Тема 8.1.
Финансовое мошенничество

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».

Финансовое мошенничество

Статья 159 УК РФ

Мошенничество

«хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотребления доверием»

Финансовое мошенничество

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

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.

Формы мошенничества и способы минимизации рисков

I. Финансовые пирамиды

Формы мошенничества и способы минимизации рисков

II. Мошенничество с использованием банковских карт

а) offline:

- банкоматы и терминалы (в т.ч. скимминг)
- оплата в магазинах или ресторанах

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
- блокировать карту немедленно в случае утери/хищения

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

Формы мошенничества и способы минимизации рисков

II. Мошенничество с использованием банковских карт

б) online:

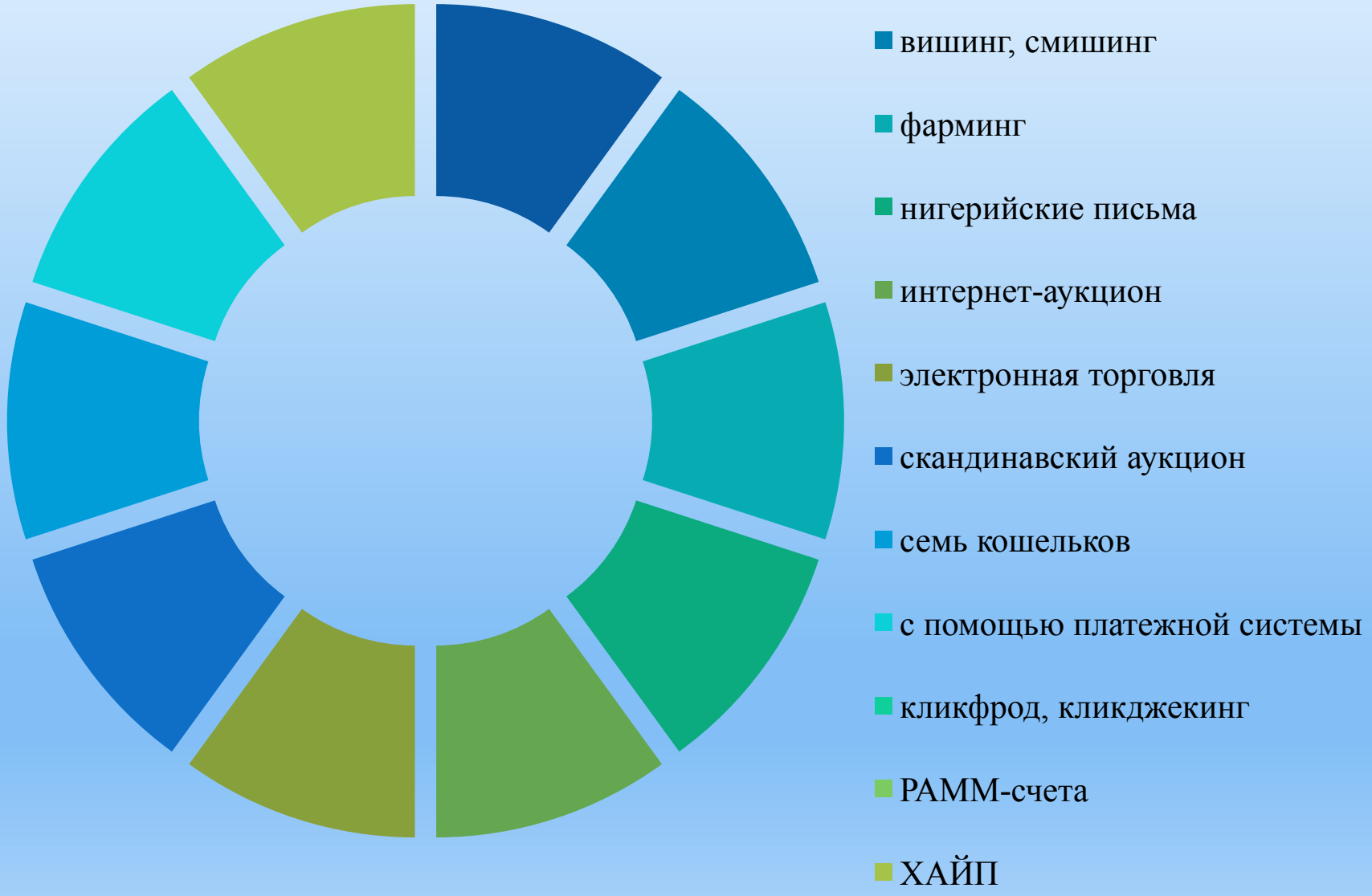
- интернет-мошенничества

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

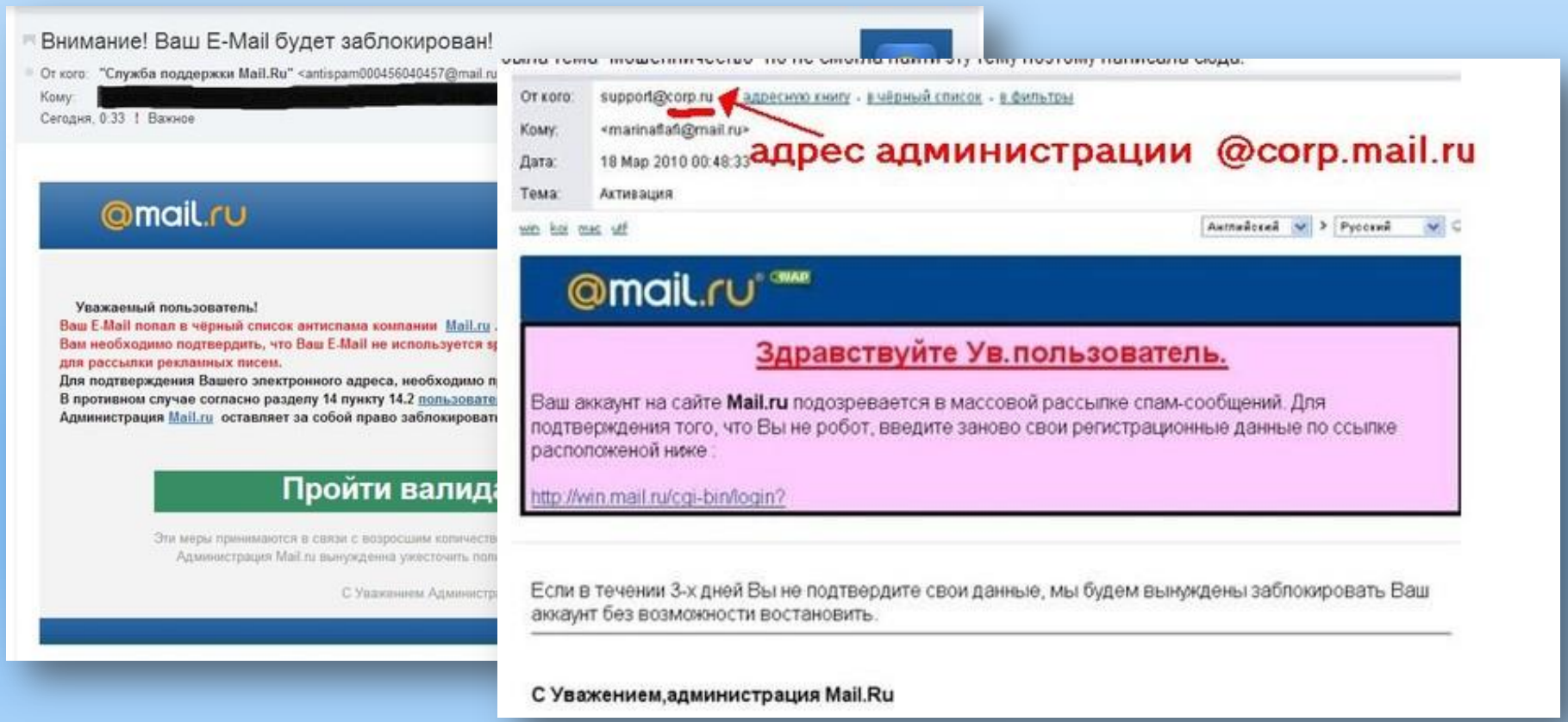
Формы мошенничества

III. Кибермошенничество



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.



Формы мошенничества и способы минимизации рисков

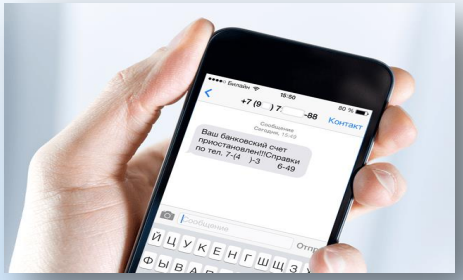
III. Кибермошенничество

Фишинг:

- а) почтовый
- б) онлайновый
- в) комбинированный

Способы минимизации рисков

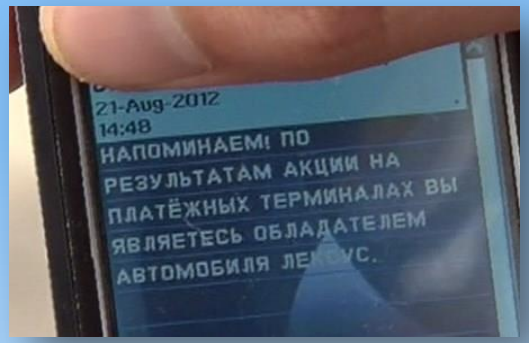
- проявлять осторожность
- застраховать карту от риска мошенничества
- использовать разные инструменты для разных видов расчетов
- использовать метод многофакторной аутентификации



Терминология

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.



Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

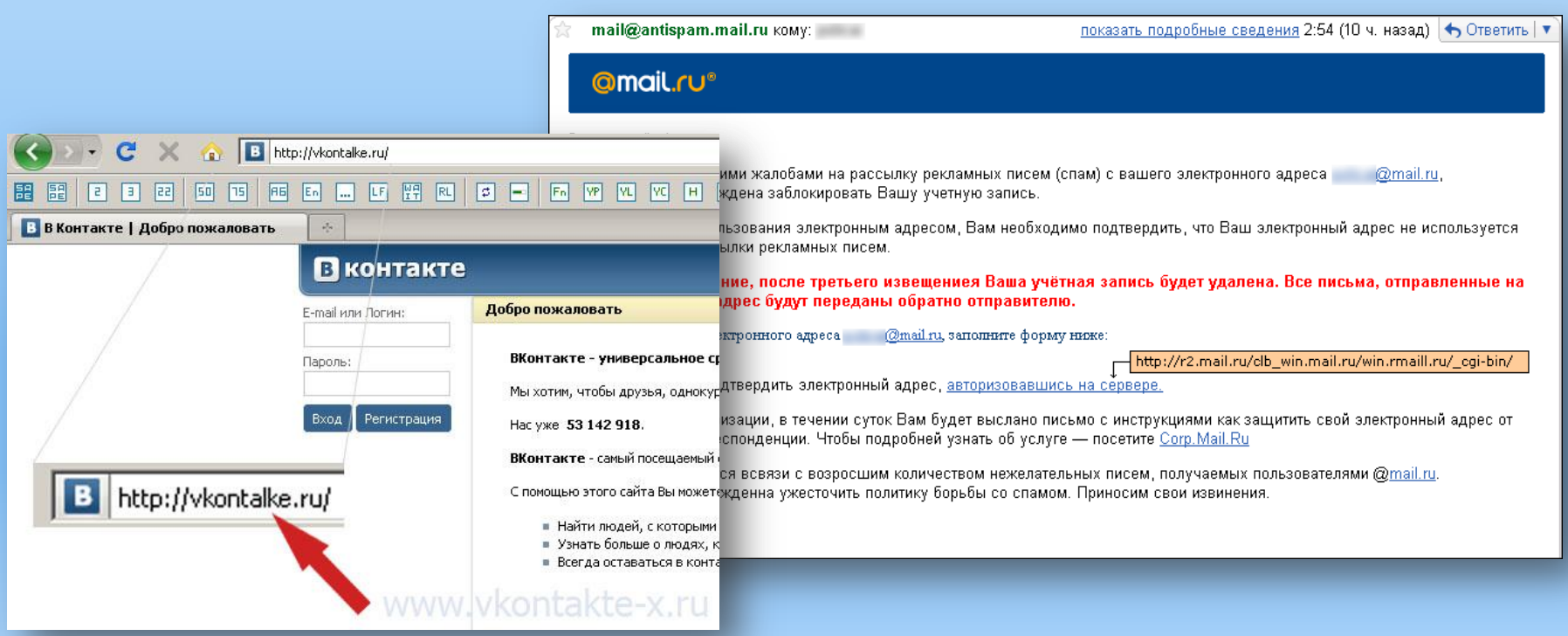
- Вишинг
- Смишинг

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

Терминология

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



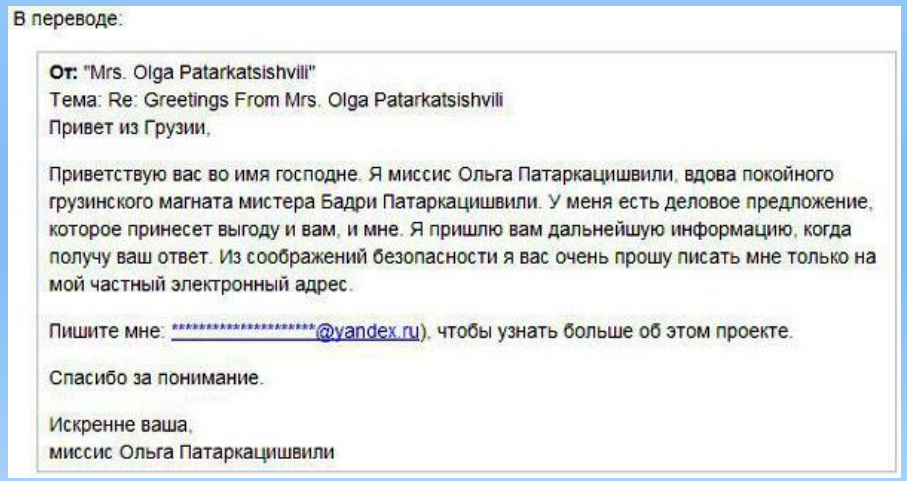
Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
Фарминг	• 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

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:

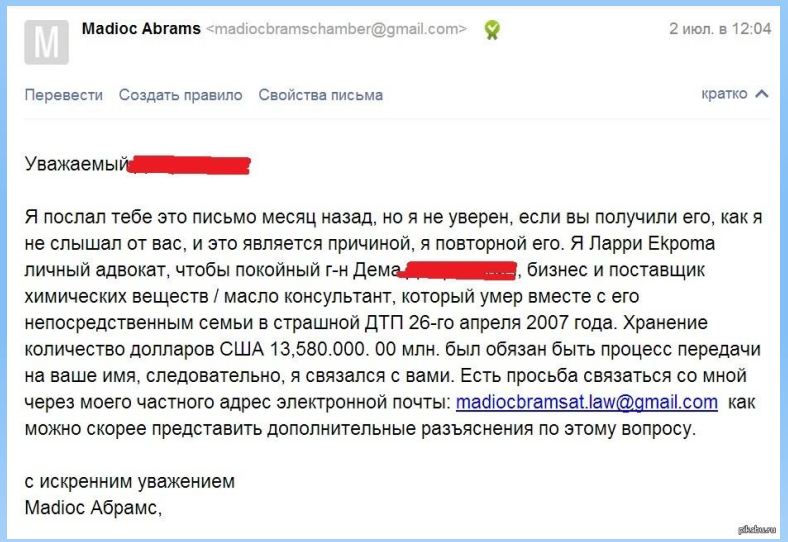
От: "Mrs. Olga Patarkatsishvili"
Тема: Re: Greetings From Mrs. Olga Patarkatsishvili
Привет из Грузии,

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 Екрома 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,

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

«Нигерийские письма»

Способы минимизации рисков

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

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

- Интернет-аукцион
- Электронная торговля
- Скандинавский аукцион
- Семь кошельков
- С помощью платежной системы

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*

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

Товара у вас нет. Претензии выставлять некому

*PayPal - крупнейшая дебетовая электронная платёжная система
Аналоги в РФ: Яндекс.Деньги, WebMoney

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 анг. 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.

Виды кликфрода

технические клики

клики рекламодателей

клики конкурентов

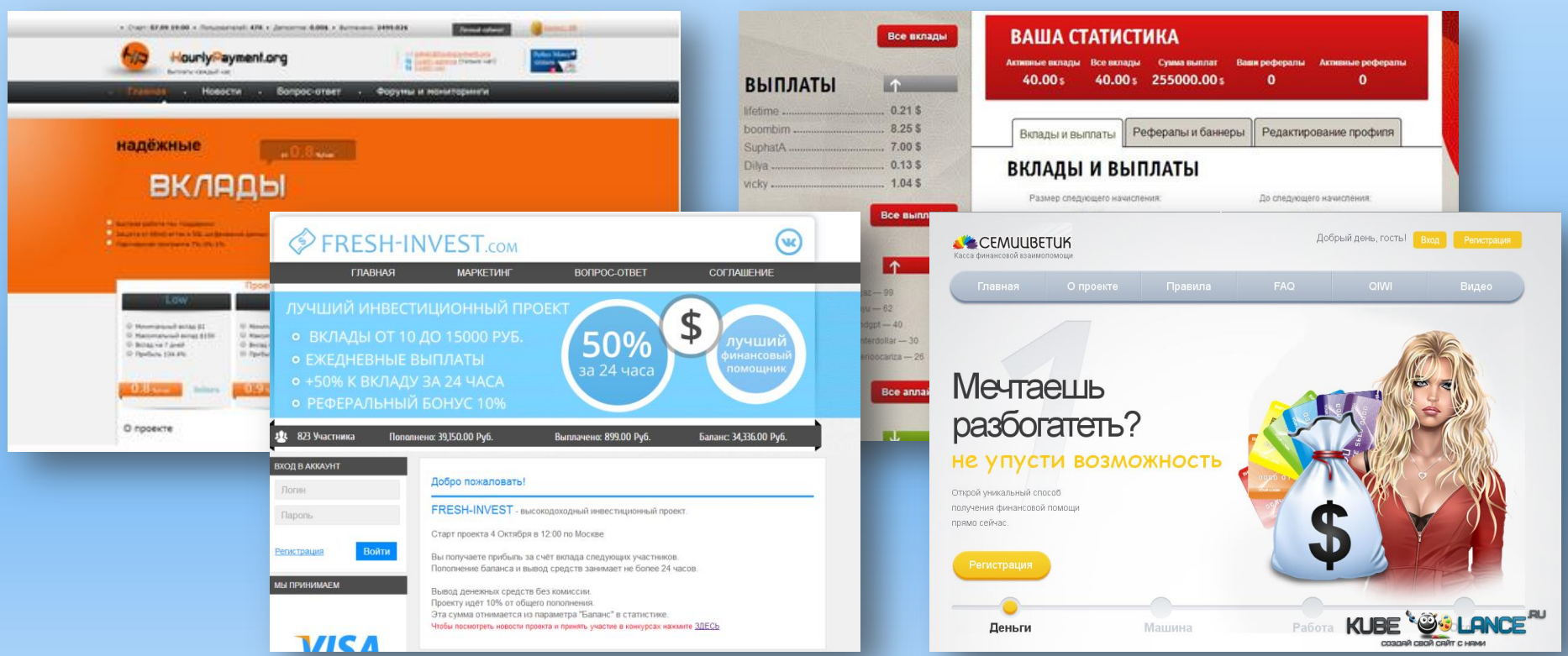
клики со стороны недобросовестных веб-мастеров

Терминология

PAMM-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.

Терминология

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



Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
Хайп	• 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»

Современные тенденции в кибермошенничестве

Социальное манипулирование (социальная инженерия) это метод управления действиями человека, основанный на использовании его слабостей и индивидуальных особенностей.

Техническая и технологическая инфраструктура используется только для обеспечения контакта.

Формы мошенничества и способы минимизации рисков

IV. 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

V. Другие виды финансового мошенничества

Финансовое мошенничество	Способы минимизации рисков
- обмен валюты	- 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.
- нелегальные кредиты	- 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.

V. Другие виды финансового мошенничества

брачные аферы

нелегальные азартные игры

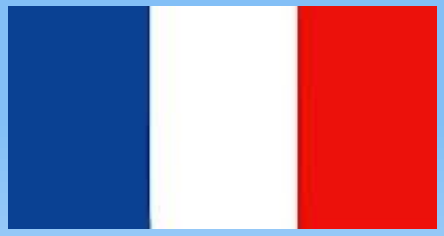
раздолжнители

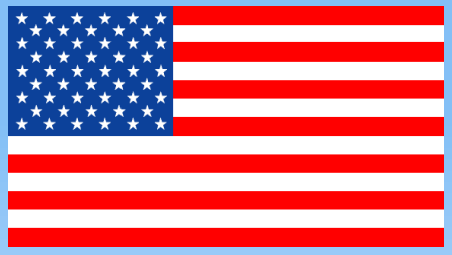
махинации с арендой/покупкой недвижимости или автомобилей

использование чужих паспортов для сомнительных сделок

Современный опыт законодательной борьбы с финансовым мошенничеством

Уголовное законодательство многих зарубежных стран имеет специальные нормы, посвященные уголовной ответственности за мошенничество.





Современный опыт законодательной борьбы с финансовым мошенничеством

Особенностью российского законодательства является то, что в нем **нет специальных норм по противодействию финансовому мошенничеству.**

Статья 159 УК РФ Мошенничество

Штраф	• исправительные работы • принудительные работами	• ограничение свободы • арест • лишение свободы

один или группой лиц	с использованием служебного положения	мошенничество с недвижимостью и в сфере предпринимательской деятельности

Современный опыт законодательной борьбы с финансовым мошенничеством

- 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 платежных карт
- Статья 159.5 УК РФ Мошенничество в сфере страхования
- Статья 159.6 УК РФ Мошенничество в сфере компьютерной информации