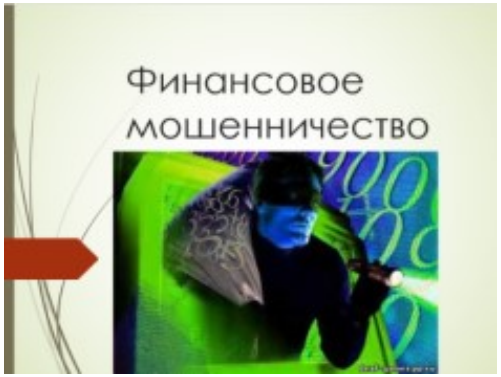


Тест «Виртуальные ловушки»

1. Финансовое мошенничество – это:

- Правонарушение, совершение которого влечёт применение к лицу мер уголовной ответственности.
- преступление, заключающееся в завладении чужим имуществом (или приобретении прав на имущество) путем обмана или злоупотребления доверием.
- Кража денег.

2. Соотнести понятие, описание и рисунок:

А) Фарминг

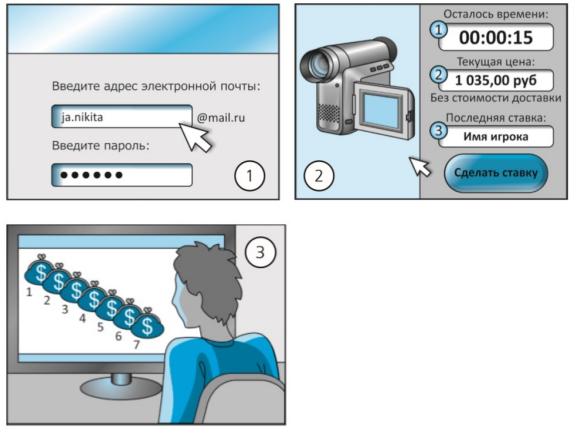
Б) Семь кошельков

В)Скандинавский аукцион

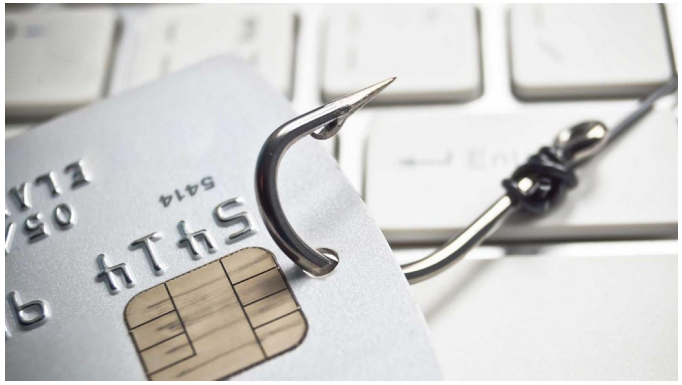
I) Продажа товаров на торгах по заниженной цене

II) Перевод пользователя на фальшивый сайт и кража конфиденциальной информации

III) Привлечение новых участников с целью заработка



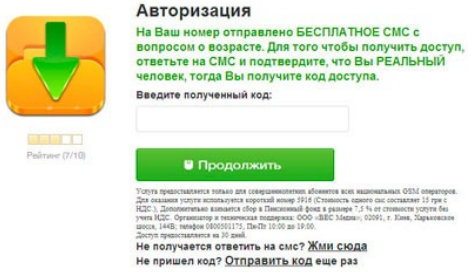
Финансовое мошенничество



Как не стать жертвой мошенников?

Ситуация 1

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 по-

следовал 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 выполните задания:

- Как вы считаете, был ли в данном случае факт финансового мошенничества?
- Если да, определите вид финансового мошенничества.
- Как данному человеку можно было избежать последствий необдуманных действий?

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.
Как разновидность используется рассылка о выгодном капиталовложении или устройстве на высокооплачиваемую работу, получении наследства или иных способах быстрого обогащения при условии совершения предварительных платежей.

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.

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.

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.

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

Фишинг (англ. phishing) – это технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как

Ситуация 2

Константин пришел в кафе, где была предложена бесплатная сеть Wi-Fi. За чашкой кофе ему пришла идея купить маме подарок в интернет –магазине. Для оплаты товара необходимо было ввести данные своей банковской карты. Когда Константин произвел данную операцию на сумму 1000 р., через несколько минут на его телефон пришло СМС, в котором сообщалось, что все средства (30000 р.) с карты были переведены на неизвестный счет.

Проанализируйте ситуацию и ответьте на следующие вопросы:

- Как вы считаете, был ли в данном случае факт финансового мошенничества?
- Если да, определите вид финансового мошенничества.
- Как данному человеку можно было избежать последствий необдуманных действий?