Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»

Нижегородский институт управления
Факультет «Высшая школа государственного управления»

Пояснительная записка к выпускной работе по теме

Методическая разработка внеурочного занятия

«Финансовый практикум «Виртуальные ловушки»»
10 класс

Список слушателей, разработавших проект:

Белаш Елена Александровна,
учитель начальных классов МБОУ СШ с.п.Селекционной станции Кстовского МР
Безденежных Галина Витальевна,
учитель химии, МОУ Пижемская СОШ Тоншаевского МР
Ватрубина Ольга Михайловна,
учитель экономики, МБОУ «Школа № 125» г.Н.Новгород
Годухина Антонина Валентиновна,
учитель экономики, МБОУ № 4 Городецкого МР
Кнаус Татьяна Владимировна,
учитель экономики, МБОУ «Гимназия № 38» ГО г.Дзержинск

Кобзева Ольга Викторовна, методист РМЦ
Рак Евгения Алексеевна, преподаватель РМЦ

Проект допущен к защите
Старший методист РМЦ_____Н.А. Мартынова

Нижний Новгород, 2016г.

ВВЕДЕНИЕ

В современной России вопрос о финансовом образовании населения является актуальным, потому что у россиян нет достаточного опыта жизни в условиях рыночной экономики. Активное вовлечение России в мировое информационное пространство дало мощный толчок развитию коммуникационных технологий, компьютеризации всех сфер экономики и повседневной жизни практически каждого человека.

Компьютерные сети все шире применяются во многих областях жизни российского общества. Столь же быстро растет число преступлений, связанных с использованием сетевого доступа, множатся способы и формы совершения такого рода деяний. По оценкам специалистов МВД, каждый год через Всемирную паутину российские преступники похищают со счетов фирм около 450 млн.долл.

Интернет-мошенничество является современной разновидностью традиционного мошенничества. Самой уязвимой «аудиторией» мошенников являются подростки. Именно поэтому актуальным становится разработка и проведение серии занятий для школьников старших классов на тему «Виртуальные ловушки».

ОСНОВНАЯ ЧАСТЬ

Эпиграф к уроку**:** *«Знать, где ловушка – это первый шаг к тому, чтобы избежать ее» (Фрэнк Херберт)*

1) Общая характеристика занятия

Вид деятельности учащихся: *внеурочная деятельность*

Количество занятий по теме/ порядковый номер в теме: *1 / 1*

Тип занятия: *практикум*

Оборудование и/ или характеристика образовательной среды:

ПК с выходом в интернет – 2 шт., мультимедийный проектор, интерактивная доска, бумага, маркеры, раздаточный материал с кейсами, видеоролики, УК РФ.

2) Педагогическая характеристика занятия

Цели занятия: достижение не менее 95 % учащимися следующих образовательных результатов

<u>Предметные образовательные результаты</u>

Усвоение понятий по теме:

– мошенничество

– виды виртуального мошенничества: финансовые пирамиды, фишинг, фарминг, нигерийские письма, скандинавский аукцион, смс мошенники, попрошайки в сети, легкий заработок.

Овладение предметными умениями:

- умение распознавать виртуальные «ловушки»;

- знание о возможностях виртуального финансового мошенничества и что нужно делать, чтобы не стать жертвой мошенников;

<u>Метапредметные образовательные результаты:</u>

- умение самостоятельно определять цели деятельности

- умение объяснять явления, процессы, связи, выявленные в ходе практической деятельности;

- умение работать в группе: учитывать разные мнения, стремиться к координации различных позиций в сотрудничестве.

3) Методическая характеристика занятия:

Структура урока

Этапы урока	Деятельность учителя	Деятельность учащихся
I.Проектировочный этап (погружение в проблему) 5 минут	Вводное слово учителя. Показ видеоролика «Как не стать жертвой виртуальных мошенничеств» (Приложение 1). Представление результатов предварительного анкетирования учащихся (Приложение 2).	Просмотр видеоролика. Учащиеся анализируют просмотренный видеоролик и результаты анкетирования и приходят к выводу о недостаточности имеющихся у них знаний о возможных финансовых мошенничествах в сети Интернет, а также о том, как не стать жертвой виртуальных мошенников. Формулируют тему и цель занятия.
II Этап реализации: 2.1. Работа в группах 15 минут.	Учитель предлагает учащимся сформировать 8 групп для работы с кейсами Учитель предлагает каждой группе выполнить определенный кейс. 1 группа – теоретический (Приложение 3)	Учащиеся формируют группы по 3-4 человека и выбирают спикера каждой группы. Учащиеся решают полученные кейсы. 1 группа теоретики: отвечают на заданные вопросы, используя различные источники информации: Интернет-ресурсы, учебное

	2-8 группы – анализ практических ситуаций (Приложения 4-10)	пособие, УК РФ. 2-8 группы – практики: работают с кейсами (разбирают практические ситуации виртуальных ловушек, разрабатывают рекомендации, как избежать конкретной ловушки)
2.2. Представление результатов работы групп и их обсуждение. 15 минут	Координирует деятельность учащихся по заполнению кластера. Учитель предлагает группам 2-8 определить к какому типу Интернет-мошенничества относятся ситуации, представленные в кейсах. Учитель предлагает проанализировав предложенные каждой группой рекомендации,	Представляют результаты своей работы, участвуют в обсуждении, оформляют кластер «Виртуальные ловушки» на плакате: 1 группа – заполняют структуру кластера (на доске) Учащиеся 2-8 групп: 1) с помощью теоретиков (при необходимости) определяют тип мошенничества в предложенной ситуации. 2) представляют выводы, полученные в ходе анализа практических ситуаций, предложенных в кейсах; 3) дополняют кластер рекомендациями, как избежать конкретных ловушек. Учащиеся просматривают предложенный видеоролик Учащиеся анализируют предложенные каждой группой рекомендации и разрабатывают общие

	разработать общие правила безопасного обращения с финансами и персональными данными в сети Интернет. Учитель фиксирует предложения учащихся в кластере. Учитель предлагает в качестве закрепления материала просмотреть видеоролик «Остерегайся мошенничества в интернете» (Приложение 11).	правила безопасного обращения с финансами персональными данными в сети Интернет. Учащиеся просматривают предложенный видеоролик «Остерегайся мошенничества в интернете»
III Этап оценки и рефлексии 10 минут 3.1. Оценка результата 3.2. Рефлексия	Учитель организует работу учащихся по выполнению итогового теста (с последующей самопроверкой) (Приложение 12) Учитель проводит рефлексию. (Приложение 13) Подведение итогов занятия В качестве домашнего задания можно предложить: - найти в сети Интернет, какие еще виртуальные «ловушки» существуют и дополнить кластер; - подготовить выступление для родителей и других учащихся на тему «Как не стать жертвой мошенничества в сети Интернет» - разработать памятки, буклеты «Виртуальные ловушки» (Приложение 15).	Учащиеся выполняют тест. Каждый учащийся высказывается одним предложением, выбирая начало фразы из списка на экране.

ЗАКЛЮЧЕНИЕ

Тема занятия выбрана не случайно, так как современные подростки легко попадаются на «удочку» виртуальных мошенников. И не все из них знают, как себя вести в той или ситуации, связанной с данной проблемой.

При планировании данного занятия, учитывались возрастные особенности детей. Занятия с ними традиционно ведутся по технологии проблемного обучения. Данная технология предполагает, что дети сами открывают для себя новые знания, поэтому и «открытие» нового знания осуществляется посредством деятельностного метода в форме подводящего диалога.

В ходе проведения занятия использовался такие приемы работы с информацией, как кейс – стадии и кластер. Метод кейсов — техника обучения, использующая описание реальных экономических, социальных и бизнес-ситуаций. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

Использование кейс-метода позволяет активизировать различные факторы: теоретические знания по тому или иному курсу, практический опыт обучаемых, их способность высказывать свои мысли, идеи, предложения, умение выслушать альтернативную точку зрения, и аргументировано высказать свою.

С помощью этого метода учащиеся имеют возможность проявить и усовершенствовать аналитические и оценочные навыки, научиться работать в команде, применять на практике теоретический материал.

Кластер — это графическая форма организации информации, когда выделяются основные смысловые единицы, которые фиксируются в виде схемы с обозначением всех связей между ними.

Были использованы такие ф*ормы работы, как:* фронтальная,

групповая. Происходит чередование различных видов деятельности. На уроке реализованы следующие дидактические принципы: Системность, научность, доступность, проблемность, принцип интереса.

Материал данного занятия может быть использован учителями как в урочной (на уроках экономики, обществознания, информатики), так и во внеурочной деятельности (классные часы, факультативы).

СПИСОК ИСПОЛЬЗОВАННЫХ ДОКУМЕНТОВ И ИСТОЧНИКОВ ИНФОРМАЦИИ

Учебник и/ или учебное пособие для учащихся:

Брехова Ю.В, Алмосов А.П., Завьялов Д.Ю. ФИНАНСОВАЯ ГРАМОТНОСТЬ. Материалы для учащихся. 10–11 кл.

Методические материалы для учителя:

Брехова Ю. В., Алмосов А. П., Завьялов Д. Ю. ФИНАНСОВАЯ ГРАМОТНОСТЬ. Методические рекомендации для учителя. 10–11 кл.

Интернет – источники:

http://asbseo.ru/moshennichestvo/moshennichestvo-v-internete.html - ролик «Остерегайся мошенничества в интернете»

https://мвд.рф/document/1910260

https://www.newstube.ru/media/kak-ne-stat-zhertvoj-virtualnogo-moshennichestva - видео «Как не стать жертвой виртуального мошенничества»

Материалы для кейсов:

http://nesoridengami.ru/moshennichestvo-v-internete/213-sms-moshennichestvo.html

http://finfact.org/piramidy

http://www.pcbee.ru/money/kak-i-skolko-zarabatyvayut-poproshajki-v-internete.html

http://int-net-partner.ru/voprosy-novichkov/moshennichestvo-v-internete.html#1.-poproshajki-v-seti

http://fb.ru/article/171737/moshennichestvo--eto-chto-takoe-vidyi-shemyi-primeryi-moshennichestva-otvetstvennost-za-moshennichestvo

Приложения.

Приложение 1.

Видеоролик «Как не стать жертвой виртуальных мошенничеств».

(http://asbseo.ru/moshennichestvo/moshennichestvo-v-internete.html)

Приложение 2

Анкета (входная).

1. Финансовое мошенничество – это:
    a) Правонарушение, совершение которого влечёт применение к лицу мер уголовной ответственности.
    b) преступление, заключающееся в завладении чужим имуществом (или приобретении прав на имущество) путем обмана или злоупотребления доверием.
    c) Кража денег.
2. Какие виды интернет-мошенничества Вам известны. Впишите:

    _____
3. Сталкивались ли Вы или Ваши друзья, близкие с мошенничеством в сети интернет?
    a) Да
    b) Нет
4. Как Вы считаете, нужно ли уголовное наказание за интернет-мошенничество?
    a) Да
    b) Нет

Задание теоретикам.

Уважаемые теоретики! Мы предлагаем вам, используя, различные источники информации (статья из Интернета, учебное пособие, УК РФ) ответить на следующие вопросы:

1. Что такое мошенничество?
2. Какие виды виртуального мошенничества существуют ?
3. Используя не более 10 слов, дайте краткую характеристику основным видам виртуальных мошенничеств. Результат представьте в виде элемента кластера (название - краткая характеристика)

Интернет-ресурсы по теме «Виртуальное мошенничество»
http://dyly.ru/moshennichestvo-v-internete-novye-vidy-i-sxemy/
http://vse-temu.org/new-kakim-byvaet-moshennichestvo-v-internete.html

Виды мошенничества в сети интернет. Как не стать жертвой мошенников...

(http://www.advokativanov.ru/mosh2.html)

Что делает среднестатистический пользователь в Интернете? Ищет информацию, скачивает музыку и фильмы, пишет в блог, посещает развлекательные сайты, пользуется почтой и т.п. Но вот однажды он сталкивается с заманчивым предложением заработать энную сумму денег за короткое время. Неважно, что именно ему предлагают, в его голове уже начинают крутиться мысли о легком заработке. Даже если он достаточно осторожен и не доверяет всему, что пишут, качественный дизайн и грамотный текст могут развеять все его сомнения. Что уж говорить о неопытных подростках… Человек отсылает нужную сумму на кошелек или проводит какие-то другие действия, и терпеливо ждет. Мошенник же получает свои деньги.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег с простодушных пользователей. Практически полная безнаказанность, анонимность мошенников, большое количество доверчивых людей – все это подпитывает такой вот своеобразный вид ‘бизнеса’.

Большинство пользователей просто забывают о том, что в Интернете действуют те же законы, что и в жизни. Сейчас редко найдешь человека, который бы попытался выиграть у наперсточника на вокзальной площади, а вот когда ему же предложат отослать деньги на так называемый ‘волшебный’ кошелек, с тем, чтобы потом получить удвоенную сумму, все защитные психологические барьеры вдруг оказываются снятыми, и он с радостью соглашается. Все это напоминает 90-е годы, когда люди только после своего горького опыта (и чаще неоднократного) становились более осторожными, встречаясь с очередным предложением ‘легких’ денег. В Интернете, как мы видим, ‘90-е’ в самом разгаре…

Главное, что нужно помнить всем - ‘халявы’ не бывает. Никто никогда не даст денег просто так. Деньги не появляются из неоткуда, даже если они ‘электронные’. А Интернет – это просто средство передачи информации.

Как известно, средствами получения денег является либо производство товаров, либо предоставление услуг. Для Интернета данное утверждение звучит так: либо вы получаете прибыль с производства интеллектуальной собственности, либо с предоставления сопутствующих услуг....

1. Мошенничества, связанные с Интернет-магазинами.

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.

Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.

Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.

Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

2. Фишинг.

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.

Одной из разновидностью данного вида правонарушения являются звонки на сотовые телефоны граждан якобы от представителей банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что никакого кредита не брал, ему предлагается уточнить данные, содержащиеся на пластиковой карте. Этого уже достаточно для покупки товаров в Интернет-магазинах.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.

3. Интернет-попрошайничество.

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

4. Мошенничества в отношении иностранных граждан (брачные аферы).

Не встретив в реальной жизни свою половину, многие мужчины продолжают искать ее в Интернете. Поиски начинаются на сайтах знакомств и дневниках, где будущие избранницы размещают свои фотографии.

Этим пользуются злоумышленники, используя фото девушек, привлекая психологов, программистов, переводчиков и посредством этих сайтов завязывают переписку с доверчивыми иностранцами.

Западные женихи «клюют» на объявления, где нетребовательные русские красавицы говорят о том, что нуждаются в серьезных отношениях. А взамен вечной любви, порой после месяцев переписки, просят решить их финансовые проблемы - помочь обеспечить сиделкой больных родителей, расплатиться с кредитом, перевести деньги на перелет к жениху в дальнее зарубежье и т.д.

После получения денег невесты перестают выходить на связь. Пылкие иностранные поклонники, поняв, что их обманули, обращаются в полицию. Злоумышленники рассчитывают только на женихов из дальнего зарубежья, т.к. представители ближнего зарубежья предпочитают приехать в гости к невесте сами, что невыгодно для мошенников.

5. Осторожно!!!!! Вирус!!!!!

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для

входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная.

Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения, например:

- программка для бесплатной отправки подарков! - http://re-url.me/abc, мне не забудь отправить!

- привет. http://www.894.joo.ru. Лови программку по бесплатному повышению рейтинга, но не давай никому больше. Это не спам.

Основные темы, которые используются для «рекламы» скачивания и запуска зараженных программ:

- бесплатное повышение рейтинга «ВКонтакте»;
- программа перехвата SMS сообщений с телефона;
- дополнительные функции в социальных сетях, которые не существуют (подарки, VIP-доступ и т.д.)

После перехода по ссылке компьютер пользователя автоматически запускает вредоносную программу.

Наши рекомендации

Пострадавшим рекомендуется изменить пароль доступа к указанным ресурсам, а также установить версии антивирусных программ с обновленными антивирусными базами.

Следует помнить, что ресурсы популярных сайтов никогда не потребуют от уже зарегистрировавшегося пользователя дополнительной авторизации, тем более за деньги путем отправки смс.

6. Осторожно!!! Новый вид мошенничества!!!

В Российском сегменте сети Интернет стала появляться информация о так называемых «звуковых» наркотиках, якобы оказывающих влияние на бинауральные ритмы человека. Реклама аудионаркотиков осуществляется посредством массовой рассылки писем на электронные почтовые адреса пользователей и на номера в системах быстрого обмена сообщениями. Доступ к прослушиванию аудио-файлов возможен после введения специального цифрового кода, получение которого происходит исключительно после оплаты в виде отправки смс-сообщения. Ресурсы, предлагающие такого рода продукцию, располагаются на площадях зарубежных провайдеров и зарегистрированы по фиктивным анкетным данным.

По мнению специалистов, достичь рекламируемого эффекта посредством звуковых колебаний невозможно. Единственным результатом применения «звуковых» наркотиков являются головные боли, частичная потеря памяти и снижение мозговой активности.

Таким образом, информация о «цифровых наркотиках» - это хорошо спланированная «черная» пиар-компания, способная привлечь новых потенциальных покупателей звуковых файлов, и очередной способ получения денег мошенниками.

7. Найдено средство от Trojan.Encoder.20

Количество вирусов, которыми наводнено пространство всемирной паутины, на сегодняшний день не поддается исчислению.

Одной из вредоносных программ, разработанных и внедренных в Интернет киберпреступниками, стал *Trojan.Encoder.20*, который является усовершенствованной версией своего предшественника *Trojan.Encoder.19*.

Новоявленная программа-вымогатель распространяется через сайты со встроенным вредоносным кодом путем скрытой загрузки на компьютер посетителя сайта. Она шифрует все файлы пользователей, после чего самоликвидируется. При попытке открыть файл на экране появляется сообщение с требованием заплатить от 10 до 89 долларов с помощью sms за возможность расшифровки информации.

Пользователям, пострадавших от данного вируса, рекомендуется скачать разработанную компанией «Dr. Web» бесплатную утилиту, которая позволяет уничтожить данный вирус.

8. Внимание! Социальные сети - как один из способов вовлечения несовершеннолетних в оборот нелегального порно!!!!

Социальные сети активно используются злоумышленниками для вовлечения детей и подростков в распространение порнографических материалов с участием несовершеннолетних посредством сети Интернет.

Для этого создается вымышленная анкета (электронная страница), где используются фотосессии и вымышленные данные несовершеннолетних, взятые из различных открытых источников. Таким образом, порноделец маскируется под видом обыкновенного подростка, который в сети Интернет пытается рассказать о себе и найти новых знакомых с общими интересами.

В ходе электронного общения создаются условия, побуждающие подростка направить свои откровенные фотографии. После их получения данные изображения распространяются на тематических форумах, файлообменных системах и фото и видеопорталах.

Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «тро́ллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах, в вики-проектах провокационных сообщений с целью собственного развлечения и созданием конфликтов между участниками). Это необходимо для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий.

Общаясь в социальных сетях, помните:

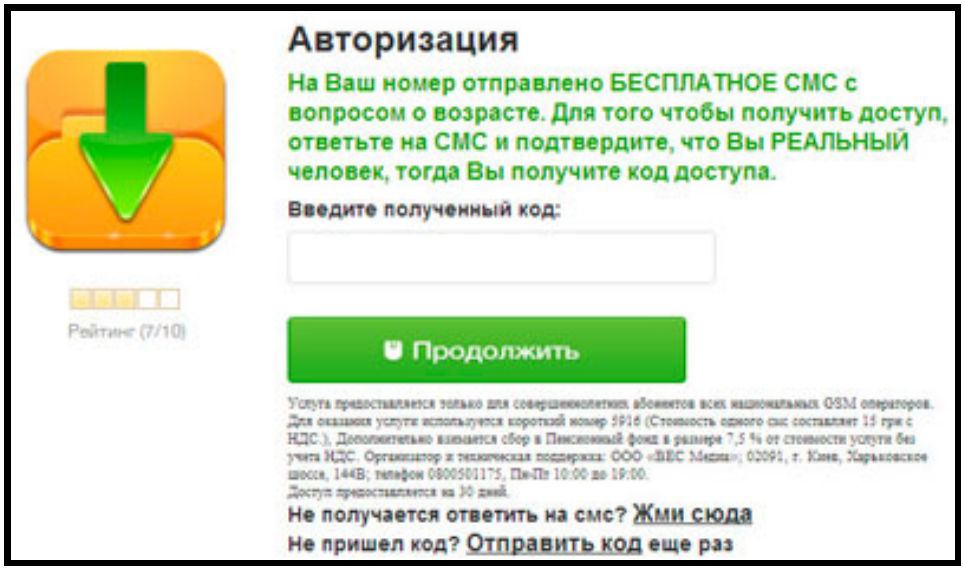
Любой человек, с которым вы познакомились в сети и вступили в переписку, может оказаться всего лишь вымышленным персонажем. Не увидев его воочию, вы никогда не сможете быть уверенными в его реальном существовании!

Информация, направляемая Вами посредством сети Интернет - будь это личные данные, фотографии либо видео - может быть использована против Вас, в том числе в корыстных и преступных целях.

Уважаемые родители! Проинструктируйте Ваших детей об элементарных правилах безопасности в Интернете!

Кейс 1 «Скачал?»

Александр долго искал программу для работы с 3-D проектировщиком. На одном из сайтов он увидел необходимую программу и большую зеленую кнопку «Скачать». Александр обрадовавшись, что сможет получить отличную программу бесплатно, нажал на кнопку, и получил следующее сообщение: «для того, чтобы снять ограничения на скачивание нужно ввести свой номер телефона и нажать «Продолжить»». Он последовал инструкции, далее появилась информация:



Александр отправил смс в ответ, но код доступа не пришел, отправил смс еще раз, но вновь кода не получил. Однако Александр обнаружил, что с его телефона списали деньги, причем немалые.

Проанализируйте ситуацию и ответьте на следующие вопросы:

1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку можно было избежать последствий необдуманных действий? *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Кейс 2 «Привет из Того»

Евгений получил на электронную почту сообщение, представленное ниже:

Привет Дорогой друг,
Хороший день для вас,
Это официальное уведомление Я U.Ofori Юрисконсульт (господина. R. Джеральд), который умер. В своей энерго и газовой месторождений компании, и я думаю с вашей помощью мы можем получить фонд вкладов моего покойного клиента. Он оставил сумму (США 25.5М) в Банке здесь в Ломе, Того.
Просьба написать мне Последующие для получения дополнительной информации, чтобы позволить мне познакомить вас с банком, в котором средства на хранение еще несколько деталей.

Я ожидаю ваш быстрый ответ.
Г-н Ofori

В ходе переписки Евгений сообщил свои персональные данные, в том числе и номер банковской карты. В течение ближайшей недели с этой банковской карты были списаны все денежные средства Евгения на неизвестный счет.

Проанализируйте ситуацию и ответьте на следующие вопросы:

1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку можно было избежать последствий необдуманных действий. *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Кейс 3 «Удачная покупка»

Михаил решил приобрести ноутбук Acer Aspira One A 110-Ab. После долгих раздумий, решил сделать это через интернет-магазин. В поисках наиболее выгодного предложения наткнулся на сайт «Скандинавский аукцион».

Условия были очень привлекательные:
при рыночной цене ноутбука в 36500 руб.

- Стартовая цена товара – 1 рубль.
- С каждой ставкой цена повышается всего лишь на 25 копеек.
- Каждая ставка увеличивает продолжительность аукциона на фиксированное время, указанное на странице конкретного аукциона.
- За возможность сделать ставку взимается символическая сумма, равная 6 рублям.
- Торги оканчиваются, если в течение определенного времени не будет подано ни одной заявки.
- Лот достается участнику, сделавшему последнюю ставку.

Михаил с увлечением включился в данные торги. На момент окончания торгов Михаил сделал 2636 ставок, что ему вылилось в 15816,00 руб. Однако, данный лот достался другому участнику, а Михаил потерял вложенную сумму денег.

Проанализируйте ситуацию и ответьте на следующие вопросы:

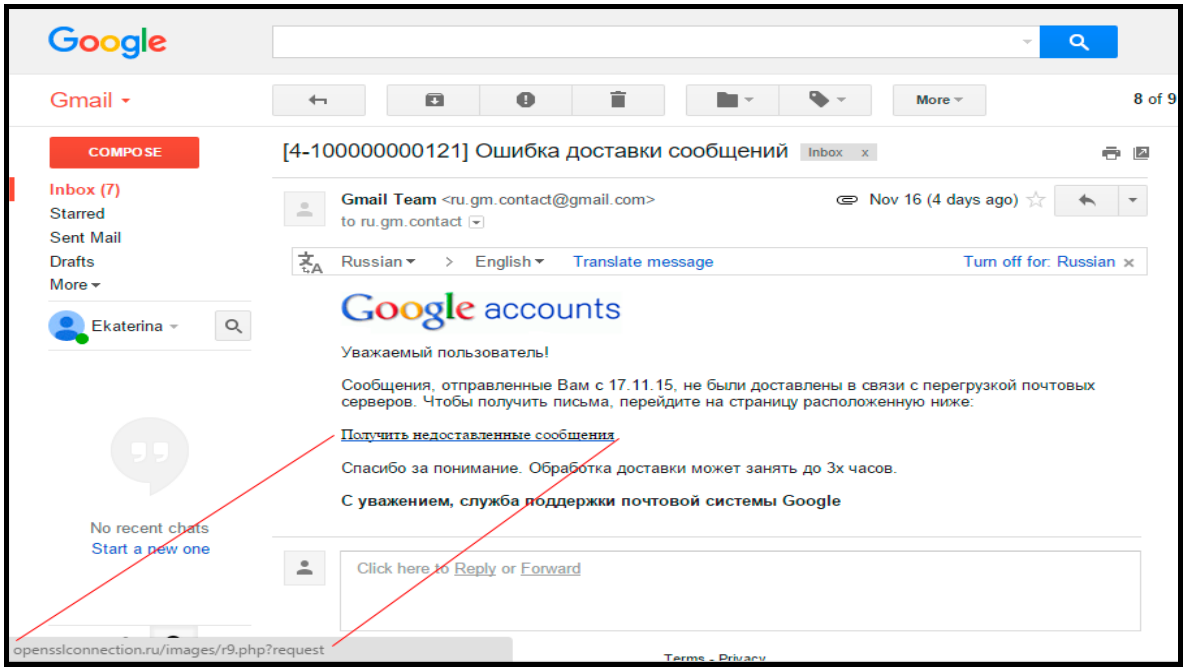
1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?

3. Как данному человеку можно было избежать последствий необдуманных действий. *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

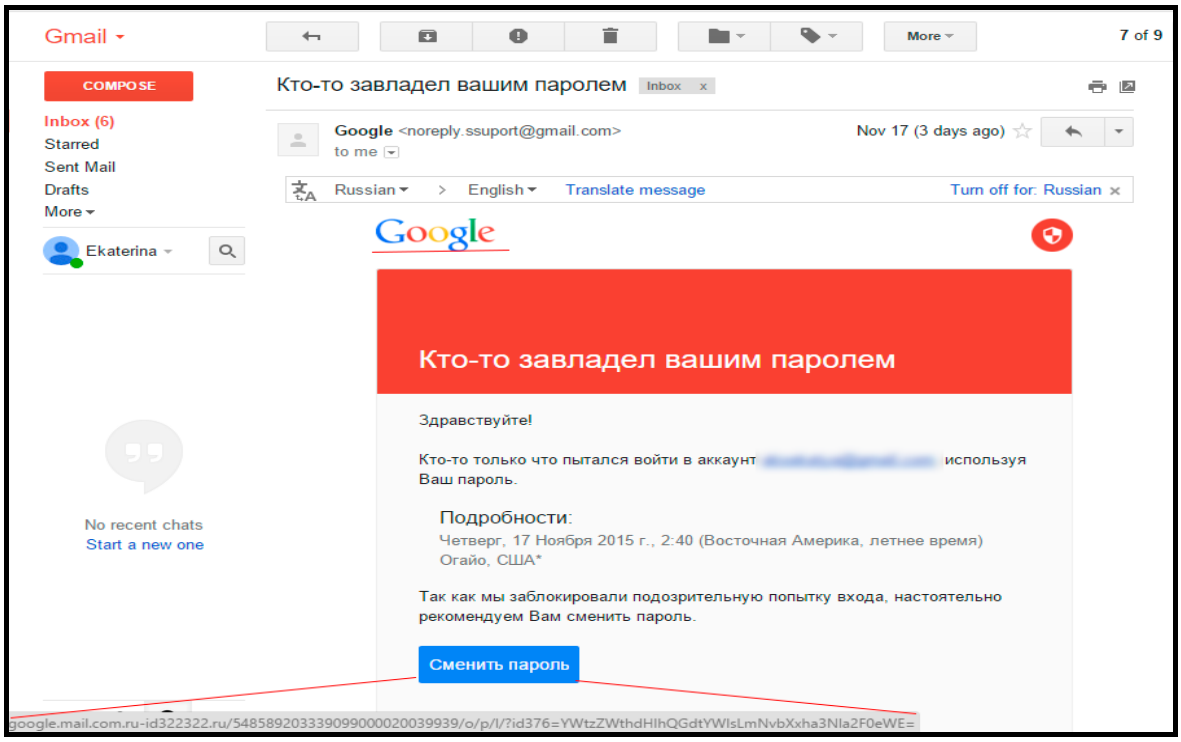
Приложение 7

Кейс 4 «Кто-то завладел Вашим паролем»

Екатерина получила на электронную почту сообщение, представленное ниже:



Так, как Екатерина ждала в этот период времени важное сообщение, то, не задумываясь, перешла по указанной ссылке. В течение суток ей на электронную почту пришло следующее сообщение:



Екатерина сменила пароль. После указанных действие Екатерина получила доступ к своей почте. Через неделю она обнаружила, что с её счетов, которые были доступны с данного компьютера, были списаны денежные средства.

<u>Проанализируйте ситуацию и ответьте на следующие вопросы:</u>

1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку можно было избежать последствий необдуманных действий. *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Кейс 5 Спасите мне жизнь!»

В «Одноклассниках» Светлана обратила внимание на информацию, которая появлялась в ее ленте не первый раз:

Светлана взяла телефон, набрала соответствующую команду и перечислила на счет 1000 рублей.

Проанализируйте ситуацию и ответьте на следующие вопросы:

1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку нужно было вести себя в данной ситуации? *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Кейс 6 «Заработать просто?»

Георгий долгое время искал способ дополнительного заработка в сети Интернет. В одной из рассылок его заинтересовала следующая информация:

Легкие деньги в интернете при помощи OlympTrade
Заработок
автор: admin

Приветствую Вас, дорогие посетители блога WebMasterDima. В данной статье я хочу вам рассказать про легкие деньги в интернете при помощи OlympTrade. Данная статья будет очень полезна к изучению именно тем, кто ищет легкие деньги в интернете.

Начни зарабатывать более 100$ в день легко и просто!
Рекомендуем Вам прямо сейчас начать зарабатывать более 18 долларов в час при помощи уникального способа! Скорее!!!
ПРИСТУПИТЬ К ЗАРАБОТКУ

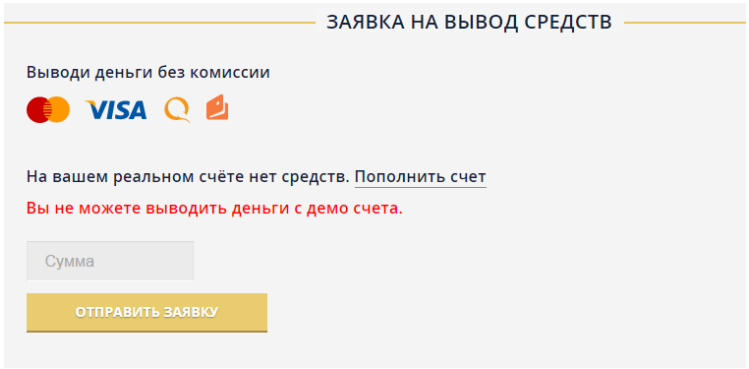
В действительности, многие сейчас могут подумать о том, что речь пойдет о валютном рынке форекс или чем то ином. Я не буду рассказывать о том, что такое бинарные опционы, я лишь расскажу о том, как любой желающий может попробовать начать зарабатывать деньги при помощи бинарных опционов, а именно с брокером Olymp Trade. Чтобы начать, вам совершенно не нужно вкладывать деньги, вы можете попробовать себя на демо счете!!! Итак, что вам необходимо сделать, а именно:

1. Регистрация в Olymp Trade

>>ЗАРЕГИСТРИРОВАТЬСЯ В OLYMPTRADE<

После регистрации вы сможете получить демонстрационный счет даже на 1000$, чтобы понять как и что нужно делать!!!

После регистрации вам предложат пройти обучение, где просто и понятно вы сможете понять всю суть работы. В действительности все довольно просто, вам нужно угадать движение графика, и в случае правильного решения уже через 1 минуту вы получаете до 80%. Работая даже с депозитом в 5000 рублей очень просто можно поднять сумму до 15 000 - 20 000 рублей в день! Внимание! Это не казино и не азартные игры, тут надо думать головой, я вам говорю просто как новичкам, что по началу вам необходимо научиться всему этому, а потом вы сможете зарабатывать стабильный и высокий доход.



Вы сможете ужасно просто и быстро вывести заработанные деньги на карту любого банка, на киви кошелек или яндекс деньги! Стоит заметить главную особенность данного сервиса в том, что после демо счета вы можете начать реальный заработок всего с 350

рублей, и никаких минимальных депозитов в 5000 рублей!!! Это заработок 21 века, и легкий заработок в интернете теперь доступен абсолютно каждому человеку!!!

Легкий заработок в интернете с OlympTrade. Действуйте!

Проанализируйте ситуацию и ответьте на следующие вопросы:

1. Как вы считаете, бал ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку нужно вести себя в этой ситуации? *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Кейс 7 «Заработал?!»

Степан Петрович в одной из рассылок получил заманчивое предложение, от которого не смог отказаться. Суть предложения:

Нужно вступить в группу, каждый новый участник которой делает входной взнос в размере 1010 рублей, который сразу же распределяется между тем, кто пригласил новичка и тем, кто привел в пирамиду пригласившего (по 500 рублей) и 10 рублей на отдельный счет организатора. Далее новичок приглашает еще трех человек. Теперь уже их взносы будут отданы в пользу более ранних участников. И так далее. Таким образом, получается, что вы отдаете 1010 руб. на «входе», а потом получаете 6000 рублей (1500 руб. в общую копилку отправляется от тех трех новых участников, которых пригласили Вы и еще 4500 от девятерых человек, которых пригласят эти новички).

Степан Петрович вступил в группу, отправил 1010 рублей (по указанным адресам по 500 рублей), а в качестве приглашенных участников вписал жену, сына и дочь, внес по 1010 рублей за них и получил на свой счет 1500 рублей. Далее нужно найти еще 9 участников.

*Он вписал своих родителей, внес 2*1010=2020 руб., на свои счета получил 2000 рублей, уговорил одного друга, получил еще 1000 рублей. Далее поступления остановились.*

Степан Петрович не стал рассказывать домашним о своей финансовой неудаче.

Проанализируйте ситуацию и ответьте на следующие вопросы:

1. Как вы считаете, был ли в данном случае факт финансового мошенничества?
2. Если да, то в чем суть данного мошенничества?
3. Как данному человеку можно было избежать последствий необдуманных действий? *(Ответ на данный вопрос зафиксируйте на предоставленном вам листе бумаги в виде конкретных рекомендаций).*

Видеоролик «Как не стать жертвой виртуального мошенничества» (https://www.newstube.ru/media/kak-ne-stat-zhertvoj-virtualnogo-moshennichestva)

Итоговый тест

Тест «Виртуальные ловушки»

1. Финансовое мошенничество – это:

a) Правонарушение, совершение которого влечёт применение к лицу мер уголовной ответственности.

b) преступление, заключающееся в завладении чужим имуществом (или приобретении прав на имущество) путем обмана или злоупотребления доверием.

c) Кража денег.

2. Соотнести понятие, описание и рисунок:

I. Фарминг

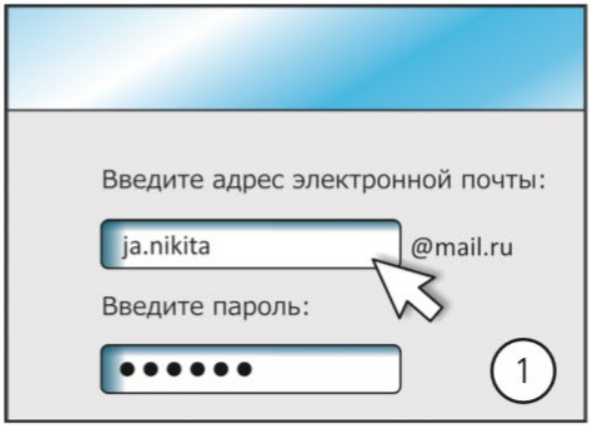
II. Семь кошельков

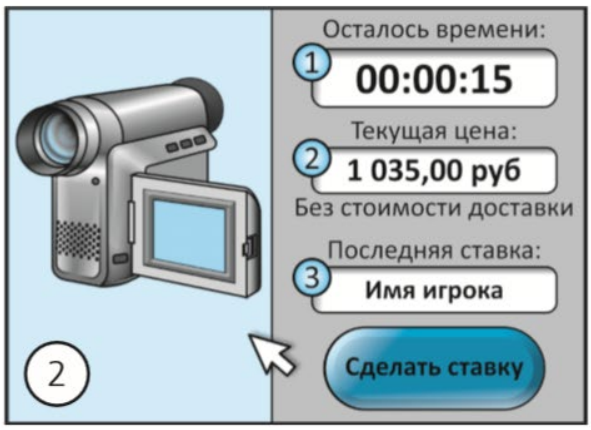
III. Скандинавский аукцион

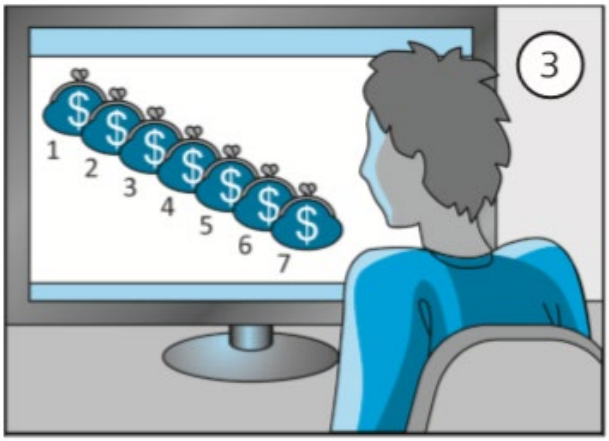
a) Продажа товаров на торгах по заниженной цене

b) Перевод пользователя на фальшивый сайт и кража конфиденциальной информации

c) Привлечение новых участников с целью заработка







3. Василий Петров, студент 3 курса, решил заработать в сети Интернет, создав финансовую пирамиду «Семь кошельков». Какими законами в РФ определяется наказание за подобное действие?

a) Уголовным кодексом РФ
b) Налоговым кодексом РФ
c) Гражданским кодексом РФ
d) Законом о защите прав потребителей
e) Конституцией РФ

Ответы на тест «Виртуальные ловушки»

1. B)
2. I – b – 1

   II – c – 3

   III – a - 2

Вопросы для рефлексии учащихся

Каждый учащийся высказывается одним предложением, выбирая начало фразы из списка на экране.

Сегодня я узнал…
Было интересно…
Было трудно…
Я выполнял задания…
Я понял, что…
Теперь я могу…
Я приобрел…
Я научился…
Я попробую…
Меня удивило…
Урок дал мне для жизни…
Мне захотелось…

Приложение 14.

Лист рефлексии для педагога.

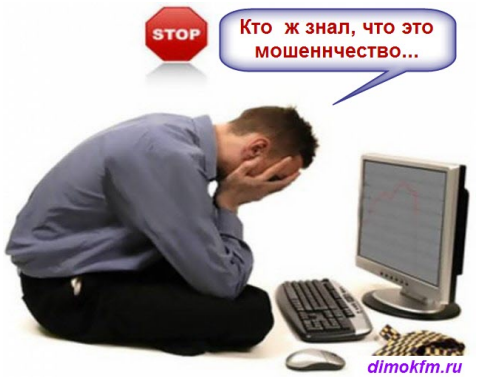
Критерии оценки	**Степень проявления**
Исчерпанность темы	Исчерпана полностью Исчерпана не полностью Не исчерпана
Степень реализации цели занятия	Цель реализована Цель реализована частично Цель не реализована
Соответствие содержания занятия намеченным целям	Достаточность объема материала Практическая значимость материала Соответствие возрастным возможностям
Подбор форм работы	Подобраны верно Подобраны неверно

Вариант буклета «Виртуальные ловушки»

Знать, где ловушка, - это первый шаг к тому, чтобы избежать ее.

Фрэнк Херберт

ПАМЯТКА
«Виртуальные ловушки»



Правила безопасного обращения с финансами и персональными данными в Интернете.

1. Регулярно обновляйте антивирусную программу на домашнем компьютере.
2. Не сообщайте реквизиты банковской карты неизвестным.
3. Будьте бдительны при вводе паролей и личных данных на сайтах, при переходе по незнакомым ссылкам.
4. Не вводите данные банковской карты с компьютеров общественного пользования.
5. Не открывайте подозрительные ссылки из писем и sms от незнакомых отправителей.
6. Помните, что ни один из платежных сервисов не требует оплаты комиссии от получателя перевода.
7. Ни в коем случае не верьте в возможность легкого заработка в сети Интернет и не поддавайтесь на уловки сайтов -„лохотронов”.
8. Получайте максимально полную и достоверную информацию о продавце или интернет-магазине перед покупкой товара и не приобретайте товары в социальных сетях

Ответственность за мошенничество в сети Интернет

В случае, если Вы были обмануты интернет-магазином, юридическое лицо обязано возместить Вам неосновательное обогащение (ст. 1102 Гражданского кодекса РФ), а также понесенные Вами убытки в полном объеме, в том числе компенсацию морального вреда (до трех тысяч рублей, в среднем) (ст. 15 Закона о защите прав потребителей). Также деятельность магазина может быть приостановлена Прокуратурой.

За мошенничество в сети Интернет, совершенное физическими лицами, предусмотрена реальная уголовная ответственность по статье 159 Уголовного кодекса Российской Федерации. Минимальное наказание за мошенничество составляет штраф до ста двадцати тысяч рублей, максимальное наказание, в зависимости от конкретного состава мошенничества, может доходить до лишения свободы на срок до шести лет (часть 3 статьи 159 УК РФ).

Помните, что лучше не становиться жертвой интернет-мошенника вовсе и быть бдительными, так как в случае, если Вы все же стали жертвой мошенника, защита своих прав и возврат денежных средств займет определенное количество времени (от одного до трех месяцев, в среднем).

Расскажите друзьям!

Виды виртуального мошенничества

Фишинг (англ. phishing) – вид интернет мошенничества, целью которого является сбор информации (персональных данных, паролей) пользователя. На электронную почту приходит письмо с уведомлением о том, что Вам необходимо срочно обновить (передать) свои персональные данные в какой-либо системе. Сообщения фишеров часто содержат угрозы, типа блокировки аккаунта, счета и т.д.

Фарминг (англ. pharming) – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации. «Нигерийские письма» (англ. «Nigerianscam») – электронное письмо с просьбой о помощи в переводе крупной денежной суммы.

Аукционы по типу "Скандинавского аукциона". На таком аукционе товар выставляется по очень низкой цене участники делают минимальные ставки и за каждую ставку с них снимается определенная сумма. Аукцион заканчивается в случае, если в течении определенного времени не будет подано ни одной заявки. После этого товар продается участнику, предложившему последнюю ставку.

«Финансовые пирамиды» - Вы будете получать доход от привлечения новых партнеров в данную организацию. И когда приход новых участников прекращается - финансовая пирамида закрывается и забирает все деньги, которые были инвестированы.

«Попрошайничество в интернете». На сайтах или социальных сетях размещаются объявления с просьбами помочь больному ребенку или сироте. В объявлении, как правило, указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, вы просто пополняете счет какому-то мошеннику.

«Легкий заработок». Заходя на любой сайт можно увидеть много предложений заработать хорошие деньги без всяких знаний и умений, достаточно только вложить 10 долларов, а через несколько недель получишь 1000. Обычно такие «вкладчики» уходят ни с чем.

SMS-мошенничество. Вас просят отправить смс на какой-либо номер, указывая, что это либо бесплатно, либо стоит немного. После того, как человек отправляет смс, со счета его мобильного телефона списывается сумма денег в десятки раз превышающая заявленную стоимость отправки смс.