

СБОРНИК МЕТОДИЧЕСКИХ МАТЕРИАЛОВ

для проведения занятий по финансовой грамотности
в организациях для детей-сирот и детей, оставшихся
без попечения родителей

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Как себя защитить



Настоящий сборник методических материалов по теме «Финансовое мошенничество» подготовлен для проведения занятий по финансовой грамотности в организациях для детей-сирот и детей, оставшихся без попечения родителей.

Сборник методических материалов может быть использован во внеурочной деятельности при проведении занятий с детьми 11–15 и 16–18 лет. Материалы сборника направлены на формирование представлений о финансовых махинациях, о том, почему люди становятся жертвами финансовых мошенников, способах защиты своих интересов на финансовом рынке. Воспитанники организаций для детей-сирот и детей, оставшихся без попечения родителей, узнают о том, что нужно делать в случае сомнительных, тревожных телефонных звонков, писем на электронную почту и СМС; как защитить в интернете свои персональные данные, реквизиты платежных карт. Дети научатся безопасно снимать деньги в банкомате и расплачиваться картой, смогут распознать популярную мошенническую схему, когда злоумышленник представляется сотрудником государственной организации.

Подготовленные сценарии занятий полностью раскрывают обозначенные темы, адаптированы для целевой аудитории, изложены в доступной игровой форме. В качестве контрольно-измерительных материалов разработаны тестовые вопросы, которые могут быть использованы по окончании изучения соответствующей темы по финансовой грамотности воспитанниками организаций для детей сирот.

Сборник методических материалов предназначен для работников организаций для детей-сирот и детей, оставшихся без попечения родителей, наставников детей-сирот, волонтеров.

Содержание

Занятия для детей 11–15 лет	2
Финансовое мошенничество	2
Кибермошенничество	8
Занятие для детей 16–18 лет	22
Мошенники, которые маскируются под сотрудников государственных организаций	22

Занятия для детей
11–15 лет

Финансовое мошенничество

Цель: сформировать у детей представление о финансовом мошенничестве.

Задачи:

- дать характеристику финансовым махинациям;
- помочь детям выявить причины, по которым люди становятся жертвой финансовых мошенников;
- охарактеризовать виды мошенничества с банковскими картами;
- предложить способы защиты от финансовых мошенников.

Оборудование:

- фломастеры или цветные карандаши;
- бланки бейджей;
- карточки для проведения игры.

Ход занятия:

Педагог: Здравствуйте, ребята! Рада встречи с вами! Чтобы познакомиться, предлагаем вам взять фломастеры/карандаши и написать свое имя на бейдже. Сделали? Молодцы. Прикрепите бейджи к одежде, давайте посмотрим, какими яркими и красочными они получились. Вот и мой бейдж. Меня зовут (*имя педагога*). А как зовут вас? Давайте познакомимся!

ПЕДАГОГ: Теперь, когда все мы познакомились, предлагаю немного поиграть. Для этого нам нужно разделиться на две команды по 8 человек. Игра будет называться «Впусти меня в свой дом». Каждому участнику игры я раздаю карточку с ролью хозяина дома — именинника, гостя или прохожего.

Именинник приготовил праздничный ужин в день своего рождения и ждет в гости друга. Случайный прохожий, заглянув в окно дома, видит красиво накрытый стол, и ему тоже хочется попасть на праздник, попробовать угощение.

В каждой команде будет по 4 хозяина, 2 гостя и 2 прохожих. Участники, получившие карточки именинников, ожидают прихода гостей. Участники — гости и прохожие не раскрывают свою роль, их задача — убедить хозяина дома, что они гости, которых ждут на ужин. Каждый из гостей и прохожих по очереди подходит

к одному хозяину и, представляясь гостем, убеждает в 3–4 предложениях пустить его в дом. Прослушав их, участник-хозяин должен принять решение: согласиться или отказать. Если он впустит прохожего или не поверит гостю, то выбывает из игры. Если впустит гостя, то побеждают сразу оба участника. Таким образом, победителем игры в каждой паре станет участник, реализовавший свою цель.

ПЕДАГОГ: Итак, ребята, давайте подведем итоги игры. Участники, игравшие роль именинников, подскажите, легко ли было поверить уговорам гостя впустить его в дом? А вам, гости и прохожие, какие аргументы помогли преодолеть сомнения хозяина дома?

ПЕДАГОГ: Как в игре, так и в жизни, ребята, мы встречаем людей, которые не всегда честны по отношению к нам, преследуют свои цели.

К таким относятся мошенники. Это люди, которые, пользуясь нашим доверием или обманывая нас, похищают наши деньги, имущество.

Знаете ли вы, что слово *мошенник* произошло от существительного *мошна* — так в Древней Руси называли сумку, карман. Человек, воровавший деньги из сумок, назывался мошенником. Со временем мошенниками стали называть обманщиков и жуликов.

Сегодня, ребята, мы поговорим с вами о мошенничестве, с которым мы можем столкнуться на финансовом рынке. Как мы знаем, существует множество компаний, оказывающих услуги по кредитованию, открытию вкладов, ведению счетов, купле-продаже ценных бумаг и валюты и так далее.

К выбору данных организаций необходимо подходить особенно тщательно, так как среди них попадает много недобросовестных компаний и просто мошенников.

ПЕДАГОГ: Как вы считаете, почему люди становятся жертвами финансовых мошенников? *(Выслушиваем ответы детей.)*

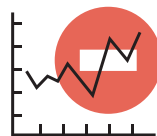
Верно, такие качества, как желание легкого заработка, невнимательное прочтение подписываемых документов, вера на слово, делают граждан легкими жертвами финансовых мошенников.

Мошенники выманивают деньги с помощью звонков и СМС, в социальных сетях и офисах.

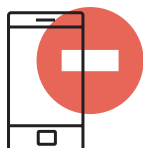
ПЕРЕЧИСЛИМ ОСНОВНЫЕ ВИДЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА:



С БАНКОВСКИМИ
КАРТАМИ



НА ФИНАНСОВЫХ
РЫНКАХ



КИБЕРМОШЕН-
НИЧЕСТВО



ФИНАНСОВЫЕ
ПИРАМИДЫ

Стать жертвой преступников может каждый, и не важно, использует он банковскую карту или предпочитает рассчитываться наличными.

Педагог: Рассмотрим мошенничество с банковскими картами подробнее. Ребята, вы, наверное, уже знаете, что представляет собой банковская карта.

Это изготовленная из пластика карта, на нее нанесена информация о держателе (содержится на магнитной полосе или чипе).

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV (специальный трехзначный код на оборотной стороне карты, необходимый для оплаты покупок в интернете).

Мошенникам нужны:



Каковы же основные способы мошенничества с банковскими картами?

КРАЖА КАРТЫ

- **Как действовать, если у вас украли карту:**
 - немедленно заблокируйте карту по телефону, указанному на ее оборотной стороне, официальном сайте банка или через личный кабинет банка.
- **Как предотвратить кражу:**
 - не храните банковскую карту вместе с ПИН-кодом. Игнорирование этого правила даст возможность мошеннику снять ваши сбережения в ближайшем банкомате или перевести через интернет;
 - установите ограничение на максимальную сумму снятия с карты в сутки и в месяц.

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О КАРТЕ

Мошенники узнают ее путем подглядывания, фото- или видеофиксации, копирования данных карты. Целью может быть не только ПИН-код, но и реквизиты вашей карты на лицевой и оборотной сторонах. Так, мошенники могут украсть ПИН-код, установив на банкомат скрытую камеру или накладную клавиатуру. Поддельную клавиатуру ставят прямо поверх оригинальной, и сам банкомат реагирует на нажатия как обычно — вы даже не заметите, что что-то идет не так. Злоумышленники, используя украденные данные, могут изготовить копию вашей карты.



КАК ПРЕДОТВРАТИТЬ?

- Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
- Старайтесь пользоваться банкоматами, установленными в безопасных местах (например, в отделениях банков).
- Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе или магазинах.
- Подключите мобильный банк и СМС- или push-уведомления. Так вы сможете увидеть, какая точно сумма списана с вашей карты после снятия денег в банкомате.
- Если вы расплачиваетесь картой в кафе, пожалуйста, просите использовать только переносной терминал, чтобы оплата происходила при вас.
- Уничтожайте копии чеков, билетов и других документов, где указан полный номер вашей карты.
- Если вам приходят СМС с уведомлениями о блокировке карты или якобы совершенных транзакциях, никогда не перезванивайте по номеру, указанному в СМС. Всегда звоните только по номеру колл-центра банка, указанному на официальном сайте, или по номеру телефона, указанному на оборотной стороне карты.

Педагог: Что же, ребята, делать, если с вашей карты списали деньги (об этом вы узнали в СМС-сообщении или взяв выписку по карте).

- Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.
- Запросите выписку по счету и напишите заявление о несогласии с операцией.
- Обратитесь с заявлением в отдел полиции по месту жительства или отправьте обращение в управление «К» МВД России.

Педагог: Давайте закрепим полученные знания на практике. Разделимся на две команды. Я раздам вам карточки, а вы расскажете, как поступите в предложенной ситуации. Эксперты выскажут нам свое мнение.

Раздаем каждой команде поочередно по две ситуационные карточки, даем ребятам 1–2 минуты посоветоваться, затем выслушиваем их мнения. Предлагаем второй команде зачитать экспертное мнение по ситуациям противников.

СИТУАЦИЯ

В кафе официант приносит вам POS-терминал, вы расплачиваетесь, но тут официант говорит, что оплата не прошла, и просит повторно ввести ПИН-код вашей карты. Ваши действия?

ЭКСПЕРТ

Вводя повторно ПИН-код, вы рискуете заплатить дважды. Подключите СМС- или push-уведомления о платежах по вашей карте. Обязательно попросите чек с уведомлением о сбое или отказе от операции (POS-терминал всегда печатает такой).

СИТУАЦИЯ

Вам нужно снять деньги с карты. На противоположной стороне улицы в стену магазина встроен уличный банкомат. Улица плохо освещена, и возле банкомата стоят какие-то люди. Ваши действия?

ЭКСПЕРТ

Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.

Проверьте банкомат: нет ли на нем посторонних устройств. Клавиатура не должна отличаться по фактуре, а тем более шататься.

Когда вводите ПИН-код, всегда прикрывайте клавиатуру свободной рукой, чтобы никто не подсмотрел.

Лучше всего, если на банкомате есть «крылья» для клавиатуры — на них невозможно поставить накладную клавиатуру. Также благодаря им сложнее подсмотреть ваш ПИН-код.

СИТУАЦИЯ

После поездки в переполненном автобусе вы не смогли обнаружить кошелек в своем рюкзаке. Очевидно, что его у вас украли. В кошельке были не только деньги, но и карта, на которую вам перечисляют стипендию. Ваши действия?

ЭКСПЕРТ

Необходимо позвонить в банк и заблокировать карту. Если вы не можете связаться с банком по телефону, зайдите в ближайшее отделение банка и напишите заявление о блокировке. Также вы можете заблокировать карту через онлайн-банк.

СИТУАЦИЯ

Вы снимаете деньги в офисе банка, довольно близко от вас стоит молодой человек и, дружелюбно улыбаясь, наблюдает за тем, как вы вводите ПИН-код на клавиатуре банкомата. Ваши действия?

ЭКСПЕРТ

Не стоит ссориться, но нужно прикрыть клавиатуру рукой в тот момент, когда вы будете набирать ПИН-код, и постараться закрыть собой монитор банкомата, чтобы никто не видел, какие именно операции вы совершаете по карте.

— Молодцы, ребята! Прекрасно справились с поставленной задачей. Будем уверены, что вы не попадетесь на удочку финансовых мошенников!

Хочется обратить ваше внимание на то, что мошеннические действия не остаются безнаказанными, — в Уголовном кодексе Российской Федерации есть статья 159 «Мошенничество», которая определяет мошенничество как хищение

чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. В статье прописаны способы наказания за совершенные преступления.

Нельзя присваивать чужое имущество и деньги. Мы не должны становиться жертвами финансовых мошенников, а тем более переходить на их сторону.

ВОПРОСЫ ПО РЕЗУЛЬТАТАМ ЗАНЯТИЯ

Педагог: А теперь, ребята, выполним небольшой тест и узнаем, как хорошо вы запомнили материал сегодняшнего занятия. Ответьте на вопросы, выбрав один из трех вариантов ответа:

1. Кто такой финансовый мошенник?

- Человек, присвоивший чужое имущество обманом
- Человек, нашедший кошелек на улице
- Человек, выигравший в лотерею

2. Как вы считаете, почему люди становятся жертвами финансовых мошенников?

- Из-за излишней доверчивости
- Из-за желания заработать быстро и много
- Все вышеперечисленное

3. Что необходимо сделать в первую очередь, если вашу банковскую карту украли?

- Забыть о случившемся
- Заблокировать карту
- Открыть новую карту

4. Вам необходимо снять деньги. В каком банкомате из нижеперечисленных вы снимете нужную сумму?

- В уличном. Много людей ходит мимо, хотя улица плохо освещена.
- В торговом центре. Не очень удобно, что вокруг банкомата постоянно много людей, но я сделаю это аккуратно.
- В офисе банка. Там наверняка банкоматы проверяют на наличие устройств видеофиксации данных карты.

5. Почему рекомендуют при наборе ПИН-кода в банкомате или POS-терминале прикрывать клавиатуру рукой?

- Так довольно сложно подсмотреть или заснять на видео ПИН-код, который вы набираете на клавиатуре банкомата или POS-терминала.
- Если не прикрывать клавиатуру рукой, то тогда ПИН-код не будет считываться в устройстве.
- Не знаю, я никогда не прикрываю.



Кибермошенничество

Цель: сформировать у воспитанников организаций для детей-сирот представление о кибермошенничестве

Задачи:

- дать характеристику кибермошенничеству;
- раскрыть содержание видов преступлений в сфере информационных технологий;
- рассказать детям о том, как надо поступать в случае сомнительных, тревожных телефонных звонков, писем на электронную почту и СМС;
- рассмотреть с воспитанниками действия мошенников в интернете с целью кражи персональных данных, реквизитов платежных карт;
- обсудить способы защиты от действий кибермошенников.

Оборудование:

- фломастеры или цветные карандаши;
- бланки бейджей;
- карточки для проведения игры.

Ход занятия

Педагог: Добрый день, ребята! Рада встрече с вами! Давайте познакомимся! Перед вами лежат бейджи. Пожалуйста, возьмите в руки фломастеры/карандаши и напишите на бейджах свои имена. Вот и мой бейдж. Меня зовут *(имя педагога)*.

Сегодня нас ждет увлекательное занятие, участвовать в котором мы будем командами. Прошу вас разделиться на две команды *(в занятии принимают участие до 20 человек, поровну в каждой команде)*. Предлагаю командам представить своих участников остальным. Для этого используйте следующие фразы *(раздаем ребятам лист с фразами)*:

1. Мы ценим *(имя)* за то, что...
2. Самый веселый среди нас — это *(имя)*.
3. Самый спортивный среди нас — это *(имя)*.
4. Лучше всех из нас поет *(имя)*.
5. Будущий артист среди нас *(имя)*.
6. Настоящий танцор среди нас — это *(имя)*.

7. Настоящий фокусник среди нас (имя).
8. Лучше всех среди нас на музыкальном инструменте играет (имя).
9. Самые лучшие поделки среди нас делает (имя).
10. Настоящий художник среди нас (имя).

ПЕДАГОГ: Молодцы, ребята! Теперь мы все знаем о ваших талантах. Хорошо поиграли, хорошо и поработаем сегодня.

Наше занятие посвящено тому, как распознать финансовых мошенников в сфере информационных технологий (компьютеров, телефонов и других гаджетов).

ПОГОВОРИМ О КИБЕРМОШЕННИЧЕСТВЕ:

- финансовом мошенничестве по телефону;
- финансовом мошенничестве в интернете;
- мошеннических СМС-сообщениях и письмах на электронный адрес.

ПЕДАГОГ: В нашей жизни складываются различные ситуации, при которых мы можем стать жертвой преступников. Мошенники умеют выманить деньги через интернет, с помощью звонков и СМС, в социальных сетях. Сейчас я раздам каждой команде по 5 карточек с описанием ситуации. Вам необходимо кратко написать свой ответ о том, что вы будете делать, и вернуть карточки мне. Ваши ответы мы обсудим немного позже.

СИТУАЦИЯ

Вы хотите продать свой старый телефон через сайт объявлений в интернете. С вами связался заинтересованный покупатель и готов перевести деньги вам на карту. Он просит вас сообщить номер карты, срок действия, имя держателя на английском языке, а также трехзначный код на оборотной стороне карты. Так деньги точно дойдут.

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

На мобильный телефон / электронную почту вам пришло сообщение: «Добрый день, будущий коллега! Хочу предложить тебе интересную, высокооплачиваемую работу. Я вижу, ты очень активен в социальных сетях, поэтому предлагаю тебе размещать посты о нашей компании в интернете. Работенка непьющая, оплата 1000 долларов США в месяц. Торопись, друг, подобное письмо я направил еще нескольким парням, кто первый из вас перейдет по ссылке _____, тот и получит работу своей мечты!»

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

Вы получили сообщение от друга через социальную сеть с просьбой одолжить денег: «Привет, срочно нужно 500 рублей, перекинь на номер х-xxx-xxx-xx-xx, я все объясню».

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

На мобильный телефон вам пришло сообщение: «Поздравляем, вы стали тысячным посетителем нашего сайта. Вы выиграли ноутбук! Это не розыгрыш, перешлите на указанный номер ХХХ фото своего паспорта, номер телефона, мы вам перезвоним для отправки ноутбука».

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

На мобильный телефон / электронную почту вам пришло сообщение: «Меня зовут Али Райзберг, я состоятельный адвокат, находящийся в плену одного из африканских племен. Мне очень нужна помощь. Необходимо перечислить 200 долларов США людям, удерживающим меня. Попав на свободу, я верну вам сумму в 10 раз больше — 2000 долларов США. Перейдите по ссылке, указанной ниже, так вы сможете перевести мне деньги со своей карты. Благодарю за помощь!»

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

На вашу электронную почту приходит письмо с адреса известной платежной системы: «Мы подвели итоги лотереи держателей карт нашей платежной системы. Поздравляем вас с победой в конкурсе! Перейдите по ссылке для получения приза». Вы перешли по ссылке и видите знакомую вам страницу сайта, правда немного, худшего качества, чем всегда (логотип платежной системы какой-то нечеткий). Перед вами форма для заполнения информации по вашей карте, куда вам перечислят деньги.

ВАШИ ДЕЙСТВИЯ

СИТУАЦИЯ

На ваш мобильный телефон пришло сообщение: «Вам поступил платеж 200 рублей». При этом вы не пополняли счет своего телефона. Вы удивлены. Через 10–15 минут приходит новое сообщение: «Извините, ошибочно перевела 200 рублей на ваш счет. Пожалуйста, верните деньги на мой номер х-xxx-xxx-xx-xx. Лиза».

ВАШИ ДЕЙСТВИЯ**СИТУАЦИЯ**

На интернет-сайте, посвященном новинкам в области мобильных гаджетов, вы увидели программу, позволяющую бесплатно звонить друзьям. Ее можно скачать на ваш телефон. Вы впервые на данном сайте, предложение скачать программу весьма заманчиво, с таким вы еще не сталкивались.

ВАШИ ДЕЙСТВИЯ**СИТУАЦИЯ**

Вы зашли на страницу банка, на карту которого получаете стипендию или пособие, для того, чтобы оплатить мобильную связь. Вас немного насторожило, что страница сайта выглядит как-то иначе, в названии банка допущена ошибка, ссылки, по которым вы собираетесь пройти, не работают. Но возможность совершить оплату присутствует. Ваши действия?

ВАШИ ДЕЙСТВИЯ**СИТУАЦИЯ**

На мобильный телефон вам звонит человек и, представляясь сотрудником банка, сообщает, что по вашей банковской карте была проведена подозрительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты.

ВАШИ ДЕЙСТВИЯ

Педагог: Ребята, заполняя карточки, вы познакомились с различными ситуациями, в которых вам предстояло сделать выбор: переводить деньги или нет, пересылать данные банковской карты третьим лицам или не пересылать. Давайте поговорим об этом подробно.

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ

КАК ЭТО РАБОТАЕТ?

Мошенники звонят в основном наугад. В зависимости от того, кто снял трубку (взрослый, ребенок, пожилой человек), они сообщают о следующем:

- кто-то из близких или друзей в беде (попал в ДТП, забрали в полицию, положили в больницу), необходимо очень срочно перевести/передать деньги по номеру телефона, передать курьеру, который подъедет по указанному адресу, и так далее;
- по вашей банковской карте была проведена подозрительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты и так далее. «Вы не должны сомневаться, потому что вам звонит сотрудник службы безопасности вашего банка», — говорит голос в трубке;
- вы стали победителем конкурса среди номеров абонентов сотовой связи / выиграли ноутбук как тысячный посетитель сайта / выиграли смартфон последней модели как активный участник социальной сети. Для получения приза необходимо переслать копию паспорта на указанный номер или перейти по ссылке, чтобы заполнить информацию о вашей банковской карте для выплаты стоимости выигрыша.

Все эти звонки объединяет одно: на другом конце телефонного провода — специалисты по обману, которые всеми правдами и неправдами хотят выманить необходимые им данные, играют на ваших желаниях, чувствах и заботе о близких.

КАК ПОСТУПИТЬ?

- Не поддавайтесь панике и подумайте о том, что вас попросили сделать. Скажите, что вы сами созвонитесь с другом и прекратите разговор, как бы настойчив ни был собеседник. Не паникуйте! Свяжитесь с другом, близким человеком и уточните, все ли у него в порядке, нужна ли ему помощь. Если он сразу не ответит на ваш телефонный звонок, не торопитесь, подождите, когда друг перезвонит. Если вы очень беспокоитесь за друга, позвоните его брату/сестре/родителям, скажите, что звонил человек, который произвел впечатление мошенника, и попросите связаться с другом. Если вам повторно перезванивают с того же номера, не берите трубку или сбросьте вызов.



- Если вас просят переслать копию паспорта, продиктовать номер банковской карты, ПИН-код, другие данные, не поддавайтесь этим уговорам! **Не паникуйте!** Настоящие сотрудники банка, министерства здравоохранения, полиции никогда не попросят по телефону вашу персональную информацию, не отправят сообщения с формой для ввода данных вашего паспорта, не попросят вас зайти в личный кабинет по ссылкам в письмах.

ПЕДАГОГ: Возвращаясь к карточкам, которые вы заполнили ранее, давайте посмотрим ответы. *(Педагог зачитывает ситуацию, ответы команд.)* Изменилось ли ваше мнение сейчас? Как вы поступите в описанных ситуациях? Предлагаю кому-нибудь из вас выступить в роли эксперта и прокомментировать, как правильно поступать в подобных случаях. *(Ребенок зачитывает карточку «Эксперт» по предложенной ситуации.)*

СИТУАЦИЯ

Вы хотите продать свой старый телефон через сайт объявлений в интернете. С вами связался заинтересованный покупатель и готов перевести деньги вам на карту. Он просит вас сообщить номер карты, срок действия, имя держателя на английском языке, а также трехзначный код на оборотной стороне карты. Так деньги точнойдут. Ваши действия?

ЭКСПЕРТ

Такой подход должен вас насторожить — для перевода денег достаточно знать только номер карты. Если вы передадите основные платежные данные карты, то рискуете остаться без денег. Мошенники смогут расплатиться картой в интернет-магазине.

СИТУАЦИЯ

Вам на мобильный телефон звонит человек и, представляясь сотрудником банка, сообщает, что по вашей банковской карте была проведена подозрительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты.

ЭКСПЕРТ

Сотрудники банка владеют необходимой информацией для блокировки карты. Им незачем спрашивать ее у вас. Не реагируйте на подобный звонок, в случае сомнений перезвоните в банк по телефону, указанному на оборотной стороне карты.

ПЕДАГОГ: Ребята, мы познакомились с уловками телефонных мошенников.



МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

КАК ЭТО РАБОТАЕТ?

Мошенники рассылают СМС-сообщения и письма на электронную почту с целью выведать данные вашего паспорта и банковской карты следующим образом:

- в социальных сетях вам предлагают купить какой-либо товар по весьма привлекательной цене. Для оплаты необходимо перейти по ссылке и ввести данные банковской карты, а возможно, и прикрепить копию паспорта;
- на вашу электронную почту или мобильный телефон приходит сообщение от друга с просьбой одолжить денег или со странной ссылкой. Очень похожее сообщение может прийти от какого-либо богатого иностранца, находящегося далеко от своего дома, просящего вас перевести ему деньги, чтобы решить проблемы. После он обещает вам вернуть гораздо больше, чем ваша помощь;
- с сайта известной компании вы получили сообщение с предложением заработать крупную сумму денег, работа непостоянная, в основном в интернете. Правда, вначале необходимо пройти обучение, которое стоит небольших денег. Оплатить курс вы можете, пройдя по ссылке;
- на вашу электронную почту или мобильный телефон приходит сообщение о вашем выигрыше в лотерею, для получения крупного денежного приза вас просят переслать реквизиты карты.

Эти и другие сообщения говорят о том, что вам пишут мошенники, играющие на вашей жалости, желании быстро и легко заработать.

КАК ПОСТУПИТЬ?

- Будьте осторожны, покупая товары с рук через социальные сети или специальные сайты. Всегда старайтесь проверить потенциального покупателя или продавца по отзывам. В сообществах и на сервисах обычно есть «черный список» (и покупателей, и продавцов) и модераторы. Проверьте профиль продавца – часто мошенники создают фальшивые страницы с минимумом информации.

- Если странные сообщения через социальные сети шлет ваш друг, как можно скорее позвоните ему и выясните, действительно ли ему нужна помощь или мошенники взломали его аккаунт и могут обмануть кого-то еще.
- Ссылки из сообщений незнакомцев не лучший способ искать заработок в интернете, потому что бесплатный сыр бывает только в мышеловке.
- Если незнакомцы пишут вам от лица компании или бренда, лучше уточнить информацию на официальном сайте компании или ее странице в социальной сети – крупные компании редко проводят конкурсы, в которых вы можете победить, даже не участвуя, и никогда просто так не запрашивают ваши личные данные, а тем более данные карты.
- Если вам приходит на почту письмо от незнакомца, например иностранца, или от известной компании, то ничего страшного не произойдет, если вы просто откроете письмо. Но не переходите по ссылкам и не скачивайте вложения из письма – так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карты. В почте есть встроенный спам-фильтр – часть подозрительных писем всегда попадает в специальную папку. Но, несмотря на это, всегда обращайте внимание на заголовок письма, его отправителя и содержание. Компании всегда рассылают почтовые рассылки с одних и тех же адресов и редко допускают ошибки в письмах, а вот мошенники часто пишут с большим количеством ошибок, нечитаемых системой символов и перевирают название компании в адресе. Не переходите по ссылкам из таких писем и не скачивайте вложения из них.

ПЕДАГОГ: А теперь давайте узнаем, что вы ответили на ситуации, описанные в следующих карточках. *(Педагог зачитывает по одной карточке, а также ответы детей на них.)* Кто хочет побыть экспертом и зачитать ответы на данные ситуации?

СИТУАЦИЯ

На вашу электронную почту приходит письмо с адреса известной платежной системы: «Мы подвели итоги лотереи держателей карт нашей платежной системы. Поздравляем вас с победой в конкурсе! Перейдите по ссылке для получения приза». Вы перешли по ссылке и видите знакомую вам страницу сайта, правда, немного худшего качества, чем всегда (логотип платежной системы какой-то нечеткий). Перед вами форма для заполнения информации по вашей карте, куда вам перечислят деньги. Ваши действия?

ЭКСПЕРТ

Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, поступила ли стипендия на вашу карту, вводите логин и пароль на сайте банка, а попадаете на сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников. В данном случае о том, что это сайт-клон, говорит нечеткое изображение логотипа. Если попытаете открыть другие страницы сайта, они могут не открываться.

СИТУАЦИЯ

На мобильный телефон / электронную почту вам пришло сообщение: «Добрый день, будущий коллега! Хочу предложить тебе интересную, высокооплачиваемую работу. Я вижу, ты очень активен в социальных сетях, поэтому предлагаю тебе размещать посты о нашей компании в интернете. Работенка непыльная, оплата 1000 долларов США в месяц. Торопись, друг, подобное письмо я направил еще нескольким парням, кто первый из вас перейдет по ссылке _____, тот и получит работу своей мечты!»

ЭКСПЕРТ

Перейдя по такой ссылке, вы не найдете работу мечты — разве что компьютерный вирус. Будьте осторожны, получая предложения легкого заработка.

СИТУАЦИЯ

На ваш мобильный телефон пришло сообщение: «Вам поступил платеж 200 рублей». При этом вы не пополняли счет своего телефона. Вы удивлены. Через 10–15 минут приходит новое сообщение: «Извините, ошибочно перевела 200 рублей на ваш счет. Пожалуйста, верните деньги на мой номер х-xxx-xxx-xx-xx. Лиза».

ЭКСПЕРТ

Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС пришло не от вашего банка, а повторное СМС прислал вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

СИТУАЦИЯ

На мобильный телефон / электронную почту вам пришло сообщение: «Меня зовут Али Райзберг, я состоятельный адвокат, находящийся в плену одного из африканских племен. Мне очень нужна помощь. Необходимо внести сумму 200 долларов США людям, удерживающим меня. Попав на свободу, я верну вам сумму в 10 раз больше — 2000 долларов США. Перейдите по ссылке, указанной ниже, так вы сможете перевести мне деньги со своей карты. Благодарю за помощь!» Ваши действия?

ЭКСПЕРТ

Перед вами письмо мошенников. Ничего страшного не произойдет, если вы просто откроете письмо, но не переходите по ссылкам и не скачивайте вложения из письма — так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карты.

СИТУАЦИЯ

Вы получили сообщение от друга через социальную сеть с просьбой одолжить денег: «Привет, срочно нужны 500 рублей, перекинь на номер х-xxx-xxx-xx-xx, я все объясню».

ЭКСПЕРТ

Получив подобное сообщение, будьте уверены, что аккаунт вашего друга взломан. Постарайтесь связаться с ним и уточнить, действительно ли ему нужна помощь. Предупредите друга, что его аккаунт взломан. Ни в коем случае не переводите деньги в ответ на данное сообщение.

СИТУАЦИЯ

На мобильный телефон вам пришло сообщение: «Поздравляем, вы стали тысячным посетителем нашего сайта. Вы выиграли ноутбук! Это не розыгрыш, перешлите на указанный номер х-xxx-xxx-xx-xx фото своего паспорта, номер телефона, мы вам перезвоним для отправки ноутбука». Ваши действия?

ЭКСПЕРТ

Таким образом мошенники пытаются выудить у вас персональные данные (паспорта, банковской карты). Как говорится, бесплатный сыр бывает только в мышеловке. Не верьте подобной информации, не отправляйте свои данные мошенникам.

Педагог: Отлично справились, ребята! А теперь давайте поговорим о финансовом мошенничестве в интернете.

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ**КАК ЭТО РАБОТАЕТ?**

- Мошенники крадут информацию о вашей банковской карте во время покупок на сайтах интернет-магазинов, при пользовании мобильным банком, копируя сайты известных компаний и банков. Например, вы решили пополнить баланс своего телефона через мобильный банк, зашли на сайт банка, а попали на сайт-клон. Если вы введете на таком сайте свои данные, они попадут в руки злоумышленников.
- На электронную почту вам может прийти сообщение от вашего банка о том, что во время последней операции произошла ошибка, в связи с чем вам нужно перейти по ссылке и повторно ввести информацию вашей карты.
- Скачивая различные программы и приложения на свой смартфон, вы рискуете заразить его вирусом, который передаст информацию о вашей карте мошенникам.



КАК ПРЕДОТВРАТИТЬ?

- Скачивайте приложения на телефон только в официальном магазине. Обращайте внимание в первую очередь на разработчика приложения – в официальных банковских приложениях указан сам банк. Внимательно читайте описание приложения. Не скачивайте приложения сторонних разработчиков.
- Пользуйтесь только личными устройствами. Делайте покупки, заходите в свой интернет-банк или мобильный банк только с личного компьютера и смартфона. Обязательно ставьте на них пароль. Если вы потеряете телефон, к которому подключено СМС-информирование или мобильный банк, срочно позвоните в банк и отключите от утерянного номера все услуги.
- Защититесь от вирусов. Обязательно поставьте антивирус на всех своих устройствах, включая мобильные, и регулярно обновляйте их. Не устанавливайте антивирусы, скачанные из неофициальных источников!
- Выбирайте безопасные сайты. Никогда не переходите по ссылкам из писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать их. Возможно, у мошенников появился доступ к их аккаунтам и они хотят получить доступ и к вашим данным.
- Набирайте интернет-адрес банка вручную, а еще лучше — сохраняйте в закладках адреса ваших банков, а также госорганов и других организаций.
- Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с <https://>. В адресной строке есть значок в виде закрытого замка.
- Выбирайте известные интернет-магазины и сервисы. Изучите отзывы о них других пользователей. Лучше всего посмотреть отзывы на нескольких независимых сайтах. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные.
- Никому не сообщайте персональную информацию. Чаще всего в краже средств со счета виноваты вовсе не банки или онлайн-магазины, а сами довер-

чивые пользователи. Мошенники знают множество уловок, чтобы втереться к вам в доверие. И ваша задача не попасться на эти уловки. Никогда не сообщайте посторонним данные своей карты, персональные данные и коды из СМС. Никому не говорите ваш ПИН-код и код проверки подлинности карты — последние три цифры на ее оборотной стороне. Даже сотрудники банка не вправе требовать от вас эти данные. Если кто-либо пытается их узнать, будьте уверены — это мошенник.

- Подключите СМС-оповещения об операциях по карте. В этом случае вы сразу же узнаете о платеже, который вы не совершали, и сможете быстро отреагировать: заблокировать карту и опротестовать операцию.

Педагог: Ребята, давайте посмотрим, как вы ответили на вопросы по интернет-мошенничеству. *(Педагог зачитывает ответы.)* Заслушаем также мнение эксперта.

СИТУАЦИЯ

Вы зашли на страницу банка, на карту которого получаете стипендию или пособие, для того, чтобы оплатить мобильную связь. Вас немного насторожило, что страница сайта выглядит как-то иначе, в названии банка допущена ошибка, ссылки, по которым вы собираетесь пройти, не работают. Но возможность совершить оплату присутствует. Ваши действия?

ЭКСПЕРТ

Возможно, ваш смартфон заражен вирусом, который перенаправил вас с официального сайта банка на сайт-клон, похожий как две капли воды на оригинальный сайт. Если вы введете информацию по карте, то ваши деньги уйдут мошенникам. Чтобы обезопасить себя, набирайте вручную адрес сайта, не переходите по ссылкам из интернета. Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с `https://`. В адресной строке есть значок в виде закрытого замка.

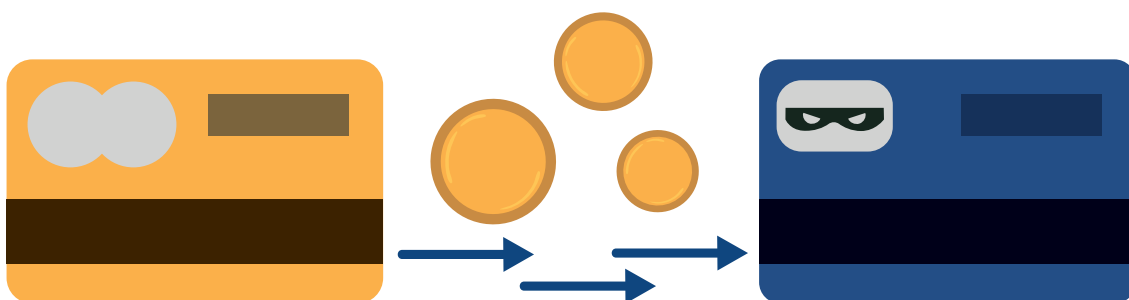
СИТУАЦИЯ

На интернет-сайте, посвященном новинкам в области мобильных гаджетов, вы увидели программу, позволяющую бесплатно звонить друзьям. Ее можно скачать на ваш телефон. Вы впервые на данном сайте, предложение скачать программу весьма заманчиво, с таким вы еще не сталкивались.

ЭКСПЕРТ

Скачав программу, вы рискуете заразить вирусом свой компьютер. Для скачивания программ используйте только проверенные интернет-магазины, интернет-сайты.

Итак, мы разобрали с вами виды кибермошенничества, узнали, что нужно сделать, чтобы не стать жертвой мошенников.



ЧТО НЕОБХОДИМО СДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1. ЗАБЛОКИРУЙТЕ КАРТУ

Если с карты списали деньги без вашего ведома, позвоните в банк и заблокируйте карту. Номер горячей линии банка указан на оборотной стороне карты. Запишите этот телефон и храните в отдельном месте.

Так же нужно поступить, если вы потеряли карту или даже просто подозреваете, что ее данные стали известны посторонним людям.

2. ОПРОТЕСТУЙТЕ ОПЕРАЦИЮ

В тот же день (максимум — на следующий), когда вы получили СМС-сообщение о снятии денег, покупке в магазине, которые вы не делали, обратитесь в отделение банка. Запросите выписку по счету и напишите заявление о несогласии с операцией, которую не совершали.

Если банк докажет, что вы нарушили правила использования карты, то вернуть деньги не получится. Например, в том случае, когда вы сами сообщили кому-то реквизиты своей карты, трехзначный код с ее оборотной стороны или ПИН-код.

2. ОБРАТИТЕСЬ В ПОЛИЦИЮ

Можно просто написать заявление в отделение полиции по месту жительства. Чем быстрее вы это сделаете, тем будет больше шансов найти преступников и вернуть деньги.

ВОПРОСЫ ПО РЕЗУЛЬТАТАМ ЗАНЯТИЯ

Педагог: Надеюсь, что полученные сегодня знания вам пригодятся в жизни! Для закрепления пройденного материала предлагаю вам, ребята, ответить на вопросы теста. Выберите 1 из 3 вариантов ответа:

1. Что вы будете делать, если в социальной сети вам пришло сообщение от службы безопасности банка с уведомлением о блокировке вашей карты?

- Перейду по ссылке, которую мне указали в сообщении, чтобы разблокировать карту.
- Не буду ничего делать, так как настоящая служба безопасности банка не рассылает сообщения через социальные сети.
- Не буду паниковать, но позвоню в банк и заблокирую карту.

2. В социальной сети вам пришло сообщение от лучшего друга с просьбой срочно перевести 1000 рублей на незнакомый номер. Каковы ваши действия?

- Прежде чем перевести деньги, созвонюсь с другом и уточню, действительно ли он прислал мне данное сообщение?
- Мне ничего не жалко для друга, обязательно переведу.
- Зачем звонить и уточнять, переведу без разговоров, сумма небольшая.

3. Вам пришло СМС с известного сайта с поздравлением с выигрышем, так как именно вы стали тысячным посетителем. Какая удача! Чтобы получить заветный выигрыш — телефон, необходимо переслать на указанный в СМС адрес копию всех страниц своего паспорта. Как вы поступите?

- Ура, я выиграл новый телефон! Конечно, перешлю копию паспорта.
- Копия паспорта нужна, иначе как доказать, что я победитель? Не очень хочется пересылать, но телефон стоит того.
- Пересылать копию паспорта не буду. Просто так новые телефоны никому не раздают. А паспортными данными могут воспользоваться мошенники.

4. Вам пришло сообщение на мобильный телефон об ошибочном зачислении 200 рублей. Просят вернуть на указанный номер. Ваши действия?

- Я честный, верну без разговоров.
- А почему не было СМС от сотового оператора о зачислении средств? Нет, явно деньги мне не поступали, свои отдавать не собираюсь.
- Подумаю, но, скорее, верну. Вдруг я попаду в подобную ситуацию?

5. Вы решили проверить баланс своей карты через интернет. Зашли на страницу сайта банка, но на первый взгляд показалось, что сайт выглядит необычно: расплывчатый логотип, в строке браузера указано не название банка, а какое-то другое слово, не все ссылки открываются. Будете ли вы вводить логин и пароль для входа в систему?

- Не буду, так как есть риск отправить свои данные мошенникам.
- Введу, просто интернет барахлит.
- Возможно, на сайте банка ведутся работы, ничего страшного, введу и логин, и пароль.

**Занятие для детей
16–18 лет**

Мошенники, которые маскируются под сотрудников государственных учреждений

Цель: научить воспитанников распознавать популярную мошенническую схему, когда злоумышленник представляется сотрудником государственной организации.

Задачи:

- продемонстрировать примеры таких махинаций;
- помочь детям понять, почему люди становятся жертвой финансовых мошенников;
- рассказать воспитанникам, как не стать их жертвой.

Оборудование:

- фломастеры (цветные карандаши);
- флипчарт;
- бланки бейджей;
- карточки для проведения игры.

Ход занятия:

Педагог: Всем привет! Давайте познакомимся. Меня зовут (*имя педагога*). Чтобы лучше запомнить имена друг друга, возьмем фломастеры и запишем их на бейджах.

ПЕДАГОГ: У меня есть знакомая — Света, ваша ровесница. Недавно с ней произошел очень неприятный случай. С неизвестного «красивого» номера ей позвонил администратор торгового центра «Мечта», где она покупала одежду на прошлой неделе. Он рассказал ей, что именно тогда в «Мечте» проходил розыгрыш призов «Мечты сбываются» и Света выиграла смартфон. Теперь ей нужно в течение трех дней подойти к администратору и забрать приз. С собой нужно взять паспорт и чек.

Света так давно хотела новый смартфон, но сомневалась — не обман ли это. Но ведь она правда была в этом ТЦ на прошлой неделе, как об этом мог узнать посторонний? Света поверила в удачу.

На следующий день она собиралась отправиться за выигрышем, но вдруг раздался звонок из налоговой. Туда передали информацию о выигрыше девушки, и теперь она должна заплатить налог — 35% от стоимости смартфона, 28 тысяч рублей. Как сказал сотрудник налоговой службы, приз достанется ей только после уплаты пошлины — таков закон. Но, если Света поторопится, то, как и со штрафами ГИБДД, ей нужно будет заплатить всего лишь половину суммы — 14 тысяч рублей. Выгода налицо, ведь новый смартфон стоит аж 80 тысяч рублей! Сотрудник налоговой согласился переслать СМС-сообщением номер счета, на который Света может перевести налог на выигрыш. Только после этого с квитанцией об уплате налога, паспортом и чеком девушке выдадут выигранный смартфон.

Как вы думаете, чем закончилась эта история?

Педагог: Давайте обсудим ситуацию. Для этого разделимся на две команды. Первой команде нужно доказать, что Света, уплатив налог на выигрыш, получила смартфон в торговом центре «Мечта», вторая команда должна объяснить, почему Света не получила обещанный приз. Достаточно высказать до 5 аргументов в поддержку мнения каждой команды.

При наличии флипчарта или доски воспитанники записывают и доказывают тезисы своих команд.

Педагог: Благодарю команды за высказанное мнение. Как бы вы поступили в такой ситуации? Что заставит поверить / не поверить звонящим вам людям?

К сожалению, случай, произошедший со Светой, весьма типичный. Часто людям приходят СМС с предложением получить компенсацию за выигрыш, приобретенные ранее лекарства, потерянные при обмене денег сбережения и т.п. Во всех этих ситуациях жертве сначала предлагают заплатить «налог» или «госпошлину», и лишь затем мнимый чиновник обещает отправить деньги. Так и со Светой: мошенники, зная, где девушка делает покупки, позвонили ей, рассказали легенду о выигрыше, а затем попросили уплатить налог.

Свету должно было насторожить, что звонок из налоговой раздался так поспешно и что деньги нужно было перевести на счет, отправленный по СМС.

- 👉 Государственные органы всегда официально уведомляют граждан. Телефон отделения налоговой есть на сайте Федеральной налоговой службы — можно сравнить оба номера.
- 👉 Мошенники всегда пытаются оказать давление на жертву, поторопить ее, не оставляя времени на размышление, говорят, что акция с призами заканчивается, необходимо срочно поторопиться, чтобы не упустить предложение.

Педагог: Сталкивались ли вы с мошенниками, которые выдают себя за сотрудников государственных органов? Что это были за ситуации и как вы поступили? Как вы думаете, кто чаще всего становится жертвой подобных мошенников?

ПЕДАГОГ: Давайте потренируемся распознавать действия мошенников. Я передам вам мешок (короб), в котором лежат карточки с описанием различных мошеннических схем. Вам нужно взять карточку, прочитать ее. Одновременно на столе разложены (или вывешены на доске) карточки с ответами на описанные схемы. Выберите из карточек с ответами ту, которая больше всех подходит к вашей ситуации.

СИТУАЦИЯ

Звонок из Министерства труда и социальной защиты. Вам рассказывают про пособие, которое положено выпускнику организации для детей-сирот. Чтобы перевести деньги на карту, необходимо сообщить ее данные звонящему.

ОТВЕТ

Необходимо проверить информацию. Государственные организации не запрашивают по телефону реквизиты банковских карт граждан. Перезвоните в Министерство труда и социальной защиты, уточните, мог ли поступить звонок от их сотрудника.

СИТУАЦИЯ

В ячейке Центрального банка лежат средства, которые вы можете получить. Поскольку деньги ждали, пока вы достигните совершеннолетия, набежали проценты за аренду ячейки в банке. Переведите на указанный счет небольшую сумму (10 тысяч рублей), и вы получите 215 тысяч рублей. Однако время ограничено, если не поторопитесь, то через 7 дней деньги в ячейке перейдут государству.

ОТВЕТ

Если вам звонят от имени Центрального банка, позвоните на телефон горячей линии Банка России: 8-800-300-3000. Помните, что Банк России не обслуживает физических лиц!

СИТУАЦИЯ

Звонок из Минздрава с предложением приобрести таблетки для похудения. Таблетки отсутствуют в аптеках, так как их разработка является абсолютно секретной. Необходимо перевести деньги на указанный сотрудником счет.

ОТВЕТ

Мошенникам невыгодно, чтобы вы были бдительными, проверяли информацию. Поэтому они могут говорить о «секретной информации» или о том, что вы должны принять решение о переводе денег, совершении покупки прямо сейчас. Не поддавайтесь на провокации.

СИТУАЦИЯ

Позвонивший вам на телефон мужчина представился полицейским. Сообщает о том, что машина вашего друга угнана и на ней совершили ДТП. Отвечать перед законом будет ваш друг. Чтобы замять инцидент, полицейский предлагает передать курьером небольшую сумму денег. Курьер приедет в назначенное место.

ОТВЕТ

Не паникуйте, позвоните в полицию и узнайте, участвовал ли конкретный автомобиль в ДТП. Не переводите деньги незнакомым людям. К тому же помните, что замять инцидент означает, по сути, дачу взятки, а это уголовное преступление!

СИТУАЦИЯ

Звонок из регионального отделения Министерства финансов. Вам предлагают компенсацию коммунальных платежей. Был сделан перерасчет по оплате за жилье, вы можете получить деньги, направив реквизиты банковской карты на указанный телефонный номер.

ОТВЕТ

Если вам предлагают деньги от имени какого-либо ведомства (например, Министерства финансов), позвоните туда, зайдя на официальный сайт министерства, и уточните информацию. Не сообщайте реквизиты банковской карты даже тем, кто представляется сотрудником министерства.

СИТУАЦИЯ

Объявление в интернете: «Государственной компании требуются на удаленную работу сотрудники без опыта работы. Оплата достойная. Обязанности: наклеивание марок на конверты для пересылки писем гражданам. Перед трудоустройством необходимо пройти двухдневное обучение, стоимость обучения – 5000 рублей».

ОТВЕТ

Подумайте, насколько реально предложение о работе. Цель мошенников — получить ваши деньги за предполагаемое обучение. Возможно, что за наклеенные и направленные работодателю конверты вам не перечислят деньги.

ПЕДАГОГ: Молодцы, справились с заданием!

А теперь посмотрите на эту памятку, давайте разберем ее вместе.

СИТУАЦИЯ

Вам звонит человек, представляющийся сотрудником государственного учреждения, просит перевести деньги на счет, чтобы вы получили ваш выигрыш или компенсацию за лекарства, коммунальные услуги, покупки. А может, на ваше имя открыт вклад в банке (Центральном банке), и вам нужно срочно его забрать за небольшое вознаграждение.

ВАШИ ДЕЙСТВИЯ

- Попросите звонящего представить доказательства того, что он действительно работает в данной организации, спросите его фамилию, имя, должность, внутренний телефон.
- Скажите, что вы перезвоните ему, и прекратите разговор.
- Зайдите на сайт названного учреждения, найдите номер горячей линии и опишите ситуацию.
- Ни в коем случае не торопитесь переводить деньги, а также не говорите данные своей банковской карты.
- Помните, что государственное учреждение может предоставить реквизиты для перевода (квитанцию на оплату) или предложить оплатить через Портал госуслуг (с обязательным наименованием «Назначение платежа»), но не будет требовать немедленного перевода денежных средств на карту.

ВОПРОСЫ ПО РЕЗУЛЬТАТАМ ЗАНЯТИЯ

1. Что такое мошенничество от имени государственных учреждений?

- Вид мошенничества, при котором злоумышленник, представляясь сотрудником государственного учреждения (пенсионного фонда, налоговой службы, полиции и других), похищает средства или имущество.
- Оплата государственных пошлин, налогов, штрафов через мобильное приложение банка.
- Предоставление пособий малоимущим слоям населения.

2. Таня — выпускница детского дома. Недавно ей позвонили из Центрального банка, ведь там на девушку оформлен именной сертификат на 500 тысяч рублей. Чтобы его получить, Таня должна оплатить комиссию за обслуживание в размере 15 тысяч рублей. Она в растерянности и просит вас дать ей совет, что делать:

- Оплатить комиссию и получить 500 тысяч рублей.
- Не рисковать. Предложить оплатить комиссию всего 5 тысяч рублей и получить меньшую компенсацию — например, 200 тысяч рублей.
- Ничего не платить, Центральный банк не работает с гражданами.

3. «Поздравляем, вы выиграли в лотерею! Это не розыгрыш, получите 100 тысяч рублей выигрыша!» — такое СМС прислали из Почты России, где вы покупали на днях лотерейный билет. Ваши действия.

- Позвоню на почту, уточню, правда ли это, так как я действительно покупал лотерейный билет.
- Это мошенники, удалю СМС.
- Перешлю данные банковской карты в обратном СМС.

4. Каковы ваши действия, если Министерство здравоохранения предлагает получить компенсацию за некачественные лекарства, купленные через интернет?

- Мне нужно получить мои деньги обратно! Передам звонящему данные моей карты.
- Такой компенсации не существует. Это попытки мошенников украсть информацию и деньги с моей карты.
- Я, конечно, не покупал никакие лекарства через интернет, но компенсацию получить готов. Сообщу свои данные.

5. Государственная компания предлагает удаленную работу через интернет. Вам не нужно сидеть в душном офисе. Работайте в любое удобное для вас время, получайте высокую заработную плату. Никаких вложений! Ваши действия.

- Очень интересное предложение! Я всегда мечтал о легкой работе с высоким заработком. Обязательно позвоню по объявлению, мне повезет!
- Предложение настораживает легким заработком. Найду на официальном сайте организации телефон горячей линии и уточню, есть ли на самом деле такая вакансия.
- Попробую позвонить по указанному в объявлении номеру, может, государственная компания действительно набирает людей таким образом.



Карточки к заданиям смотрите в сборнике демонстрационных материалов «Финансовое мошенничество. Как себя защитить»

СБОРНИК ДЕМОНСТРАЦИОННЫХ МАТЕРИАЛОВ

для проведения занятий по финансовой грамотности
в организациях для детей-сирот и детей, оставшихся
без попечения родителей

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Как себя защитить



Москва 2019



Банк России



Министерство просвещения
Российской Федерации



По вопросам финансовой грамотности:

fingramota@cbr.ru

Сайт Банка России по финансовой грамотности:

fincult.info

Контактный центр Банка России:

8 800 300-30-00

(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:

www.cbr.ru/reception