СЦЕНАРИЙ ПРАКТИКУМА «МАНИМАФИЯ»

ДЛЯ 7-8 КЛАССА

Сценарий разработан АО «ПАКК» по заказу Министерства финансов Российской Федерации в ходе реализации Проекта «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации».

Сценарий предназначен для свободного использования любыми заинтересованными лицами, занимающимися просвещением в области финансовой грамотности. При использовании сценария необходимо ссылаться на разработчиков.

Больше сценариев мероприятий по финансовой грамотности на сайте <http://edu.pacc.ru/>

Со всеми возникающими по использованию сценария вопросами, комментариями, отзывами, предложениями обращайтесь по адресу [edu@pacc.ru](mailto:edu@pacc.ru)

Москва 2020

1. Оглавление

1. ОПИСАНИЕ МЕРОПРИЯТИЯ 3

1.1. Цель и задачи мероприятия 3

1.2. Краткая характеристика мероприятия 3

1.3. План мероприятия 3

1.4. Технические требования к месту проведения, реквизиту и оборудованию 4

1.5. Правила игры 5

2. ХОД МЕРОПРИЯТИЯ 7

2.1. Подготовка мероприятия (30 минут) 7

2.2. Объяснение правил игры, представление команд (10 минут) 7

2.3. Основная часть игры – истории персонажей (65 минут) 8

2.4. Подведение итогов и рефлексия (10 минут) 8

3. ОПИСАНИЕ ПЕРСОНАЖЕЙ И ПРИМЕРЫ ОТВЕТОВ НА ВОПРОСЫ 12

3.1. Консультант вуза 12

3.2. Сотрудник службы безопасности банка 14

3.3. Специалист по набору персонала 16

4. ПОДСЧЕТ БАЛЛОВ 18

5. ПРИЛОЖЕНИЯ 19

# ОПИСАНИЕ МЕРОПРИЯТИЯ

## Цель и задачи мероприятия

**Цель мероприятия** – сформировать у участников установку на умение распознавать мошенников.

**Образовательные результаты:**

* Понимать, что такое мошенничество (в чем его опасность).
* Знать некоторые распространенные виды мошенничества.
* Знать приемы психологического воздействия (манипулирование, внушение, обман), используемые мошенниками.
* Уметь распознавать приемы психологического воздействия, используемые мошенниками.
* Знать признаки мошеннических действий или намерений (необычайно выгодное предложение, необходимость принять решение/совершить какие-то действия незамедлительно и т.п.)
* Уметь распознавать признаки мошеннических действий или намерений (необычайно выгодное предложение, необходимость принять решение/совершить какие-то действия незамедлительно и т.п.).
* Знать и уметь применять правильный порядок действий при столкновении с потенциальными мошенниками (не предпринимать поспешных действий: не оставлять информацию о себе, не передавать деньги, искать дополнительную информацию и т.д.).

## Краткая характеристика мероприятия

Таблица . Основные параметры мероприятия

|  |  |  |
| --- | --- | --- |
| № | Параметр мероприятия | Характеристика |
| 1 | Тема | Мошенничество |
| 2 | Формат | Практикум |
| 3 | Количество участников | 15-30 человек (5 команд по 3-6 человек) |
| 4 | Возраст участников | 7-8 класс (12-14 лет) |
| 5 | Количество ведущих | 1-2 модератора (может быть помощник ведущего) |
| 6 | Общая продолжительность | 45-90 минут |

«Манимафия» - это коммуникативная игра на тему мошенничества.

Участники делятся на команды. Перед ними выступает ведущий, который играет роль различных персонажей (продавца в магазине, сотрудника благотворительной организации и т.п.). Основная задача команд – задать персонажу такие вопросы, которые позволят выявить, является ли персонаж мошенником. После каждого персонажа участники заполняют карточки с итоговым решением группы: является ли персонаж мошенником, и по каким признакам команда сделала такой вывод. За правильные ответы участники получают баллы. Побеждает в игре команда, которая набрала как можно больше баллов.

## План мероприятия

Таблица 2. Тайминг мероприятия

|  |  |  |  |
| --- | --- | --- | --- |
| № | Блок игры | Этап мероприятия | Время |
| 1 | Приветствие и анонс мероприятия | Приветствие участников, презентация темы мероприятия, деление на команды. | 5 минут |
| 2 | Подготовка к проведению игры | Команды придумывают название команды, распределяют роли, знакомятся между собой. Ведущий объясняет правила игры. | 10 минут |
| 3 | Основная часть игры | Ведущий рассказывает историю от лица персонажа, участники задают вопросы, определяют мошенник персонаж или нет, заполняют карточки - описывают признаки мошенничества. | 65 минут |
| 4 | Подведение итогов | Ведущий игры подсчитывает результаты и проводит дискуссию, в ходе которой участники объясняют, как принимали решения.  Подводит итоги и делает вместе с участниками необходимые выводы. Отвечает на вопросы. | 10 минут |
| Итого | | | 90 минут |

## Технические требования к месту проведения, реквизиту и оборудованию

Для проведения игры необходима аудитория площадью не менее 30 кв.м. (может быть школьный класс) с незакрепленной мебелью, спортивный зал или уличное пространство.

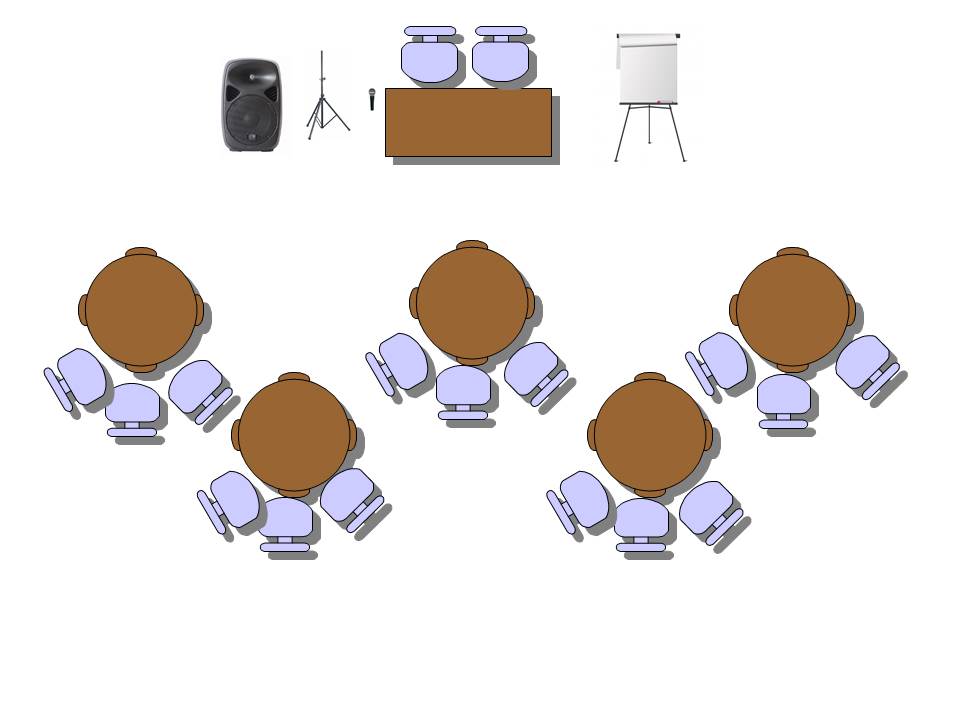
Минимальные требования к аудитории для проведения игры:

|  |  |
| --- | --- |
| Мебель | 1 стол и 2 стула для игротехников (поставить перед командными местами);  15-30 стульев и 5 столов (расставить для каждой команды). |
| Оборудование | Может быть музыкальное сопровождение – тогда необходим комплект оборудования и микрофон.  Удобно использовать доску или флипчарт для подсчета баллов. |

В аудитории (или на улице) нужно организовать пространство для игры – стулья и столы для каждой команды.

Основной ведущий должен располагаться таким образом, чтобы все участники могли поддерживать с ним визуальный контакт. Это отдельный стол и 2 стула. Если используется музыкальное оборудование, то оно тоже должно располагаться в зоне ведущих для удобства работы. Если в помещении есть доска или флипчарт, то он тоже должен находиться около ведущих.

Рисунок Примерная схема расстановки мебели и оборудования в аудитории

Никакого специального реквизита для игры не нужно. Для удобства работы каждой команды у них должны быть бумага и ручки.

Необходимо распечатать:

* Карточки для командного решения (Приложение 1) – 15 шт
* Карточка «Наушники Tony» (приложение 2) – 5 шт.

Все печатные материалы нужно **заранее разрезать и разложить** в отдельные стопки для раздачи участникам.

## Правила игры

Ведущий распределяет участников на 5 групп по 3-6 человек. Команды знакомятся между собой и распределяют роли в команде. Нужно выбрать: капитана и курьера. Капитан будет в течение игры задавать вопросы от команды ведущему, а курьер передавать карточки ведущему.

В течение игры команда может поменять капитана и курьера.

Далее ведущий объясняет правила.

Он от своего лица будет рассказывать историю персонажа (она может быть как мошеннической, так и нет). Участники внимательно слушают, подмечают детали, совещаются и формулируют вопросы, которые они хотят задать персонажу, чтобы точно определить - законны его действия или нет.

Капитаны команды с места задают по одному вопросу. Так проходит один круг (каждая команда задала по 1 вопросу), после этого еще раз совещаются и задают по второму вопросу (второй круг). Команды не должны повторять вопросы, а также должны внимательно слушать ответы ведущего на вопросы чужих команд.

После того как вопросы от команд заданы, каждая команда заполняет карточку, где отмечает мошенник персонаж или нет, и по каким признакам команда сделала такой вывод.

Если команды верно указали роль персонажа, то получают 10 баллов.

За каждый верный признак команда получает еще по 3 балла. Ведущий раскрывает персонажа, объясняет участникам, по каким признакам можно было догадаться о мошенничестве.

После этого ведущий рассказывают историю следующего персонажа.

В финале игры подводятся итоги - считаются баллы. Команда, набравшая наибольшее количество баллов – побеждает. Ведущий проводит рефлексию, рассказывает как грамотно вести себя с мошенниками. Игроки могут задать какие-то уточняющие вопросы, высказать свое мнение.

Игра рассчитана на 45-90 минут. За 45 минут ведущий может успеть обсудить истории 2 персонажей, за 90 минут 3-4 истории.

# ХОД МЕРОПРИЯТИЯ

## Подготовка мероприятия (30 минут)

Перед началом мероприятия необходимо проверить расстановку столов и стульев, подготовить оборудование. Проверить наличие всего необходимого (см. пункт 1.4 Технические требования к месту проведения, реквизиту и оборудованию).

## Объяснение правил игры, представление команд (10 минут)

Далее речь Ведущего (прямая речь) обозначена обычным шрифтом, варианты вопросов выделены в тексте **полужирным шрифтом**. Действия Ведущего и учащихся в ходе мероприятия *выделены курсивом.*

*Участники делятся на 5 команд и занимают предназначенные для них места.*

*Ведущий объясняет игровую задачу и правила игры, отвечает на вопросы участников.*

Здравствуйте, ребята! Сегодня мы с вами будем играть в игру «Манимафия». «Манимафия» - это игра, в которой вам предстоит вывести на чистую воду мошенников.

Мошенничество – это хищение чужого имущества путём обмана или злоупотребления доверием с корыстными целями.

Ситуации в жизни бывают разные – иногда мошенники маскируются под добропорядочных граждан, которые втираются к нам в доверие. А иногда наоборот обычные действия работников разных сфер могут казаться подозрительными.

В игре вам предстоит встретиться с разными персонажами, которые поведают вам свои истории. Вы должны внимательно их прослушать (зафиксировать основные детали) и решить, является ли персонаж, который предстал перед вами, мошенником или он честный гражданин.

Вы уже разделились на команды и в дальнейшем будете в них играть. Придумайте название команды и выберите капитана и курьера.

Задача капитана – подводить итог вашего группового обсуждения. Курьер будет относить ваши ответы.

Итак – даю вам пару минут на придумывание названия и выбор капитана и курьера*.*

*(Команды придумывают названия, знакомятся, выбирают капитана и курьера.*)

Теперь, когда вы придумали названия – давайте знакомиться*.*

*(Ведущий по очереди просит представиться команды и капитана*.)

Приятно познакомиться! Теперь о правилах.

Чтобы выяснить, является ли персонаж мошенником, вы в командах совещаетесь и решаете, какие уточняющие вопросы нужно задать персонажу, чтобы определить, как именно он совершал преступление.

Каждая команда задает вопросы по очереди. Одному персонажу вы сможете задать только 2 вопроса. Повторять вопросы нельзя, поэтому внимательно слушайте, какие вопросы задают другие команды, и как на них отвечает персонаж.

Если вы затрудняетесь задать вопрос, то я засекаю минуту. Если в течение этого времени вопрос у вас так и не появился, то он сгорает для вас. А команда, которая задает вопросы после вас, может задать не один, а два вопроса.

Параллельно вы получаете карточки, которые нужно заполнить. Во время игры вы можете делать для себя пометки, запоминать детали.

После того, как всего команды задали свои вопросы, вы заполняете карточки.

В карточках вы пишете финальный вердикт – мошенник персонаж или нет. Также вы должны указать, по каким признакам вы решили, что это мошенник. Если, по вашему мнению, герой не мошенник, то вы все равно должны указать, как вы поняли, что это так.

Курьеры каждой команды сдают карточки с вашим ответом. Если вы верно ответили мошенник персонаж или нет, вы получаете по 10 баллов. За каждый верный признак вы получаете еще по 3 балла.

Побеждает в игре команда, которая набрала больше всего баллов.

Итак, начинаем!

## Основная часть игры – истории персонажей (65 минут)

*Ведущий рассказывает историю от первого лица.*

*После этого участники совещаются и задают вопросы. Отвечать на вопросы нужно максимально правдоподобно, но при этом не раскрывать сущность персонажа. Вопросы по принципу «Вы мошенник?» - не принимаются.*

*Описание персонажей представлено в разделе 3.*

Таблица . Тайминг для работы с 1 персонажем:

|  |  |
| --- | --- |
| Действие | Время |
| Ведущий рассказывает историю от первого лица | 1 минута |
| Команды совещаются, придумывают вопросы | 3 минуты |
| Первый круг вопросов (5 команд – 5 вопросов) | 5 минут |
| Команды совещаются, придумывают вопросы | 2 минуты |
| Второй круг вопросов (5 команд – 5 вопросов) | 5 минут |
| Заполнение карточек | 5 минут |
| ИТОГО: | 21 минута |

## Подведение итогов и рефлексия (10 минут)

Друзья, мы завершаем нашу игру. И сейчас мы узнаем, какая команда оказалась самой внимательной и набрала наибольшее количество баллов.

*(Ведущий вместе с помощником подсчитывают баллы и оглашают их участникам)*

По количеству баллов у нас побеждает команда…. Молодцы ребята!

Второе место…. Отлично!

Третье место… Замечательно!

*(Ведущий подводит итоги и задает вопросы*)

* 1. **Что было самым интересным в игре? Что было понятно, а что – нет?**
  2. **Как победить в этой игре?**
* **В чем секрет взаимодействия с мошенниками?**
* **Как не попасть в лапы мошенников?**
* **О чем всегда нужно помнить при общении с мошенниками?**

Мошенничество считается уголовным преступлением и наказывается в соответствии с Уголовным кодексом РФ. Общие финансовые потери в мире, связанные с мошенничеством, измерить невозможно. Очевидно одно — они значительны.

Мошенничество может принимать много разных форм. Наиболее распространенные из них:

1. **Совершение сделки от чужого имени** (любые ситуации, когда произошла кража данных и мошенник пытается совершить сделку от вашего имени – от заключения кредитного договора до пользования вашей банковской картой);

2. **Обман** (намеренная попытка донести неверную информацию – сокрытие любой информации, дополнительных взносов, скрытых процентов; схемы «Нигерийское письмо», «7 кошельков», «Финансовые пирамиды»);

3. **Манипуляция** (давление на «больные места» ради достижения цели – фальшивая благотворительность, звонки и сообщения с просьбой собрать деньги на операцию маме, просто давление на собеседника и попытка заставить быстро принять решение).

Появляющиеся новые технологии призваны обезопасить потребителя, но часто мошенники оказываются впереди планеты всей и придумывают методы злого умысла сразу, как только новая технология входит в нашу жизнь.

И, пожалуй, самая опасная и часто встречающаяся цель мошенников – это кража личной информации в сети Интернет.

Как это может произойти:

**Сообщения в социальных сетях** с подозрительными ссылками (могут перенаправлять на фишинговые или иные подозрительные сайты)

* Просьба проголосовать за человека в каком-нибудь конкурсе. Вы нажимаете на ссылку, переходите на поддельный сайт, и там вас просят войти в свой аккаунт в социальной сети для голосования. Таким образом, происходит кража личной информации, и злоумышленники могут распоряжаться вашим аккаунтом (например, просить деньги от вашего лица у ваших подписчиков и прочее).
* Предложение скачать файл или предложение получить какой-то интересный файл (видеоролик, книгу, чек-лист и т.д.).

При открытии ссылки для скачивания могут попросить оставить номер мобильного телефона. Тем самым подключить абонента к платному контенту без его ведома. Схема действует так, что вы ставите где-нибудь «галочку», что согласны с условиями голосования (пользовательского соглашения или прочего) а условия, как правило, не читаете. Либо же вам приходит смс на телефон с кодом подтверждения, а на сайте написано, что для продолжения скачивания нужно ввести этот код (таким образом происходит подтверждение подключения услуги). В итоге у вас есть подписка на прогноз погоды, музыкальную композицию вместо гудка или рассылку материалов. Вы в замешательстве, так как не понимаете, как это подключили и на каком ресурсе. Помочь отключить услугу вам смогут в салонах связи (если говорим про мобильные устройства) или представители вашего сотового оператора по телефону.

**Сообщение в социальных сетях** и мессенджерах, которые содержат в себе различный обман и манипуляции.

Это могут быть просьбы дать в долг на пару дней, просьба помочь средствами в сложной жизненной ситуации (проблемы со здоровьем, ДТП, пожар, грабеж и т.д.).

**Сообщения в социальных сетях**, которые содержат информацию о фиктивных благотворительных сборах (больные дети, старики, животные, различные несуществующие фонды).

**Вирусные атаки**

Как правило, это возникает, если ваш компьютер или телефон подвергся атаке вредоносного программного обеспечения.

Например, вы могли зайти на какой-то подозрительный сайт или нажать на подозрительную ссылку, что запустит действие вируса на вашем устройстве. Обычно подобные мошеннические схемы работают так, что у вас появляется «окно» на весь экран с какой-то неприятной или неприличной информацией. Окно не закрывается, не дает возможность пользоваться компьютером, и в целом, смущает пользователя. Как правило, в этом окне есть сообщение - «заплатите нам какую-то сумму денег», «отправьте смс на номер» и прочее. Смущенный пользователь отправляет сообщения или свои средства, и окно пропадает. Справиться с этой неприятной ситуацией можно иными способами – не пользоваться подозрительными сайтами, иметь антивирусную активную систему на устройствах.

**Розыгрыши и аукционы**

* Сообщения на различных сайтах, похожие на «Получи классный телефон всего за 500 рублей. Участвуй в нашем конкурсе». Работает это так – вы оплачиваете свой конкурсный билет и ждете розыгрыша, которого не существует.
* Другой вариант, когда формат аукциона требует каждый «шаг» вносить небольшую сумму денег, но в итоге, за время аукциона вы вкладываете больше средств, чем стоит приз. И, как правило, не выигрываете его.
* «Розыгрыш» завершился, вы стали «победителем» - именно такая информация вам может прийти на почту или в мессенджер. Что бы получить несуществующий приз нужно дать данные, куда его нужно отправить или заплатить за пересылку приза. Это могут быть и ФИО, и домашний адрес, и паспортные данные, и номер телефона. Приза никакого нет, и мошенники просто выманили у вас личную информацию, либо деньги на доставку.

**Анкеты, приложения, регистрации**

Еще один формат мошенничества в сети интернет, это подробное заполнение анкет и полей регистрации на подозрительных сайтах.

Какую-то информацию про регистрации оставлять не опасно – например, адрес электронный почты. Но бывают случаи, когда вам обещают какое-то вознаграждение, если вы подробно заполните анкету на сайте. Например, дополнительные бонусы или игровые деньги. Или же вам обещают большие деньги за заполнение анкеты, но в финале просят оплатить небольшую сумму за пересылку приза/оформление денежного приза и т.п.

Также подробную информацию у вас могут попросить различные приложения, которые вы можете устанавливать на свои устройства. Например, популярно такое приложение, которое показывает, как ваш номер телефона записан у других пользователей. Это очень любопытно. Но есть один неприятный момент, когда вы нажимаете галочку, что согласны с пользовательским соглашением, вы передаете право обрабатывать вашу базу контактов приложению. И как ей распорядятся разработчики вам доподлинно неизвестно.

**Давайте разберемся, как мошенники выбирают своих жертв?**

Большая часть действий мошенников рассчитана на то, что жертва не готова оказать сопротивление: не знает своих прав и не понимает своих интересов. Поэтому риски мошенничества можно существенно снизить, если **знать порядок действий** в таких ситуациях.

Основные характеристики мошенников:

* ищут «легких жертв» (им невыгодно связываться с теми, кто проявляет признаки бдительности);
* осуществляют массовую проверку на примитивные ошибки;

Например, хакеры гораздо чаще не «ломают» конкретный почтовый ящик, пробуя на нем разные пароли, а перебирают миллионы разных, «случайно» «взламывая» те, где стоит пароль типа «123» или «qwerty».

Мошенники не готовы к неожиданной реакции/вопросам (предпочитают в таких случаях бросить жертву и начать искать новую). Они боятся затягивания взаимодействия (это не только трата времени, но и резкое возрастание риска поимки).

**Знание и соблюдение простых правил безопасности** и стандартных приемов мошенников резко снижает этот тип рисков без больших затрат времени/денег.

Можно выделить несколько самых важных защитных приемов против мошенников:

* спрашивать **документы** (паспорт, подтверждение места работы, договор, гарантийный талон, лицензию и т.д.);
* **перепроверять информацию** (звонить в банк, найти в интернете сайт компании и т.д.) – ОСОБЕННО в тех случаях, когда контрагент утверждает, что действует от имени финансовой организации;
* вместо немедленного заключения сделки **брать время «на подумать»** и контакты для обращения в ближайшем будущем;
* в случае давления **никогда не оправдываться**, вместо этого самому задавая вопросы.

Спасибо большое за игру, надеюсь, вы сделали для себя важные выводы. И самое главное получили полезный навык, который формирует ваше ответственное финансовое поведение*.*

# ОПИСАНИЕ ПЕРСОНАЖЕЙ И ПРИМЕРЫ ОТВЕТОВ НА ВОПРОСЫ

*В игре несколько персонажей, от лица которых ведущий ведет диалог с участниками:*

* *Консультант вуза (платное тестирование) – не мошенник;*
* *Сотрудник службы безопасности банка (мошенническая операция по карте) – мошенник;*
* *Специалист по набору персонала (нигерийское письмо) – мошенник;*

*Задача ведущего рассказать о ситуации, которая происходит с персонажем.*

*Если персонаж - мошенник, то ведущий может намеренно грубо себя вести, постоянно задавать вопросы участникам, давя на них в принятии решения. Также ведущий может уклончиво отвечать даже на те вопросы, которые описаны в сценарии. На вопросы, которые в сценарии не описаны, ведущий должен отвечать в соответствии с легендой или просто уклончиво.*

*Если участники теряются и не могут сформулировать вопрос, то ведущий может подсказывать участникам, мошенник он или нет своим поведением. Также, если после первого круга вопросов участники не задали вопросы, позволяющие явно определить, кем является персонаж, то ведущий может постараться натолкнуть своими репликами участников на нужные вопросы.*

## Консультант вуза

Вы планируете поступление в высшее учебное заведение. Сложно определиться, куда пойти учиться. Вы посещаете мероприятия вузов (дни открытых дверей), постоянно просматриваете различные сайты. Как-то раз вы оказались на выставке образования. В большом холле представлены стенды разных вузов и колледжей. К вам подходит молодой человек-промоутер и говорит:

- Добрый день. Я представитесь Высшей школы гуманитарных наук. Вы рассматриваете поступление в вузы гуманитарной направленности? Если – да, то предлагаю вам пройти профориентационное тестирование, чтобы узнать к каким профессиям вы наиболее склонны. Бонусом нашего тестирования является короткий тест на уровень общих знаний, который показывает предположительные баллы по ЕГЭ, которые вы можете получить. А значит узнать, есть ли у вас шанс поступить в наш вуз на бюджетные места или нет.

Стоимость тестирования и индивидуальной консультации – 1000 рублей. Тестирование поможет вам оценить, какие сферы профессиональной деятельности вам стоит рассматривать. Интересно? Подходите к нашему стенду.

Какие вопросы вы зададите промоутеру?

*Вопросы, которые могут задать участники:*

* *Почему тестирование платное?*

Любое профориентационное тестирование – это платная услуга. Его проводят профессиональные психологи и педагоги. У нас оно качественное и интересное. Попробуйте.

* *Зачем мне проходить ваше тестирование?*

Тестирование построено по психологическим принципам и поможет вам определиться с выбором профессии, даже если в итоге, вы не планируете поступление именно в наш вуз.

* *Вы государственный вуз?*

Наш университет негосударственный, но имеет образовательную лицензию, государственную аккредитацию и прекрасных выпускников. Также у нас есть часть мест, которые финансируются из бюджетов наших спонсоров. Вы можете учиться на бюджете именно за счет этих средств. Вы можете зайти на наш сайт, где представлены учебные планы, фотографии с мероприятий и отзывы наших выпускников. Подходите к нашему стенду и познакомьтесь с преподавателями и представителями разных факультетов, они могут ответить на вопросы.

* *Что входит в ваше тестирование?*

Тест по профориентации – это такой многоуровневый тест, где мы с вами вместе выясним, к каким профессиям вы имеете склонность, какие профессиональные сферы будут для вас наиболее успешными, что из предметов вам дается легко, какие из них вам действительно интересны.

Далее вы будете общаться с психологом, который интерпретирует ваши результаты.

Затем вы сможете пообщаться с представителями разных факультетов и задать им свои вопросы. По итогу тестирования и консультации у вас на руках останутся результаты, которыми вы сможете пользоваться при выборе вуза и специальности.

Также в наше тестирование входит короткий тест на общую эрудицию и базовые школьные знания. Тестирование покажет, какие у вас шансы на поступление в наш вуз на бюджет*.*

* *Как мне оплатить тестирование?*

На нашем стенде есть электронная касса. Вы можете оплатить банковской картой или наличными. Мы выдаем чеки и небольшой договор об оказании услуги*.*

* *Кто будет проводить тестирование?*

Сначала наш консультант, затем вы общаетесь с психологом – ее зовут Ферапонтова Мария Алексеевна, она кандидат психологических наук и преподаватель нашего вуза. Она уже больше 20 лет проводит тест по профориентации. Вам очень повезет, если вы поучаствуете в тестировании именно с Марией Алексеевной. Кстати, можете почитать о ней на нашем официальном сайте. В разделе «Факультет психологии».

* *А вы кто? Вы работаете в вузе?*

Да, я работаю в вузе в приемной комиссии.

**Пояснение к ситуации**

**Персонаж – не мошенник.**

**Признаки, которые участники могут выделить, свидетельствующие, что промоутер не мошенник:**

* Промоутер предлагает классическую платную услугу.
* Услугу можно оплатить с помощью кассы и получить чек и договор.
* По результатам тестирования потребитель получает документы о результатах тестирования.
* У вуза есть сайт, стенд на выставке.
* Тестирование проводит дипломированный специалист.

Промоутеры на различных выставках могут казаться навязчивыми и даже немного агрессивными. Но их задача привлечь вас к какой-то активности. Иногда даже убедить приобрести услугу или товар. Вам может показаться, что промоутер вуза обещает вам больше, чем может обеспечить, но в данном случае это не так – он четко описывает, в чем состоит смысл услуги, как вы можете ее получить, и сколько она стоит.

Ваша задача, если вы попадете в подобную ситуацию понять, нужна вам услуга или нет (может стоить приобрести ее в другом месте и по другой цене). Необходимо задать все интересующие вопросы, чтобы получить информацию для принятия решения.

Реклама на сегодняшний день бывает разная. Маркетологи прибегают к работе лидеров мнений – блогеров, знаменитостей и селебрити. Не стоит доверять каждому из этих людей, любую рекламу стоит проверить – почитать отзывы на товар или услугу, провести свой анализ (посмотреть сайт, описание товара или услуги).

## Сотрудник службы безопасности банка

Вам поступает звонок на мобильный телефон:

Добрый день! Меня зовут Ангелина, я сотрудник службы безопасности вашего банка. С вашей карты совершен подозрительный платеж. Переведено 6000 рублей некому Афанасию Сергеевичу Н., Вы знаете такого человека? Нет, тогда, скорее всего это мошенники. Проверьте, ваша карта при себе? Может быть, вы заходили в личный кабинет? Я вижу в базе, что последний раз вы заходили с телефона Android. Нам стоит заблокировать вашу карту и подключить дополнительные средства безопасности, например, двойную аутентификацию. Пожалуйста, назовите вашу фамилию, имя и отчество, номер карты и кодовое слово и мы продолжим блокировку вашей карты…

Стоит ли раскрывать вашу личную информацию? Какие вопросы стоит задать?

* *Представитель какого вы банка?*

Вашего, где вы обсуживаетесь.

* *Как вы можете подтвердить, что вы сотрудник службы безопасности банка?*

Я звоню с официального номера вашего банка. Вам нужно срочно заблокировать карту. Объясняю ситуацию. Какие вам нужны подтверждения?

* *Я могу позвонить в вашу службу безопасности самостоятельно?*

Можете, но зачем? Я и так вам уже звоню. Давайте не терять время – мне нужны ваши данные для подтверждения.

* *Такие звонки от вашего банка обычное дело?*

Да, если по карте проводятся подозрительные операции, то система это автоматически выявляет. Служба безопасности банка обычно перезванивает клиенту, чтобы убедиться, что действия санкционированы*.*

* *Откуда у вас информация о переводе?*

У нас есть электронная база, и мы видим все подозрительные переводы. Давайте уже перейдем к защите вашей карты, назовите вашу фамилию, имя и отчество….

* *Мне не проходило смс-сообщение о переводе средств, как вы можете это объяснить?*

Тогда этот перевод точно мошеннический! Вам срочно нужно заблокировать карту и подключить двойную аутентификацию! Сейчас мы отправим вам смс-сообщение, назовите цифры из этого сообщения мне…

* *Сколько средств осталось на моем лицевом счете? Какие последние операции вы видите?*

Я не могу вам этого сказать без подтверждения личности, назовите свои ФИО и кодовое слово*.*

* *Что такое двойная аутентификация?*

Это такая дополнительная функция для вашей карты, чтобы воспользоваться картой для оплаты товаров и услуг в интернете, вам нужно будет ввести код, который придет в смс-сообщении. СМС сейчас вам отправили, назовите мне код для подтверждения подключения услуги.

* *Что будет, если я не заблокирую карту?*

Скорее всего, злоумышленники снимут все оставшиеся средства.

**Пояснение к ситуации**

**Сотрудник службы безопасности банка – мошенник.**

**Признаки, что персонаж мошенник:**

* Спрашивает информацию, которую сотрудники банка и так должны знать (номер карты, ФИО).
* Не дает точную информацию, что за организацию он представляет («ваш банк» - какой мой банк?).
* Отговаривает от звонка в службу безопасности (зачем вам звонить, я же вам уже звоню).
* Давит на клиента, уговаривает совершить необдуманные действия.

Если вам звонят по телефону и стараются выяснить любую лучную информацию стоит задуматься. Представители банка никогда не звонят с номера мобильного телефона (обычно это городской). Сотрудник банка не будет у вас спрашивать личную информацию при входящем вызове.

Если вы звоните в банк, то у вас действительно могут спрашивать ФИО, кодовое слово, паспортные данные и номер карты, так банк определяет, что вы действительно его клиент. Но на сегодняшний момент, если вы звоните с мобильного телефона, то сотрудники банка автоматически определяют вас как клиента банка, также, как правило, спрашивают только последние цифры номера карты.

Представители банка могут позвонить, если совершается операция на большую сумму, чтобы подтвердить перевод.

Обычно, когда звонят мошенники, они стараются быстро узнать ваши данные, застать вас в состоянии растерянности. А если вы не отвечаете на вопросы, то заканчивают разговор. Так происходит по нескольким причинам.

* Во-первых, если разговор длинный, то есть возможность отследить звонок.
* Во-вторых, если вы сразу не соглашаетесь, то, скорее всего, и дальше не согласитесь, а только будете задавать все больше и больше вопросов.
* В-третьих, мошенникам проще позвонить нескольким людям, и попасть на легко убеждаемого человека, чем долго разговаривать с вами.

Что не следует делать: сообщать мошенникам данные своей карты, любую личную информацию, CVC и CVV-коды, пин-коды, коды из смс-сообщений.

Что следует делать: прекратить разговор, сказать, что Вы лично перезвоните в службу безопасности банка.

**Базовые меры безопасности:**

* Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже - заблокируйте карту.
* Сохраняйте все документы до окончания проверки правильности списанных сумм.
* Сообщайте банку актуальные контактные данные.
* Подключите услугу SMS - уведомлений, всегда имейте при себе телефон службы поддержки.
* В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

## Специалист по набору персонала

Вы хотите найти работу на лето. Неожиданно вам приходит сообщение в социальной сети от неизвестного вам пользователя:

«Здравствуйте! Меня зовут Арсений. Я работаю в кадровом агентстве «Найдем работу». Мы подумали, что вы наверняка хотели бы поработать летом. Хотим предложить удаленную работу в социальных сетях. Зарплата сдельная от 1.000 до 20.000 рублей в неделю. Но для начала вам нужно заполнить анкету и пройти обучение. Обучение длится 5 часов и стоит 500 рублей. Там мы подтверждаем серьезность ваших намерений работать. Регистрируйтесь по ссылке».

Какие вопросы вы зададите Арсению?

* *Что это за агентство «Найдем работу»?*

Мы работаем как индивидуальные менеджеры по набору персонала: у нас обращаются различные организации, которые ищут сотрудников, а мы уже осуществляем поиск вакансий в социальных сетях – пишем тем, кто интересуется поиском работы. Личные контакты гораздо эффективнее, да и вы можете сразу задать все вопросы о работе. Это удобно.

* *У вашего агентства есть сайт, контакты, реквизиты?*

У нас нет официального сайта, мы работаем как индивидуальные менеджеры. Вы можете писать мне в сообщения, это моя личная страница. Я почти всегда онлайн. Также вы можете подписаться на новости нашей группы, там появляются вакансии.

* *Что за работа? Что необходимо делать?*

Вам необходим будет просматривать определенные страницы в социальных сетях, и отслеживать реакции на эти страницы и посты: лайки и репосты. Но это я очень общими словами говорю, подробности во время обучения. Кстати, там осталось совсем мало мест, скорее регистрируйтесь быстрее!

* *Как я могу оплатить 500 рублей?*

С помощью электронного кошелька. Я вышлю вам ссылку. Зарегистрирован на Иванова Ивана.

* *Я получу какие-то документы об обучении?*

Да, вы получите чек-лист[[1]](#footnote-1) «Найдем работу» и гайд «Как правильно работать».

* *Мне нужно заполнить анкету, а что за вопросы?*

*Ваша контактная информация, чтобы мы легко могли заключить с вами договор – ФИО, паспортные данные, номер карты, на которую мы будем вам переводить вознаграждение и т.д. Вот ссылка – заполняйте скорее, а то места на обучении закончатся.*

* *Как понять, сколько я смогу зарабатывать?*

Об этом мы расскажем на обучении. Если будете усердно работать, то сможете зарабатывать до 20.000 рублей в неделю, и это при свободном графике, просто просматривая посты в социальных сетях! У нас есть сотрудники, которые на этой неделе заработали 18500 и 19900. Простые ребята, школьники, как и вы.

* *Что мне понадобится для работы?*

Время, усердие и компьютер или смартфон с постоянным выходом в Интернет. И естественно, знания, полученные на обучении. Всего 500 рублей, а так много полезных знаний за 5 часов. Это лучшее, на что вы можете потратить свои деньги.

**Пояснение к ситуации**

**Специалист по набору персонала – мошенник.**

**Признаки мошенничества:**

* Организация без юридического статуса (нет сайта, официальной информации);
* Связь с «менеджером» только в социальной сети;
* Оплата обучения через электронную платформу на частное лицо;
* Отсутствие документов об обучении (сертификатов, удостоверений);
* Просьба оставить личные данные в анкете по ссылке (неизвестно вредоносная ссылка или нет, но в любом случае личные данные не стоит оставлять в неизвестных анкетах в сети).
* Обещание прибыли за «легкую работу» при небольшом вложении.

Достаточно часто встречающийся вид мошенничества – это «Нигерийское письмо». Оно представляется в разных формах – обычно, это обещание баснословного богатства, за скромные расходы по оформлению документов. Обычно, речь идет о наследстве. Якобы у вас скончался богатый дальний родственник, и он передал все наследство вам. Для того, что бы его получить необходимо оплатить услуги юриста (или еще кого-то). Раньше такие письма могли приходить не только на электронный адрес или в личные сообщения в социальной сети, но и обычным бумажным письмом. В этом письме даже могли быть фирменные бланки и печати реальных организаций.

Сегодняшняя технология в основном построена на взаимодействии мошенника и жертвы в социальных сетях. Предложение хорошо зарабатывать для школьника пройдя какое-то небольшое платное обучение – это тоже форма, похожая своим содержанием на «Нигерийское письмо».

Обычно рекомендуется закрыть это письмо, отметить как «Спам» и удалить.

В данном случае, помимо небольшого вознаграждения мошенник параллельно пытается еще и получить личные данные. Это выглядит даже «неподозрительно» – когда вы приступаете к работе, обычно вы действительно заполняете трудовой договор (или договор подряда), где указываете свои персональные данные. Но это делается в отделе кадров, и вы реально там присутствуете. А здесь у вас просят оставить свои данные просто в анкете по ссылке. Это опасно. Так делать не стоит.

Всегда обращайте внимание, какие именно данные у вас запрашиваются. Например, если у вас просят адрес электронной почты и имя – то это, скорее всего, неопасно. Скорее всего, вам просто хотят отправлять письма – информационную рассылку.

В любом случае, прежде, чем оставлять свои контактные данные – читайте пользовательское соглашение, все входящие сообщения по этому вопросу, задавайте вопросы, если вам что-то непонятно.

# ПОДСЧЕТ БАЛЛОВ

Примеры признаков мошенничества и не мошенничества, за которые участники могут получить баллы:

|  |  |  |
| --- | --- | --- |
| **Персонаж** | **Признак мошенничества и не мошенничества** | **Баллы** |
| **Промоутер ВУЗа – не мошенник** | Промоутер предлагает классическую платную услугу. | 3 балла |
|  | Услугу можно оплатить с помощью кассы и получить чек и договор. | 3 балла |
|  | По результатам тестирования потребитель получает документы о результатах тестирования. | 3 балла |
|  | У вуза есть сайт, стенд на выставке. | 3 балла |
|  | Тестирование проводит дипломированный специалист. | 3 балла |
| **Сотрудник службы безопасности банка - мошенник** | Спрашивает информацию, которую сотрудники банка и так должны знать (номер карты, ФИО). | 3 балла |
|  | Не дает точную информацию, что за организацию он представляет («ваш банк» - какой мой банк?). | 3 балла |
|  | Отговаривает от звонка в службу безопасности (зачем вам звонить, я же вам уже звоню). | 3 балла |
|  | Давит на клиента, уговаривает совершить необдуманные действия. | 3 балла |
| **Специалист по набору персонала - мошенник** | Организация без юридического статуса (нет сайта, официальной информации); | 3 балла |
|  | Связь с «менеджером» только в социальной сети; | 3 балла |
|  | Оплата обучения через электронную платформу на частное лицо; | 3 балла |
|  | Отсутствие документов об обучении (сертификатов, удостоверений); | 3 балла |
|  | Просьба оставить личные данные в анкете по ссылке (неизвестно вредоносная ссылка или нет, но в любом случае личные данные не стоит оставлять в неизвестных анкетах в сети). | 3 балла |
|  | Обещание прибыли за «легкую работу» при небольшом вложении. | 3 балла |

# ПРИЛОЖЕНИЯ

1. Карточка для командного решения (Приложение 1)

1. **Чек-лист** – это список, состоящий из нескольких пунктов. **Гайд** – руководство, в котором указана последовательность действий. В последнее время в социальных сетях все большее распространение особенно среди подростков получили продажи таких «чек-листов» и «гайдов» от известных личностей и блогеров. Стоят они, как правило, недорого, поэтому школьники могут себе это позволить. Зачастую в них находится информация, которую легко найти в интернете в свободном доступе, но выдается она за уникальные и эксклюзивные авторские наработки. [↑](#footnote-ref-1)