

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



Сборник демонстрационных материалов по теме «Финансовое мошенничество» является неотъемлемой частью сборника методических материалов по соответствующей теме и предназначен для проведения занятий по финансовой грамотности в организациях для детей-сирот и детей, оставшихся без попечения родителей.



Содержание

Демонстрационные материалы к разделу «Занятия для детей 11-15 лет»	3
---	---

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Ситуационные карточки «Финансовое мошенничество»	3
Вопросы по результатам занятия	9

КИБЕРМОШЕННИЧЕСТВО

Ситуационные карточки «Кибермошенничество»	11
Ситуационные карточки «Мошенничество по телефону»	21
Ситуационные карточки «Мошеннические СМС-сообщения и электронные письма»	23
Ситуационные карточки «Финансовое мошенничество в интернете»	33
Вопросы по результатам занятия	37

Демонстрационные материалы к разделу «Занятие для детей 16-18 лет»	39
---	----

МОШЕННИКИ, КОТОРЫЕ МАСКИРУЮТСЯ ПОД СОТРУДНИКОВ ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЙ:

Ситуационные карточки «Распознавание действий мошенников»	39
Вопросы по результатам занятия	47

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

СИТУАЦИЯ 1

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

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

СИТУАЦИЯ 2

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

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

СИТУАЦИЯ 3

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

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

СИТУАЦИЯ 4

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

. ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЭКСПЕРТ 1

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).

. ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЭКСПЕРТ 2

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, а также благодаря им сложнее подсмотреть ваш ПИН-код.

. ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЭКСПЕРТ 3

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, а также вы можете заблокировать карту через онлайн-банк.

. ФИНАНСОВОЕ МОШЕННИЧЕСТВО

ЭКСПЕРТ 4

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.

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 устройством.
- Не знаю, я никогда не прикрываю.



КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 1

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

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 2

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!»

ВАШИ ДЕЙСТВИЯ



КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 3

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

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 4

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

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 5

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

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 6

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



КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 7

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-ХХХ-ХХХ-ХХ-ХХ. Лиза».

ВАШИ ДЕЙСТВИЯ

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 8

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



КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 9

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

КИБЕРМОШЕННИЧЕСТВО

СИТУАЦИЯ 10

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

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ

СИТУАЦИЯ 1

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.

ЭКСПЕРТ 1

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.

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ

СИТУАЦИЯ 2

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 2

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.



МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 1

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

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 2

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!»

ВАШИ ДЕЙСТВИЯ

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 3

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

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 4

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 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



МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 5

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

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

СИТУАЦИЯ 6

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

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 1

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.

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 2

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

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 3

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.

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 4

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.

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 5

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.

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА

ЭКСПЕРТ 6

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.



ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

СИТУАЦИЯ 1

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

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

СИТУАЦИЯ 2

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

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

ЭКСПЕРТ 1

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.

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

ЭКСПЕРТ 2

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

Ответьте на вопросы, выбрав один из трех 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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 1

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 2

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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!

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 3

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 4

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 придет в назначенное место.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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!

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 5

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

СИТУАЦИЯ 6

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».

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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.

РАСПОЗНАВАНИЕ ДЕЙСТВИЙ МОШЕННИКОВ

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.



Ответьте на вопросы, выбрав один из трех вариантов ответа:

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.



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