопасности компьютера в интернете;
- проводить финансовые операции только с защищенных веб-сайтов;
- не сообщать пароль доступа к своему счету через интернет;
- использовать надежные пароли;
- по окончании работы выходить из учетной записи;
- не отвечать на электронные сообщения с запросом на изменение параметров защиты;
- использовать разные инструменты для разных видов расчетов.

Фишинг (англ. phishing) — это технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли

доступа, данные банковских и идентификационных карт, посредством спамерской рассылки или почтовых червей. Бывает почтовый, онлайн-овый, комбинированный.

Способы минимизации рисков:

- проявлять осторожность;
- застраховать карту от риска мошенничества;
- использовать разные инструменты для разных видов расчетов;
- использовать метод многофакторной аутентификации.

Вишинг (англ. vishing) — это технология интернет-мошенничества, заключающаяся в использовании автонабирателей и возможностей интернет-телефонии для кражи личных конфиденциальных данных, таких как пароли доступа, номера банковских и идентификационных карт и т.д.

Смишинг – это вид мошенничества, при котором пользователь получает СМС-сообщение, в котором с виду надежный отправитель просит указать какую-либо ценную персональную информацию (например, пароль или данные кредитной карты). Смишинг представляет собой подобие фишинга, при котором мошенниками с той же целью рассылают электронные письма.

Способы минимизации рисков:

- внимательно изучить правила безопасного использования банковской карты;
- не сообщать никому, в том числе сотруднику банка, ваши персональные данные и данные банковской карты;
- при возникновении факта мошенничества обратиться в ваше отделение банка;
- в случае необходимости заблокировать карту;
- не звонить по предложенному в смс номеру телефона по вопросам безопасности вашей карты.

Фарминг (англ. pharming) – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации.

Способы минимизации рисков:

- установка антивирусной программы;
- установка обновлений от производителей по и поставщика услуг интернета;
- проверка url;
- проверка изменения адреса http на https при переходе на страницу оплаты.

«Нигерийские письма» (англ. «Nigerianscam») – электронное письмо с просьбой о помощи в переводе крупной денежной суммы, из которой 20-30% должно получить лицо, предоставляющее счет. При этом получателю необходимо срочно 6-10 тысяч долларов США отправить по системе электронных платежей по требованию адвоката. Как разновидность используется рассылка о выгодном капиталовложении или устройстве на высокооплачиваемую работу, получении наследства или иных способах быстрого обогащения при условии совершения предварительных платежей.

Способы минимизации рисков:

- установить антиспамские программы;
- критически относиться к предложениям получения быстрого и неограниченного дохода;
- получить консультацию экспертов в области финансового мошенничества;
- проявлять осмотрительность при принятии быстрых финансовых решений.

Способы минимизации рисков:

- пользуйтесь проверенными мировыми и российскими торговыми площадками;
- заключайте сделку только через выбранную площадку;
- требуйте максимально полной информации о продавце дешевого товара;
- по возможности оплачивайте товар по факту его получения.

Мошенничество с PayPal - крупнейшая дебетовая электронная платежная система. Аналоги в РФ: Яндекс.Деньги, WebMoney.

Вы разместили объявление о продаже. Мошенник высылает Вам письмо с предложением купить товар, иногда за большую цену и не для себя. Вы просите перевести деньги. Мошенник просит вас указать адрес, зарегистрированный в PayPal, и говорит, что выслал деньги туда, но они появятся на счете в PayPal, когда вы введете номер почтового отправления. К вам приходит письмо, похожее на PayPal. Вы отправляете товар и вводите номер отправления в указанную в письме страницу. Товара у вас нет. Претензии выставлять некому.

Кликфрод (от англ. click fraud) — один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении. Может осуществляться с помощью автоматизированных скриптов или программ, имитирующих клик пользователя по рекламным объявлениям Pay per click.

Виды кликфрода: технические клики, клики рекламодателей, клики конкурентов, клики со стороны недобросовестных веб-мастеров.

Кликджекинг (от англ. clickjacking) механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу.

РАММ-счета (от англ. Percent Allocation Management Module – модуль управления процентным распределением) – специфичный механизм функционирования торгового счета, технически упрощающий процесс передачи средств на торговом счете в доверительное управление выбранному доверенному управляющему для проведения операций на финансовых рынках.

Хайп (англ. HYIP, High yield investment program) – это высокодоходная инвестиционная программа, капитал которой формируется из взносов пользователей сети Интернет.

Способы минимизации рисков:

- провести «тестовый режим» участия в хайп-проекте;
- анализировать информацию сайтов мониторингов и форумов, освещающих состояние дел по интересующему вас хайп-проекту;
- распределять денежные средства между несколькими хайп-проектами;
- не инвестировать заемные средства;
- не инвестировать «последние деньги».

Социальное манипулирование (социальная инженерия) - метод управления действиями человека, основанный на использовании его слабостей и индивидуальных особенностей. Техническая и технологическая инфраструктура используется только для обеспечения контакта.

2. Мошенничество в социальных сетях - Сетевые домушники, Интернет-угонщики, Сетевые грабители

Способы минимизации рисков:

- проявлять должную осмотрительность при выкладывании в сеть личных

данных;

- ограничить доступ незнакомых людей к информации, потенциально интересной для мошенников;
- не публиковать «горячую» информацию, находясь в отпуске.

Способы минимизации рисков:

- совершать валютно-обменные операции в банках;
- минимизировать данные операции в обменных пунктах;
- быть внимательным, так как курс может быть указан без учета комиссии, либо выгодным он является исключительно при обмене очень больших сумм;
- всегда пересчитывать денежную сумму.

Способы минимизации рисков:

- изучить официальную информацию о компании (реквизиты, юридический и фактический адрес);
- проверить наличие информации о финансовой компании на сайте надзорного органа – ЦБ РФ;
- посмотреть отзывы о компании в независимых блогах и социальных сетях.

Нелегальные азартные игры

Раздолжнители - заёмщикам предлагают купить вексель, который равен по сумме просроченному кредиту, и расплатиться им с банком. А за вексель предлагается расплатиться с компанией-раздолжнителем в рассрочку на несколько лет под определенную ставку годовых.

Махинации с арендой/покупкой недвижимости или автомобилей («двойные продажи», продажи людям квартир в незаконно построенных домах и т.д.)

Как себя обезопасить от финансовых махинаций:

- При краже карты — позвонить в банк, заблокировать карту.
- При получении смс-сообщения о списании суммы с вашего счета, получения запроса на подтверждение операции, которую вы не производили — позвонить в банк и уточнить об операции.
- Никому не сообщать номер банковской карты, пин-код; не давать пароль к доступу своего счета через интернет.
- Не передавать банковскую карту третьим лицам.
- Перед использованием банкомата, всегда внимательно его осматривать.
- Закрывать клавиатуру при вводе пин-кода банковской карты.
- Не открывайте подозрительные письма.
- Не заходить на сайты, которые не вызывают у вас доверия.
- При открытии подозрительных писем, не переходите по ссылкам. Не устанавливать подозрительные программы.
- Установить антивирусные программы.
- Не раскрывать ваши персональные данные, звонящим с незнакомых номеров.

Перед заключением каких-либо сделок с вложением финансов необходимо убедиться в благонадежности компании, для этого:

- найти и проверить отзывы о компании;
- проверить реальное существование компании в государственных реестрах;
- убедиться в наличии необходимых лицензий, разрешений для осуществления деятельности компании;
- проверить имеет ли данная компания официальный сайт.

Если против вас совершено мошенничество, необходимо срочно обратиться в правоохранительные органы.

Ответственность предусмотрена Уголовным кодексом РФ ст.159 «Мошенничество»:

Статья 159.1 УК РФ Мошенничество в сфере кредитования.

Статья 159.2 УК РФ Мошенничество при получении выплат.

Статья 159.3 УК РФ Мошенничество с использованием электронных средств платежа.

Статья 159.5 УК РФ Мошенничество в сфере страхования.

Статья 159.6 УК РФ Мошенничество в сфере компьютерной информации.

Данная статья подразделяет меры ответственности в зависимости от:

- количества участников (один участник или группа лиц);
- суммы ущерба (в крупном размере, особо крупном).

Ответственность за совершение мошеннических действий предусматривает несколько видов наказаний, вплоть до лишения свободы. В соответствии с ст. 159 УК РФ ответственность будет следующей:

1. наложение штрафа;
2. обязательные работы;
3. исправительные работы;
4. ограничение свободы;
5. принудительные работы;
6. арест;
7. лишение свободы.

На итоговое наказание влияет тяжесть содеянного, т.е. ущерб и наличие сговора.

Контрольные вопросы

1. Виды мошеннических действий.
2. Способы защиты от мошенников на финансовом рынке.
3. Финансовые пирамиды.
4. Правовые нормы для защиты прав потребителей финансовых услуг.
5. Ответственность за мошенничество.