КРАЕВАЯ ПРОГРАММА «ПОВЫШЕНИЕ УРОВНЯ ФИНАНСОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ СТАВРОПОЛЬСКОГО КРАЯ И РАЗВИТИЕ ФИНАНСОВОГО ОБРАЗОВАНИЯ В СТАВРОПОЛЬСКОМ КРАЕ»

ЗНАНИЯ ДЛЯ ЖИЗНИ

МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дружи с финансами

мастер-класс «ФИНАНСОВЫЕ МОШЕННИЧЕСТВА И БЕЗОПАСНОСТЬ: ЗАЩИТИТЕ СЕБЯ И СВОЮ СЕМЬЮ»

КРАЕВАЯ ПРОГРАММА «ПОВЫШЕНИЕ УРОВНЯ ФИНАНСОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ СТАВРОПОЛЬСКОГО КРАЯ И РАЗВИТИЕ ФИНАНСОВОГО ОБРАЗОВАНИЯ В СТАВРОПОЛЬСКОМ КРАЕ»

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.

КРАЕВАЯ ПРОГРАММА «ПОВЫШЕНИЕ УРОВНЯ ФИНАНСОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ СТАВРОПОЛЬСКОГО КРАЯ И РАЗВИТИЕ ФИНАНСОВОГО ОБРАЗОВАНИЯ В СТАВРОПОЛЬСКОМ КРАЕ»

Финансовое мошенничество

*Согласно данным отчета, размещенного на официальном сайте ЦБ РФ, **в 2018 году** с использованием методов социальной инженерии было совершено **более 97%** хищений со счетов физических лиц и **39%** - со счетов юридических лиц.*

РАСПРОСТРАНЕННЫЕ ВИДЫ МОШЕННИЧЕСТВА:

- Телефонные мошенничества
- Интернет мошенничества
- Интернет и мобильный банк. Платежные системы.
- При совершении финансовых операций в банкоматах, небанковских платежных терминалах
- Прочие финансовые «разводы»

ЦЕЛЬ МОШЕННИКОВ – ПОЛУЧИТЬ:

- ваши персональные данные
- конфиденциальную информацию о ваших банковских данных, финансовых операциях (пароли доступа, коды активации платежных операций и т. п.)
- ваши деньги/имущество

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».

Формы мошенничества и способы минимизации рисков

I. Финансовые пирамиды

Финансовая пирамида –

это структура, в которой доход первым участникам выплачивается за счет вкладов последующих участников.

Последствия вложений в пирамиды.

Алина: "Инвестировала 100 000 кредитных. Малышу 2 годика, и еще дочка родится через месяц. В надежде на лучшую жизнь. А сейчас просто хочется рыдать, и света не видно в конце туннеля".

Ирина: "У меня кредит 500 тысяч, маленький ребенок. Помогите!"

Карина: "120 тысяч кредита и тоже декрет".

Руслан: "Миллион с копейками кредит остался. Похоже, квартиру продавать придется".

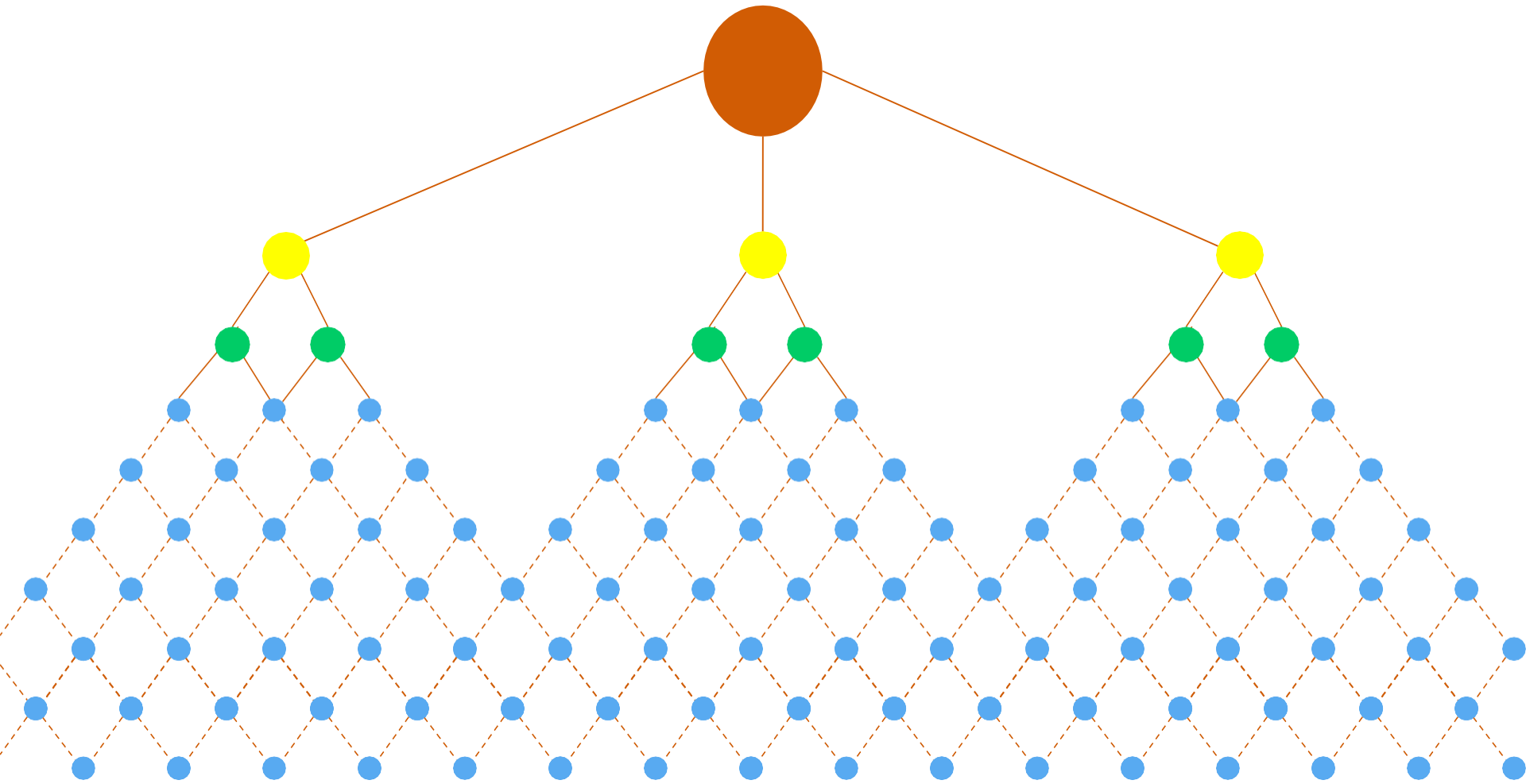
Денис: "У меня 300 тысяч кредит, выплатил только 50".

Альбина: "Кредиты с мужем на двоих у меня 280, у него 464 тысячи".

Татьяна: "У меня два маленьких сына, я мать-одиночка. И кредит 200 тысяч".

Юля: "Меня кинули на полмиллиона. Сейчас не работаю, получаю детские 3000 рублей. Взяла кредит, вступила 25 сентября. Не вывела ни копейки".

Классическая (многоуровневая) финансовая пирамида



Волны финансовых пирамид в России

Период	Примеры
Первая волна 1993 – 1998 гг.	«МММ», «Хопер-Инвест», «Властилина», Банк «Чара», «Русский дом Селенга», ГКО
Вторая волна 2008 – 2011 гг.	ООО «Золотая лига», «Глобал», «РуБин», «Бинар», МММ-2011, КПК РОСТ, Российская социальная программа.
Третья волна 2013 –2017 гг.	MBM.Partners, Impetra Plus, Академия Победителей, Сберкарта, Give1 Get4, SETinBOX , Руссинвест, РСП
Четвертая волна 2017 г. по настоящее время	Элитные клубы, хайп-проект, облачный майнинг, MLM –компании.

Варианты рыночного позиционирования финансовых пирамид

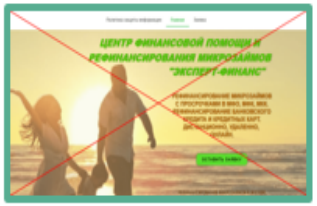
Типы и примеры пирамид

Проекты, позиционирующие себя как альтернатива потребительскому ипотечному кредитованию

Классические проекты, организованные на принципах сетевого маркетинга

«Псевдо профессиональные участники» финансового рынка

Проекты, работающие под видом микрофинансовых организаций, кредитно-потребительских кооперативов и ломбардов.



Проекты, предлагающие финансовые услуги по рефинансированию кредитных задолженностей.

Варианты рыночного позиционирования финансовых пирамид

Как вам такое предложение?

1. Доходность по инвестициям до 600% годовых
2. Ежедневное начисление доходности по инвестициям
3. Множество тарифных инвестиционных планов на любой вкус
4. Страхование инвестиций, гарантийный фонд залогового имущества

Микрозаймы

МИКРОЗАЙМЫ ЧАСТНЫМ ЛИЦАМ

ТАРИФ	СРОК	ДОХОДНОСТЬ
РАЗВИТИЕ	100 ДНЕЙ	НЕ ДОСТУПЕН
УЛЬТРА	200 ДНЕЙ	НЕ ДОСТУПЕН
ЛАКШЕРИ	400 ДНЕЙ	+220% ЗА СРОК

Преимущества инвестирования в микрозаймы:

- Высокая доходность
- Ежедневные выплаты
- Минимальные риски
- Разнообразие тарифов
- Мультивалютный кабинет

Займы малому и среднему бизнесу

ЗАЙМЫ МАЛОМУ И СРЕДНЕМУ БИЗНЕСУ

ТАРИФ	СРОК	ДОХОДНОСТЬ
РОСТ	100 ДНЕЙ	НЕ ДОСТУПЕН
ФЛАГМАН	200 ДНЕЙ	НЕ ДОСТУПЕН
ПРЕМЬЕР	400 ДНЕЙ	+260% ЗА СРОК

СТАТИСТИКА

ФИНАНСОВЫЕ ПИРАМИДЫ

По данным Центрального Банка РФ

в 2018г. россияне потеряли в финансовых пирамидах **более 2,7 млрд. руб.**

В 2019 году Банк России выявил

237 финансовых пирамид,

это почти в **1,5 раза больше**,

чем в 2018 году

Инновации в "пирамидостроительстве"

Пирамиды клубного типа

Хайп-проекты

CRP CENTER
ПРОФЕССИОНАЛЬНАЯ ПЛАТФОРМА

Современные бизнес-модели с элементами финансовых пирамид

Сетевой маркетинг (или многоуровневый маркетинг; англ. *multilevel marketing, MLM*) — концепция реализации товаров и услуг, основанная на создании сети независимых дистрибьюторов (сбытовых агентов), каждый из которых, помимо сбыта продукции, также обладает правом на привлечение партнёров, имеющих аналогичные права.

Компании, реализующие бизнес-модели на основе MLM

AVON

MARY KAY

Amway

HERBALIFE

oriflame

natural swedish cosmetics

Признаки финансовой пирамиды

Если Вы вложились в пирамиду и прогорели.

ЧТО ДЕЛАТЬ?

ШАГ ПЕРВЫЙ - составьте претензию и направьте ее в адрес компании заказным письмом с уведомлением. Или отнесите лично и удостоверьтесь, что его зарегистрировали. Возьмите расписку о получении, чтобы компания якобы случайно не потеряла ваше письмо.

ШАГ ВТОРОЙ- если компания отказывается вернуть деньги, то соберите все документы (от договоров до выписок о внесении средств на счет) и обратитесь в правоохранительные органы с заявлением.

ШАГ ТРЕТИЙ- свяжитесь с юристом и попробуйте найти других жертв мошенничества этой компании.

Если Вы вложились в пирамиду и прогорели.

ВЫ МОЖЕТЕ ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ:

- ✓ Банк России www.cbr.ru - бесплатный звонок - 8 800 250 40 72
- ✓ Общероссийский Проект «За права заемщиков» http://zapravazaemschikov.ru
- ✓ Союз защиты прав потребителей финансовых услуг (ФинПотребСоюз) http://www.finpotrebsouz.ru - бесплатная горячая линия - 8 800 707 05 21
- ✓ Конфедерация обществпотребителей (КонфОП). Союз общественных объединений «Международная конфедерация обществ потребителей» http://konfop.ru т.+7 (495) 722-16-27
- ✓ Федеральный общественно-государственный фонд по защите прав вкладчиков и акционеров http://fedfond.ru т. 8 (495) 989-72-80

Формы мошенничества и способы минимизации рисков

Банкоматы, небанковские платежные терминалы.

«Хотел воспользоваться терминалом Сбербанка. Передо мной на нем что-то бесконечно вводила девушка в чадре. Когда она отошла, я как обычно увидел: "Вставьте карту, введите пин-код..." — и 15 тыс. улетело на оплату чужого телефона»

Через «фальшивые» терминалы мошенники пытаются получить номер и Pin-код карты или Ваши деньги.

Списание завышенной комиссии за проведение платежа, либо все внесенные деньги без предоставления точной информации

Удержание денежных средств или **считывание с банковской карты** секретной информации с помощью специальных устройств

Формы мошенничества и способы минимизации рисков

Мошенничество с использованием банковских карт

a) 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

Интернет и мобильный банк. Платежные системы.

«Вчера моя карта Кукуруза была кем-то подключена к Apple pay (судя по входящему смс) и все деньги были переведены на Tele2. Никаких кодов подтверждения также не поступало и, соответственно, не отправлялось»

«Пару часов назад карта Кукуруза была привязана к Apple pay и, спустя пару минут, выведена существенная сумма денег без СМС»

Получение через общедоступные сети WI-FI доступа к вашему устройству

Получение данных или перевод денег путем использования **«поддельных» программ и интернет банка (фишинг).**

Заражение ваших устройств вредоносными ПО **через общедоступные сети WI-FI**

Получение мошенниками доступа **к Apple Pay и Google Pay** через NFC

Формы мошенничества и способы минимизации рисков

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 и способы минимизации рисков

Как заблокировать карту на примере ЦБ РФ

Через сотрудников отделения банка

Через контактный центр или клиентскую службу*

Через сервис Мобильный банк

Через Сбербанк-Онлайн

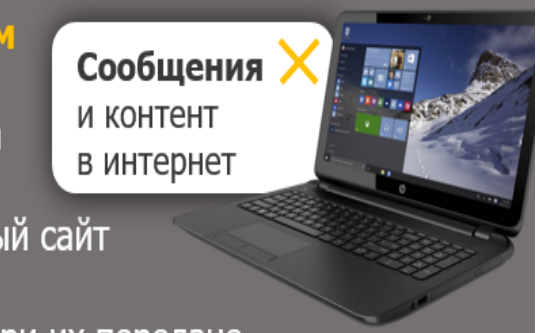
* Позвонив по номеру 8-800-555-55-50; 8-800-200-37-47 заблокировать карту при ее нахождении может и третье лицо

Формы мошенничества и способы минимизации рисков

Интернет мошенничества

К сотрудникам известного сервиса безопасности бренда обратился владелец веб-сайта, чей ресурс неожиданно оказался в черном списке антивируса.
Как оказалось, в страницу сайта был внедрен вредоносный код программы-скиммера, нацеленный на кражу денежных средств с карт пользователей. Кроме того, выяснилось, что злоумышленники заменили одну букву в названии адреса сайта на другую и обманом завлекали пользователя на поддельный сайт, отличающийся от оригинала на один символ.
Неподозревающие пользователи самостоятельно вводили свои данные, предоставляя таким образом мошенникам конфиденциальную информацию о себе.

Подделка сайта путем незначительного изменения адреса сайта и завлечение пользователей на данный сайт



Похищение данных при их передаче оператору-злоумышленнику на поддельном сайте

«Фальшивые» интернет-магазины – предоставление некачественного товара или не представление его совсем, завышение цен на товары, получение предоплаты за несуществующий товар.

«Ваш аккаунт заблокирован», пришлите СМС для получения кода доступа или перейдите по ссылке

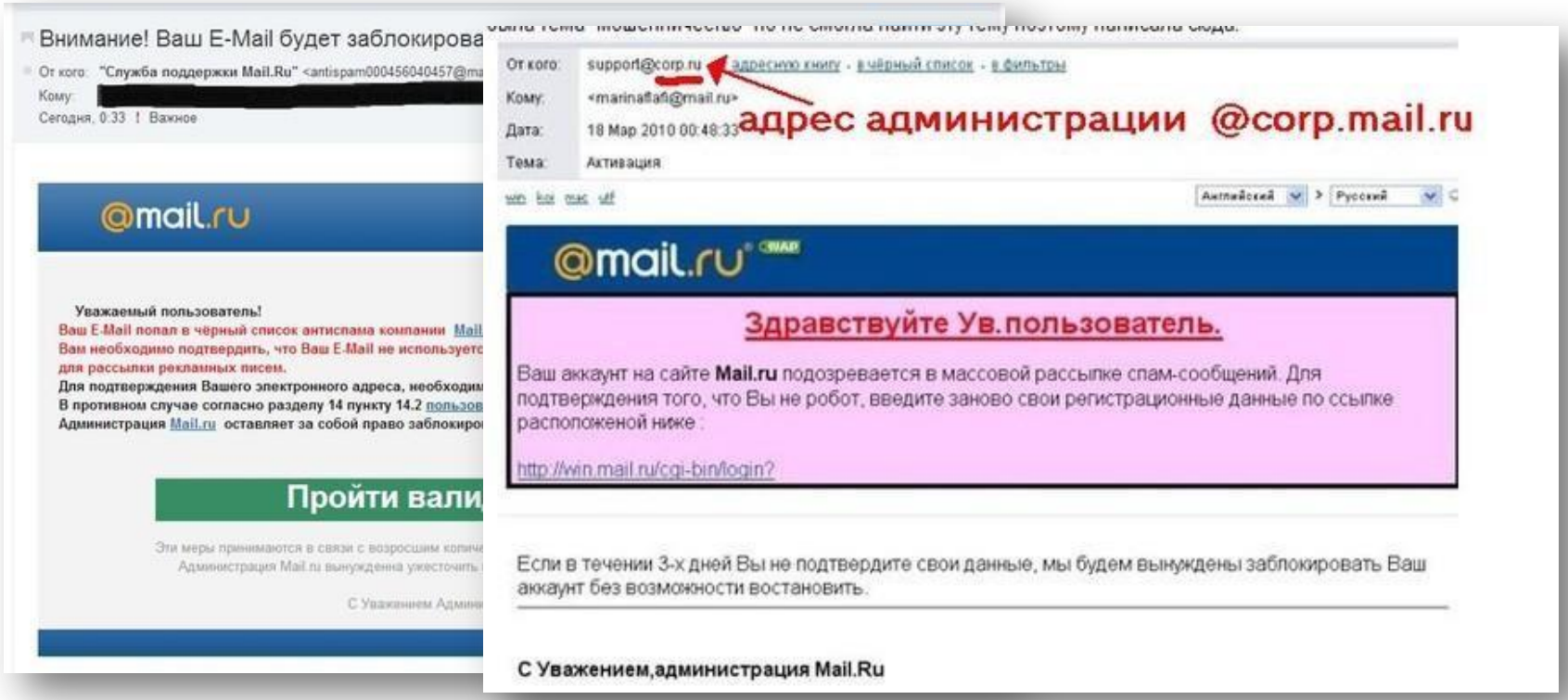
Формы мошенничества

Кибермошенничество

- *фишинг*
- *вишинг, смишинг*
- *фарминг*
- *нигерийские письма*
- *интернет-аукцион*
- *электронная торговля*
- *скандинавский аукцион*
- *семь кошельков*
- *с помощью платежной системы*
- *кликфрод, кликджекинг*
- *РАММ-счета*
- *ХАЙП*

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

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

Кибермошенничество

Вишинг

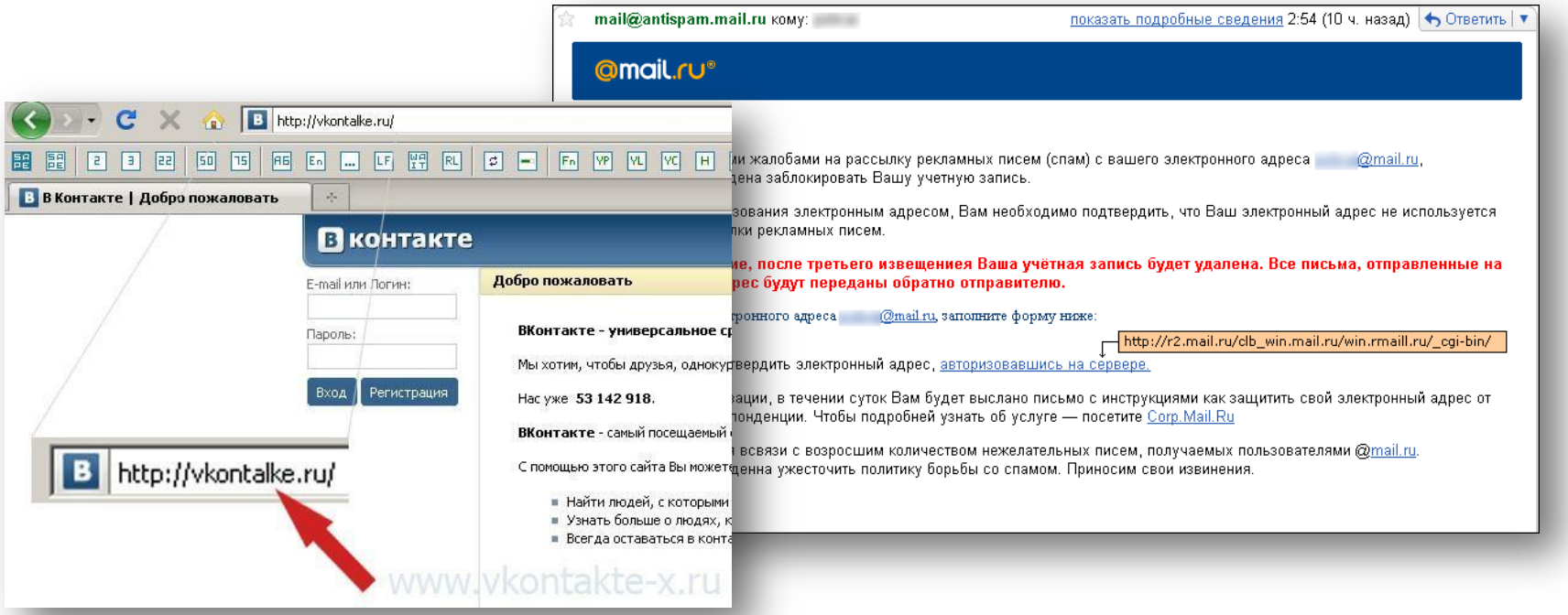
Смишинг

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

Кибермошенничество

Фарминг

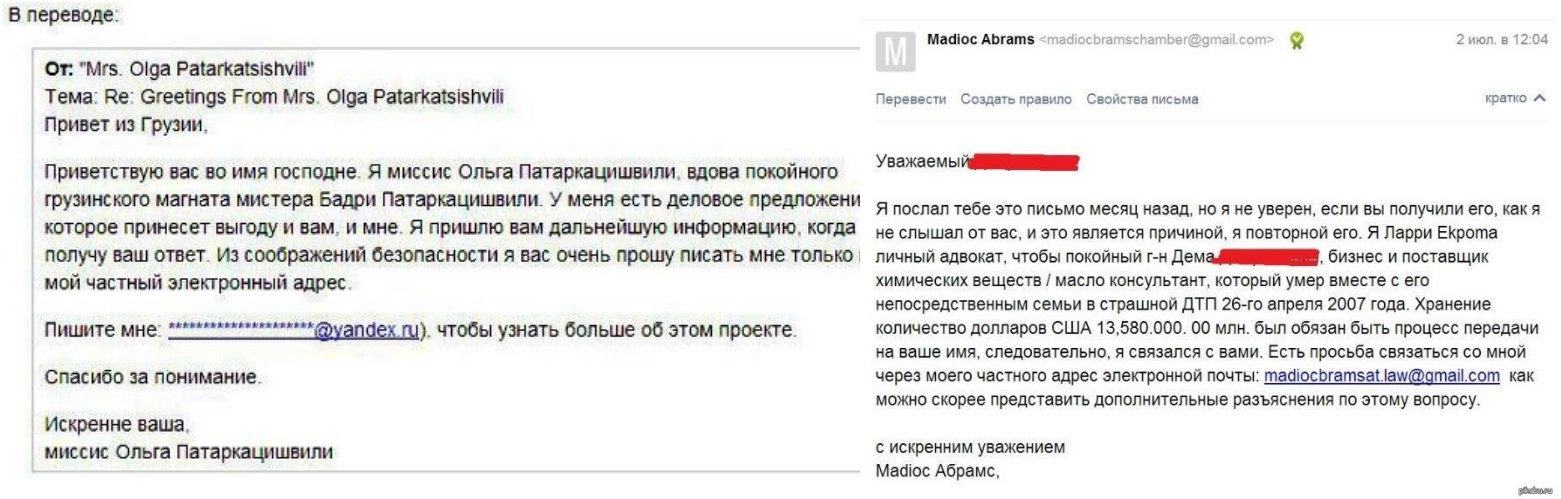
Способы минимизации рисков

- 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

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 предложени 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 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

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

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 платѐжная 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

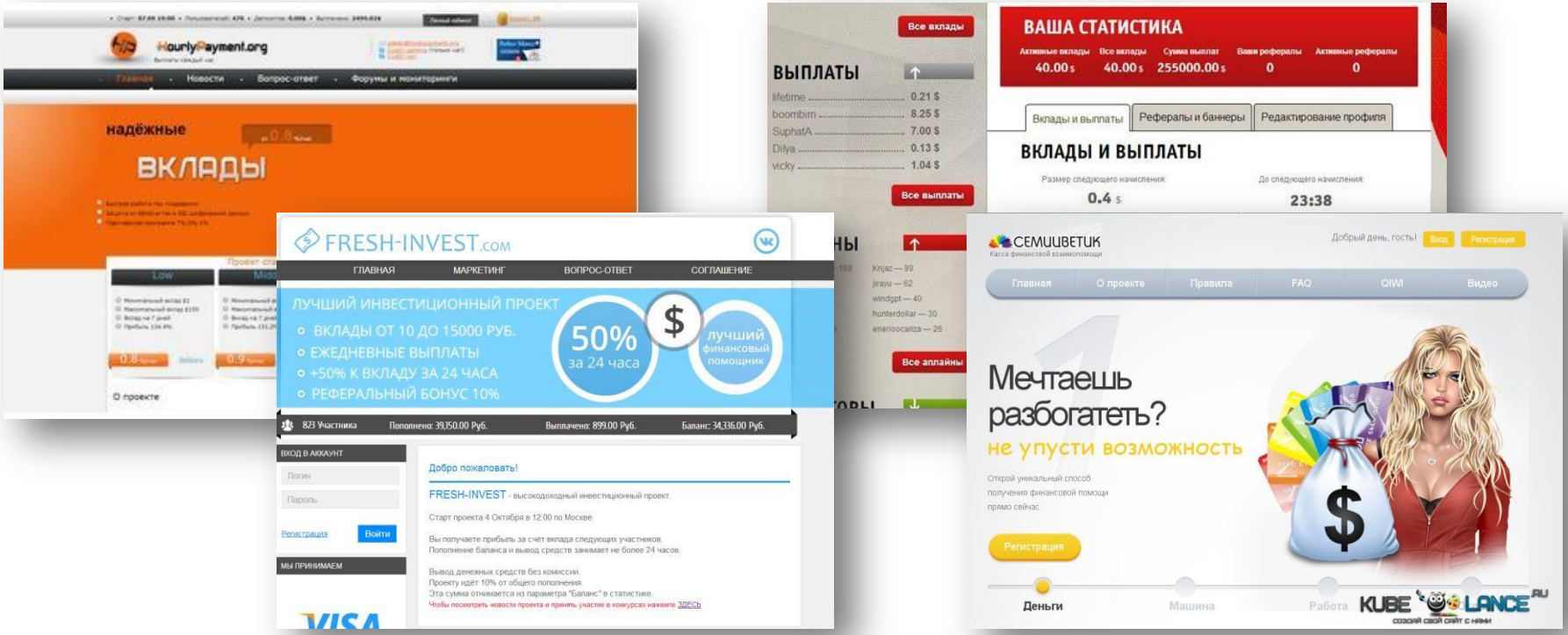
Клики со стороны недобросовестных веб-мастеров

Терминология

PAMM-счета (от англ. Percent Allocation Management Module – модуль управления процентным распределением) – специфичный механизм функционирования торгового счѐта, технически упрощающий процесс передачи средств на торговом счѐте 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

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»

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

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

Формы мошенничества и способы минимизации рисков

Телефонные мошенничества.

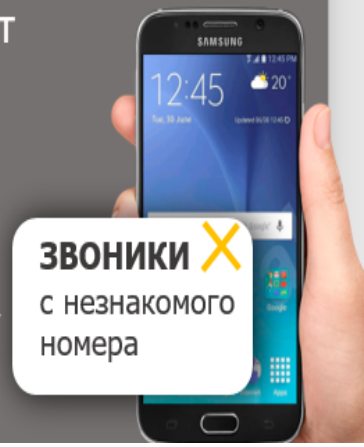
«Мне поступил звонок с городского телефона. Мужчина представился сотрудником ВТБ, назвал себя по имени и отчеству, так же обратился ко мне по имени и отчеству. Он сказал, что от моего имени получено заявление на закрытие счета, и спросил, в какое время и в каком отделении банка мне удобно получить деньги. Я понял, что это «развод» и прервал разговор. Потом я пытался дозвониться по этому телефону, но номер был неактивен...»

Мошенники звонят с коротких номеров, представляясь сотрудником различных организации

Звонят и представляются сотрудником банка и обманным путем получают Ваши банковские данные

«Сотрудники банка» предлагают вам перевести деньги на безопасный счет через удаленный доступ

Мошенники вводят Вас в заблуждение манипулируя безопасностью родных, знакомых, а также играют на Ваших слабостях



Формы мошенничества и способы минимизации рисков

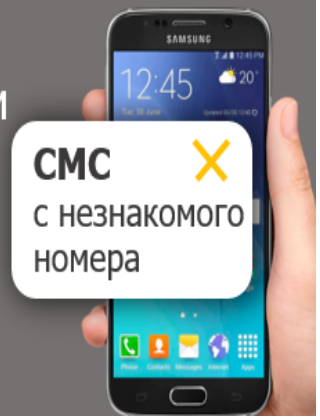
Телефонные мошенничества.

- **СМС с информацией о выигрыше** и предложением направить ответное СМС, позвонить, отписаться от рассылки
- **СМС от якобы друга/родственника** с просьбой срочно перевести деньги
- **СМС со ссылкой**, по которой нужно обязательно перейти
- **СМС с информацией**, что у вас задолженность по кредиту и просьбой перезвонить по указанному номеру
- **СМС с короткого номера** о зачислении денег и следом с просьбой вернуть деньги
- **СМС в мессенджерах** с подобными схемами обмана

Вам пишут/звонят не друзья,
а мошенники.

Вы попадаете
на «фишинговый» сайт, на котором передаете свои персональные данные или устанавливаете вредоносное ПО

Ответное СМС или звонок оказываются платными и очень дорогими



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.

Другие виды финансового мошенничества

Брачные аферы

Нелегальные азартные игры

Раздолжнители

Махинации с арендой/покупкой недвижимости или автомобилей

Использование чужих паспортов для сомнительных сделок

Методы защиты от финансовых мошенников

- **Не оставляйте телефон без присмотра** и не передавайте чужим людям.
- **Установите пароль** для разблокировки и доступа к личным данным.
- **Никогда не сообщайте никаких персональных сведений** кому-либо.
- **Удаляйте СМС,** которые получены с незнакомых номеров.
- **Перезванивайте** на реальные телефоны друзей и родственников, уточняйте у них информацию.
- **Отказывайтесь** от затяжных разговоров по странным темам.
- **Подключите СМС-информирование и СМС-уведомления** по банковской карте, в целях безопасности и контроля за вашими денежными средствами.
- **Не сообщайте никому CVV-код** и одноразовый пароль.
- **Заранее узнайте,** какова комиссия по вашему платежу.
- **Не допускайте посторонних** к банковской карте, электронному кошельку, мобильному телефону и компьютеру.
- **Сообщайте в финансовую организацию о потере банковской карты, «взломе»** электронного кошелька (данные карты стали известны посторонним или с нее без вашего согласия списаны деньги).
- **Используйте сложные** и разные пароли, не сохраняйте их в интернет-сервисах.
- **При пользовании банкоматом** обращайте внимание на посторонних вокруг, подозрительные устройства и накладки в местах ввода ПИН-кода и карты.

ЗНАНИЯ ДЛЯ ЖИЗНИ

МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дружи с финансами

Спасибо за внимание!