КАК ОПОЗНАТЬ ФИНАНСОВОГО МОШЕННИКА И ОБЕЗОПАСИТЬ СЕБЯ

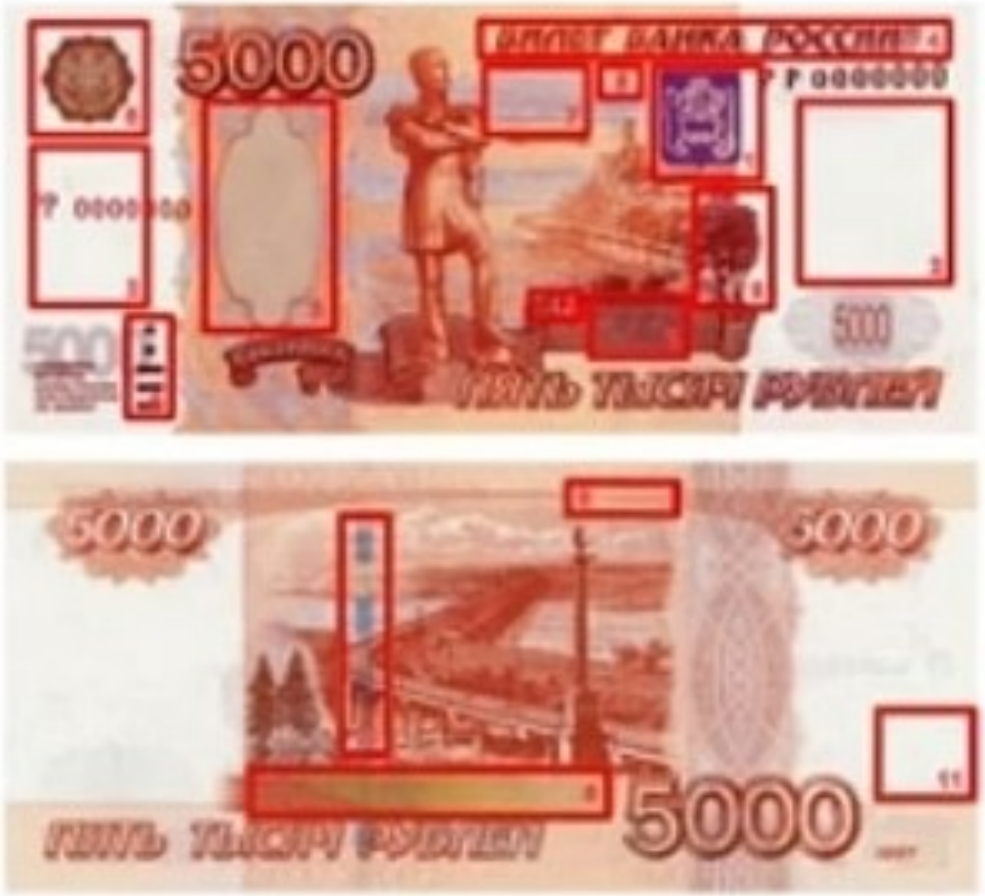
Финансовые ошибки и финансовое мошенничество

Финансовая ошибка – самостоятельные действия субъекта финансовых отношений, приведшие к потере денежных средств

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

Виды финансового мошенничества

Признаки фальшивых купюр



Главные детали для проверки на подлинность купюр:

- радужный эффект рисунка,
- лазерная перфорация,
- объемный водяной знак на полях купюры,
- кипп-эффект, или скрытое изображение, видное под острым углом,
- «ныряющая» металлизированная нить, которая внедрена в бумагу банкноты и видна только на одной стороне в виде толстой пунктирной линии.

Что делать при обнаружении фальшивой купюры?

Петр получил в банкомате купюр
в 1000 руб. При ближайшем
рассмотрении она показалась
ему странной.

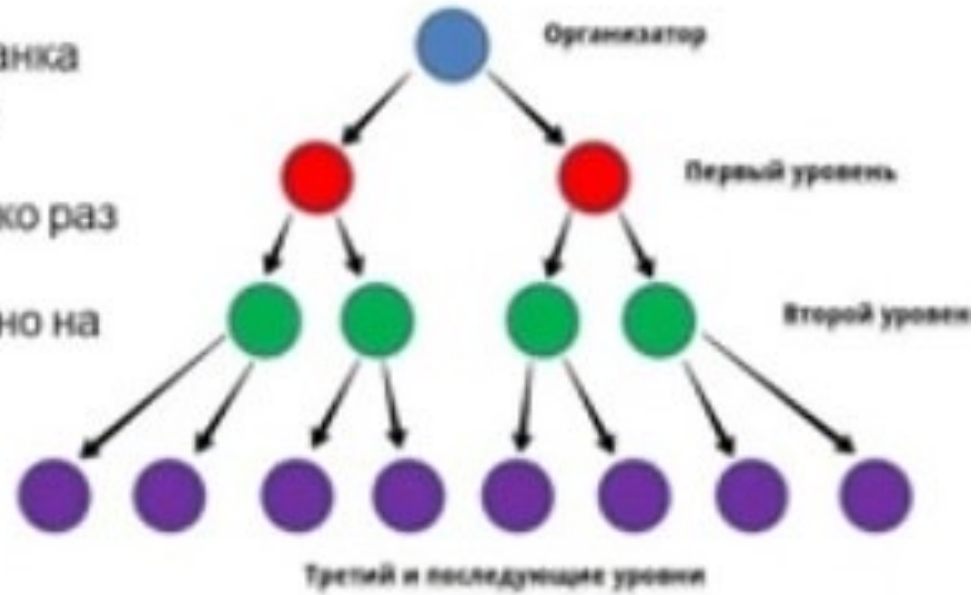
Как бы вы предложили поступить
Петру: пойти в магазин и
попытаться купить на фальшивы
деньги что-то или обратиться в
полицию?
Почему вы выбрали этот
вариант?

Финансовые пирамиды

Финансовые пирамиды - это мошеннические схемы по принципу обеспечения дохода через привлечение других участников «пирамиды» или вложения под проценты.

Признаки:

- отсутствие лицензии ФСФР 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);
- отсутствие какой-либо информации о финансовом положении организации.



Английская компания предлагает услуг по ивестированию ваших денег на фондовом рынке Великобритании.

Открытие счета осуществляется только по паспорту. Никаких иных документов не нужно. Полная конфиденциальност данных.

Минимальный уровень доходности составлет 80% годовых, но чаще клиенты получают 150-200% годовых, что обусловлено стабильность английской экономики в целом и фунтов стерлингов в частности.

Кроме того Вы будете получать по 10% от дохода приведенных вами в компанию клиентов.

На русской версии сайта вывешены красивые фото довольных клиентов и графики роста их финансового благополучия.

Отсутсиве каких либо документов аргументируется тем, что организация находится под защитой Британского законодательства и не подчиняется законодательству РФ.

Способы предотвращения финансового мошенничества при инвестировании

Не раскрывать ваши персональные данные незнакомым людям

- Персональную информацию (сведения о паспорте, СНИЛС, ИНН и т.п.)
- Сведения о вашей банковской карте (пин-код, CVV и т.п.
- Пароли и логины от электронной почты, личных кабинетов и пр.

Перед заключением каких-либо сделок убедиться в надежности компании

- 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

Финансовое мошенничество с использованием банковских карт

Оффлайн (через банкоматы и терминалы)

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.

Ольга Петровна решила снять с банковской карты часть наличных денежных средств для поездки на отдых. К сожалению ближайшее отделение банка в котором находился банкомат было закрыто и Ольга Петровна решила воспользоваться банкоматом своего банка в ближайшем торговом центре.

По пути она увидела еще один банкомат расположенный на улице рядом с магазином. Подойдя ближе и рассмотрев банкомат она увидела странные крепления на клавиатуре и картоприемнике банкомата. Ольга Петровна решила что безопаснее дойти до знакомого ей банкомата в торговом центре. Верны ли ее действия ?

Финансовое мошенничество с использованием банковских карт

Претекстинг - мошенники связываются с владельцем карты либо через телефон, либо по смс и обманным путем узнают от него данные по его карте по заранее заготовленному сценарию. Именно поэтому способ называется *претекстинг* (от англ. *pretext, предварительный текст*): мошенник озвучивает заранее заготовленный текст со всеми заготовленными психологическими ловушками.

- **Звонки от лица сотрудников банка**
- **Звонки от лиц сотрудников МВД**
- **СМС о блокировке карты / необходимости сменить пин-код и т.п.**

Меры предупреждения финансового мошенничества с банковскими картами

- 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
- Подключите услугу смс-оповещений о движении денежных средств по вашему счету

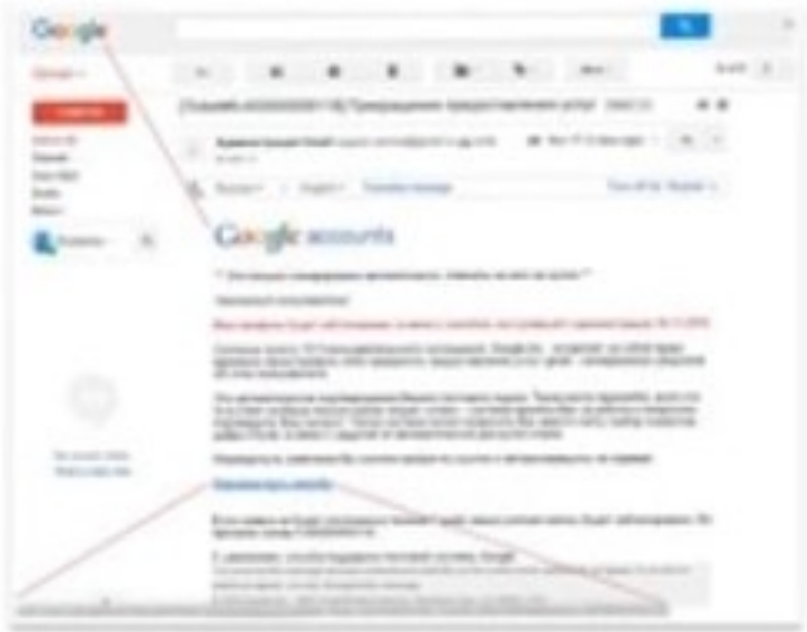
Мошенничество в социальных сетях

Сетевые домушники, интернетугонщики, сетевые грабители

Меры предупреждения:

- 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.

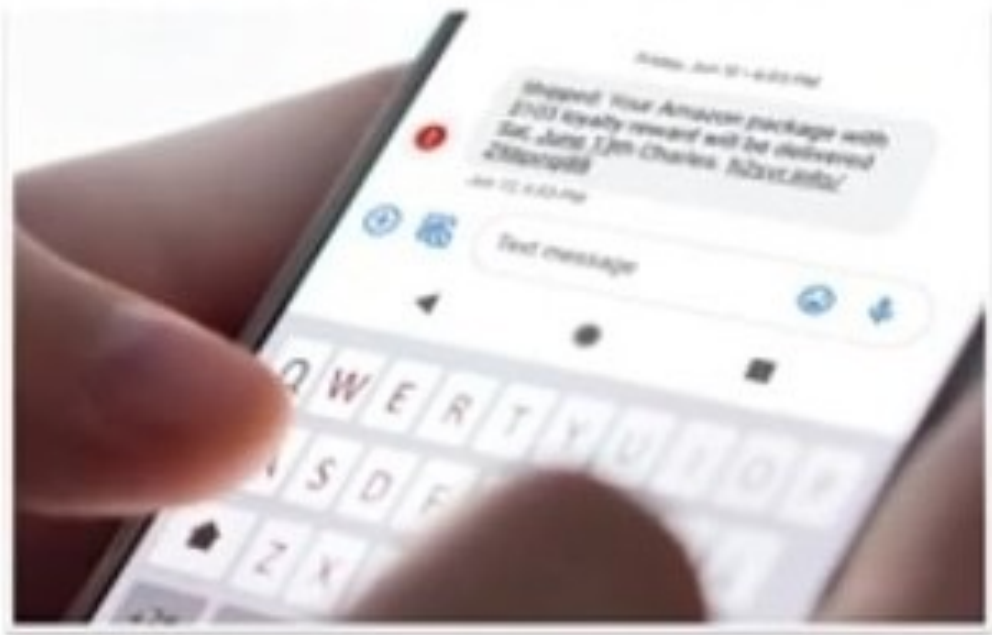
Кибермошенничество и его виды



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, онлайновый, комбинированный.

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

Кибермошенничество и его виды



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.

Кибермошенничество и его виды

Кликфрод (от англ. click fraud) — один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении.

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.

Способы защиты от кибермошенничества

Что делать если вы попались на уловки финансовых мошенников?

Спасибо за внимание!