

Финансовое мошенничество



КЛАССНЫЙ ЧАС

Мошенничество



- «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» (ст. 159 УК РФ)



Финансовое мошенничество

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

Предпосылки роста финансового мошенничества в современном мире

- ✓ увеличение объема финансовых транзакций у каждого из нас;
- ✓ снижение возраста участников товарно-денежных и иных видов сделок;
- ✓ разнообразие видов денег и ценных бумаг;
- ✓ повышение доступности и конфиденциальности персональных данных;
- ✓ увеличение объема сделок вне личного контакта участников (интернет-торговля);
- ✓ исчезновение границ для свободного перемещения денег, товаров, услуг в процессе глобализации (рост транснациональной финансовой преступности);

Предпосылки роста финансового мошенничества в современном мире

- ✓ резкое ускорение процессов технологизации нашей жизни (технологическая сингулярность);
- ✓ отставание технологий защиты функционирования финансовых систем всех уровней перед кибермошенниками;
- ✓ поведенческий и интеллектуальный разрыв между организаторами мошеннических схем и другими участниками финансовых отношений;
- ✓ сверхвысокие доходы участников финансовых афер при весьма умеренном наказании в большинстве стран мира;
- ✓ несоответствие поведенческих стереотипов участников финансово-денежных отношений новому уровню рисков.

Основные общие признаки указывающие на риски финансового мошенничества

- ✓ вознаграждение существенно превышает деловую практику по данному типу сделок;
- ✓ использование технологий «социальной инженерии» и манипулирование такими интересами как жадность, желание быстро разбогатеть, зависть;
- ✓ предложение решить все финансовые проблемы в короткий срок;
- ✓ необходимость первоначальных выплат;
- ✓ анонимность контрагента;
- ✓ необходимость мгновенного принятия сложного финансового решения;
- ✓ несоответствие складывающейся ситуации стандартной схеме;
- ✓ наличие указания на эксклюзивный, кастомизированный характер предложения.

Поведенческие стереотипы потерпевших от финансовых мошенничеств (I)

- ✓ нацеленность на высокий гарантированный доход, несоразмерный объему инвестиций или затратами труда;
- ✓ неадекватно высокий уровень доверия к контрагентам, граничащий с наивностью;
- ✓ отсутствие критического взгляда на фактическое состояние ситуации;
- ✓ нарушение регламента пользования финансовыми инструментами;
- ✓ невнимательность при осуществлении транзакций с банкоматами или с использованием программных продуктов;
- ✓ низкая финансовая грамотность;
- ✓ нежелание погружаться в детали сделки или читать условия договора в полном объеме;

Поведенческие стереотипы потерпевших от финансовых мошенничеств (II)

- ✓ отказ от советов и консультаций профессиональных юристов и экономистов при оценке и заключении сделки;
- ✓ готовность к принятию быстрых необдуманных финансовых решений;
- ✓ игнорирование предупреждений и дисклеймеров контролирующих и правоохранительных органов;
- ✓ потеря бдительности при взаимодействии с незнакомыми или малознакомыми контрагентами;
- ✓ технологическая отсталость в условиях современных финансовых взаимодействий;
- ✓ высокая готовность к риску, зачастую на грани «русской рулетки».

Статистика

В 2015 году в России было совершено 38 тысяч преступлений мошеннического характера с использованием средств мобильной связи. Рост по сравнению с 2014 г. – более чем на 50 %.

Ущерб от подобных преступлений в 2015 году составил 1,5 млрд. рублей.

Статистика

По данным Сбербанка годовой ущерб России от киберпреступлений составил **70 млрд. руб.** Ежедневно банк предотвращает кражи на **170-200 млн. руб.**

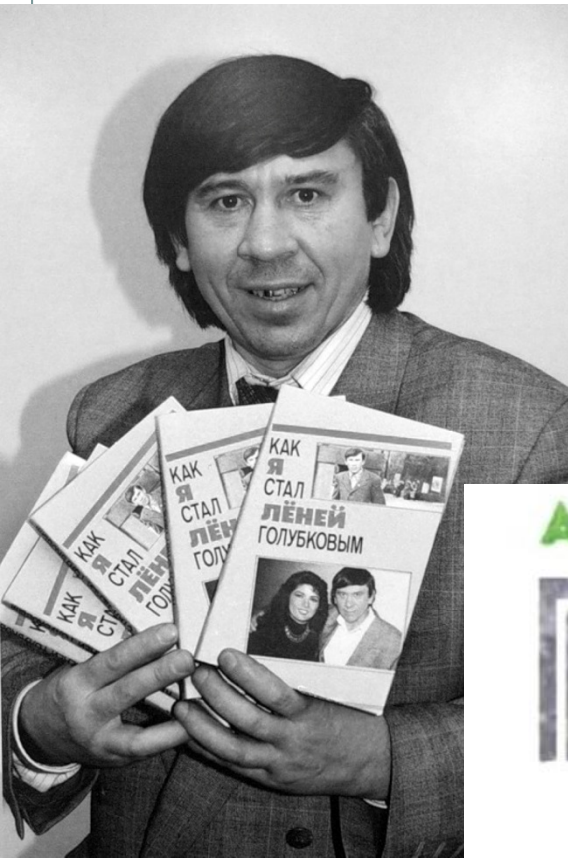
Ежегодные потери мировой экономики от кибератак Всемирный банк оценивает в **445 млрд. долл.**

Финансовая пирамида -

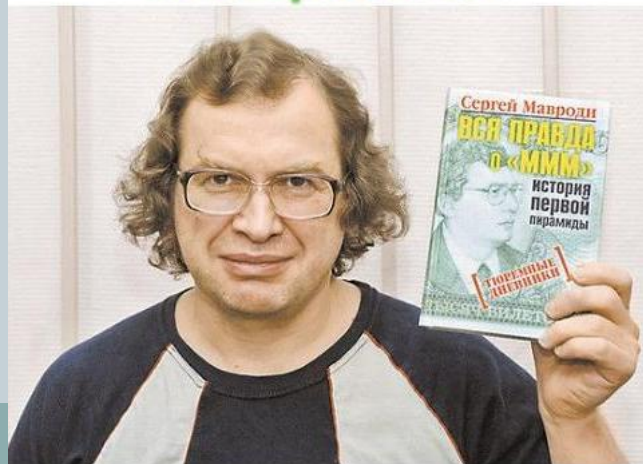


организация, обеспечивающая свой доход и доход инвесторов за счет постоянного привлечения денежных средств





АКЦИОНЕРНОЕ
ММ
ОБЩЕСТВО



Список крупнейших финансовых пирамид

Схема Понци

Португальская пирамида Доны Бранки

Схема «Двойной шах»

Схема Лу Перлмана

Европейский королевский клуб

Афера Бернарда Мейдоффа

Муравьиные фермы Вана Фэна

МММ Сергея Мавроди

Американская система страхования

Терминология

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.



*от англ. skim -
СНИМАТЬ СЛИВКИ

Терминология

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.

Внимание! Ваш E-Mail будет заблокирован!

От кого: "Служба поддержки Mail.Ru" <antispam000456040457@mail.ru>
Кому: [REDACTED]
Сегодня, 0:33 ! Важное

Ваша тема: мошенничество по почте

От кого: support@corp.ru **адресную книгу · в чейный список · в фильтры**
Кому: <marina@corp.ru>
Дата: 18 Мар 2010 00:48:33
Тема: Активация

адрес администрации @corp.mail.ru

win | loc | mac | utf

Английский > Русский

@mail.ru

Уважаемый пользователь!

Ваш E-Mail попал в чёрный список антиспама компании Mail.ru. Вам необходимо подтвердить, что Ваш E-Mail не используется для рассылки рекламных писем.

Для подтверждения Вашего электронного адреса, необходимо подтвердить Ваш электронный адрес. В противном случае согласно разделу 14 пункту 14.2 пользователь Администрации Mail.ru оставляет за собой право заблокировать Ваш аккаунт.

Пройти валидацию

Эти меры принимаются в связи с возросшим количеством спама. Администрация Mail.ru вынуждена ужесточить политику борьбы с ним.

С Уважением Администрация Mail.Ru

Здравствуйте Ув.пользователь.

Ваш аккаунт на сайте Mail.ru подозревается в массовой рассылке спам-сообщений. Для подтверждения того, что Вы не робот, введите заново свои регистрационные данные по ссылке расположенной ниже:

<http://win.mail.ru/cgi-bin/login?>

Если в течении 3-х дней Вы не подтвердите свои данные, мы будем вынуждены заблокировать Ваш аккаунт без возможности восстановить.

С Уважением, администрация Mail.Ru

Терминология

«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.

В переводе:

От: "Mrs. Olga Patarkatsishvili"

Тема: Re: Greetings From Mrs. Olga Patarkatsishvili

Привет из Грузии,

Приветствую вас во имя господне. Я миссис Ольга Патаркацишвили, вдова покойного грузинского магната мистера Бадри Патаркацишвили. У меня есть деловое предложение, которое принесет выгоду и вам, и мне. Я пришлю вам дальнейшую информацию, когда получу ваш ответ. Из соображений безопасности я вас очень прошу писать мне только на мой частный электронный адрес.

Пишите мне: *****@yandex.ru), чтобы узнать больше об этом проекте.

Спасибо за понимание.

Искренне ваша,
миссис Ольга Патаркацишвили



Madioc Abrams <madiocbramschamber@gmail.com>



2 июл. в 12:04

Перевести Создать правило Свойства письма

кратко ^

Уважаемый [REDACTED]

Я послал тебе это письмо месяц назад, но я не уверен, если вы получили его, как я не слышал от вас, и это является причиной, я повторной его. Я Ларри Екрота личный адвокат, чтобы покойный г-н Дема [REDACTED], бизнес и поставщик химических веществ / масло консультант, который умер вместе с его непосредственным семьи в страшной ДТП 26-го апреля 2007 года. Хранение количество долларов США 13,580.000. 00 млн. был обязан быть процесс передачи на ваше имя, следовательно, я связался с вами. Есть просьба связаться со мной через моего частного адрес электронной почты: madiocbramsat.law@gmail.com как можно скорее представить дополнительные разъяснения по этому вопросу.

с искренним уважением
Madioc Абрамс,

Терминология

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.

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.

Терминология

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



Групповая работа



2 группа: изучает и анализирует материалы «Примеры финансового мошенничества»

Вопросы:

- по каким признакам можно распознать мошенников?
- какие способы используют мошенники для «одурачивания» почтенных граждан?

Групповая работа



3 группа: изучить статьи УК РФ и ГК РФ, касающиеся финансового мошенничества

Вопросы:

- какая ответственность грозит за различные виды финансового мошенничества?
- какие факторы будут влиять на строгость наказания за финансовое мошенничество?

Групповая работа



- ***4 группа:***

подготовить памятку «Как защитить себя и свою семью от финансового мошенничества?»»

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

Хайп

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»

Формы мошенничества и способы минимизации рисков

IV. Мошенничество в социальных сетях

Сетевые домунники

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

Рефлексия



- сегодня я понял...
- сегодня я решил...
- сегодня я почувствовал...

Р.С. Эти знания полезны обеим
сторонам



Благодарим за внимание!