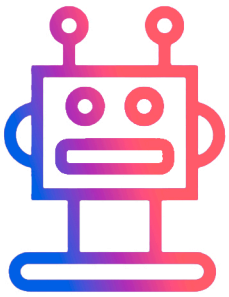
# КИБЕРДИКТАНТ.РФ

## ПО ФИНАНСОВОЙ IT-ГРАМОТНОСТИ

**Работа над ошибками**

**Для аудитории 12-17 лет**



Российская государственная детская библиотека

Банк России

Координационный центр доменов .RU/.РФ

РОЦИТ

Министерство культуры Российской Федерации

# Вопрос № 1

**Вредоносные программы – это:**

а) Антивирусные программы.

б) Программы, которые наносят вред данным и программам на компьютере. (правильный ответ)

в) Вирус, распространяющийся на человека.

г) Разновидность компьютерных игр.

*Зараженный компьютер может не только лишиться данных, но и заразить другие компьютеры. Вредоносные программы способны заставить зараженный компьютер выполнять любые команды злоумышленников, а также обеспечить доступ преступников ко всем данным пользователя.*

# Вопрос № 2

**Как выбрать надежный пароль?**

а) Использовать дату рождения одного из членов семьи.

б) Использовать в качестве пароля имя любимого исполнителя.

в) Придумать пароль, который состоит минимум из 8 символов и включает заглавные, строчные буквы, а также цифры и спецсимволы, например, знаки препинания. (правильный ответ)

г) Выбрать в качестве пароля адрес электронной почты.

*Специалисты в области информационной безопасности применяют именно такие требования к безопасности пароля. Также важно помнить, что даже сложный пароль нужно периодически менять.*

# Вопрос № 3

**Что такое фишинг?**

а) Вид интернет-мошенничества, цель которого – получить доступ к конфиденциальным данным пользователей. (правильный ответ)

б) Заражение компьютера или смартфона вирусом-вымогателем.

в) Создание фейковых (ложных) новостей.

г) Создание сайтов с пиратскими фильмами.

*Фишинг – это распространенный вид интернет-мошенничества, целью которого является кража конфиденциальных данных пользователей. Разнообразные фишинговые сайты завлекают жертв супервыгодными предложениями о продаже мобильной техники, услуг, недвижимости и т.д., чтобы ничего не подозревающие граждане оставили злоумышленникам свои контактные данные или данные своих банковских карт.*

# Вопрос № 4

**Что из перечисленного ниже <u>не является</u> угрозой заражения для компьютера?**

а) Переход по ссылкам в Интернете.

б) Вложения в электронной почте.

в) Использование карт памяти и флеш-накопителей.

г) Внезапное отключение электроэнергии. (правильный ответ)

*Переход по подозрительным ссылкам, скачивание вложений из писем от неизвестных отправителей, а также использование карт памяти и флеш-накопителей неизвестного происхождения несут потенциальную угрозу заражения компьютера вредоносным программным обеспечением.*

# Вопрос № 5

**Как защититься от кражи денег с банковской карты или свести потери к минимуму?**

а) Подключить СМС-информирование или всплывающие уведомления в мобильном приложении банка об операциях по карте. Это поможет быстро отреагировать, если злоумышленник спишет с твоей карты деньги.

б) Установить разовый и суточный лимит операций по банковской карте.

в) Никому не сообщать полные данные карты: срок действия, имя владельца, CVV/CVC-код на обратной стороне карты. Для перевода денег на карту достаточно знать только ее номер.

| г) Все варианты верные. (правильный ответ) |
|---|

*Современные банковские приложения позволяют быстро произвести необходимые настройки, которые связаны с информированием и лимитами. Не менее важным является сохранность данных, которые расположены на самой банковской карте: срок действия, имя владельца, CVV/CVC-код на обратной стороне карты.*

# Вопрос № 6

**Как мошенники могут украсть данные твоей карты?**

А) На игровом портале, когда тебе предлагают купить игровую валюту, амуницию, артефакты за реальные деньги.

б) На фишинговом сайте, который может выглядеть как близнец официального сайта банка, онлайн-магазина или другой организации.

в) Психологическими приемами («социальная инженерия»).

| г) Всеми вышеперечисленными способами. (правильный ответ) |
|---|

*Украсть данные возможно всеми указанными способами. Не все игровые порталы защищены, поэтому мошенники могут получить доступ к данным банковской карты. Нужно использовать только официальные сервисы, проверять информацию и быть внимательным. Фишинговые сайты также используются для получения доступа к конфиденциальным данным жертв. Социальная инженерия – еще один распространенный способ кражи данных, например, мошенник звонит, сообщает о «блокировке» банковской карты, а затем просит сообщить ее номер и CVV\CVC-код, чтобы «разблокировать».*

# Вопрос № 7

**Ты получил от друга в социальной сети сообщение с просьбой срочно перевести деньги на указанный номер банковской карты, потому что ему нужна помощь. Твои действия:**

а) Сразу же перечислю.

б) Вступлю в переписку, чтобы узнать, что произошло.

в) Позвоню другу и уточню, действительно ли что-то случилось. (правильный ответ)

г) Не буду ничего предпринимать, проигнорирую сообщение.

*Страницей друга мог завладеть злоумышленник и таким способом вымогать деньги у доверчивых друзей и знакомых. Лучше позвонить другу и удостовериться, что у него все хорошо.*

# Вопрос № 8

**Ты играешь в онлайн-игру, и вдруг всплывает окно с сообщением, что компьютер заражен и необходимо перейти по ссылке, чтобы установить программу для устранения вируса. Что будешь делать?**

а) Сразу же перейду по ссылке, компьютер нужно спасать от вирусов.

б) Закрою окно и проверю компьютер на наличие вирусов с помощью антивируса. (правильный ответ)

в) Отошлю друзьям ссылку на эту программу, пускай заранее защитят свои гаджеты.

г) Проигнорирую информацию и продолжу играть.

*Переход по такой ссылке может привести к заражению компьютера или мобильного телефона. Чтобы избежать риска заражения компьютера или мобильного телефона, необходимо установить антивирус и регулярно его обновлять.*

# Вопрос № 9

**Ты находишься в кафе и переписываешься с другом, вдруг мобильный Интернет закончился, а сообщение отправить ты не**

**успел. Ты решил подключиться к сети через открытую точку доступа WI-FI. Может ли что-то случиться, пока ты переписываешься с другом?**

а) Нет, открытая точка доступа – это безопасно.

б) Да, злоумышленники могут перехватить передаваемые данные и переписку. (правильный ответ)

в) Нет, но скорость соединения будет очень низкой.

г) Да, телефон выйдет из строя, и придется покупать новый.

*Открытые сети WI-FI не являются защищенными, их не рекомендуется использовать для оплаты через приложения банков или переписки в социальных сетях.*

# Вопрос № 10

**Друзья купили билеты на концерт любимой группы. Своей радостью они решили поделиться и выложили фотографии билетов в общем доступе в социальной сети. В день концерта оказалось, что билеты недействительны, и ребят не пропустили в зал. Почему так получилось?**

а) Должно быть, мошенничество. Злоумышленники могли воспользоваться наивностью друзей, которые выложили фото билетов в сеть, подделать их и заранее прийти на концерт. (правильный ответ)

б) Наверно перепутали день и место и пришли не на концерт, а на другое мероприятие. Внимательнее нужно быть!

в) Их не пустили, потому что билеты были оплачены онлайн.

г) Ребята купили билеты в последний день продажи.

*Такое действительно возможно. В сети необходимо быть осторожным и не выкладывать фотографии с документами или другие важные личные данные, например, номер домашнего телефона или домашний адрес.*

# Вопрос № 11

**Друг прислал тебе в социальной сети архив с фотографиями с праздника, где тебя не было, с предложением открыть его и**

**посмотреть, как здорово друзья провели время. Как ты поступишь?**

а) Не буду открывать. Вдруг там вредоносная программа, которая при открытии файла установится на мой гаджет? (правильный ответ)

б) Конечно, открою. Интересно же посмотреть, что за праздник был!

в) Перешлю файл всем друзьям, пусть тоже порадуются.

г) Вступлю в переписку, чтобы узнать, зачем мне прислали этот файл.

*Мошенники могли получить доступ к странице друга или знакомого и осуществить рассылку сообщений с вредоносным программным обеспечением. Существует множество менее подозрительных способов поделиться фотографиями с праздника.*

# Вопрос № 12

**Что необходимо сделать, если тебе пришло СМС или сообщение в социальной сети с информацией о неожиданном выигрыше и телефонным номером для обратной связи?**

а) Перезвонить по указанному номеру.

б) Удалить сообщение, так как это могут быть мошенники. (правильный ответ)

в) Попросить перезвонить родителей.

г) Вступить в переписку, чтобы узнать подробности.

*Это яркий пример социальной инженерии, еще одного часто используемого мошенниками способа выудить конфиденциальную информацию у жертвы. Таким образом злоумышленники побуждают жертв позвонить по указанному номеру. Подготовленный оператор попытается узнать данные банковской карты или навязать какую-нибудь услугу. Звонить по такому номеру не рекомендуется, лучше удалить сообщение.*

# Вопрос № 13

**Тебе очень хочется посмотреть фильм, но в кинотеатре он уже не идет. Ты решил поискать его в Интернете. На одном сайте фильм нашелся: здесь его можно скачать в один клик. Ты включаешь скачивание и ждешь загрузку, но вместо этого появляется сообщение с предложением ввести номер телефона, на который придет СМС с кодом подтверждения скачивания. Зачем нужна эта процедура?**

а) Администратор сайта должен удостовериться, что фильм скачивает не бот или злоумышленник, а человек, поэтому и необходимо ввести номер мобильного телефона, а затем код.

б) Номер телефона и подтверждение необходимы, чтобы получать информацию о новинках кино, которые появляются на сайте.

в) Это обман! После ввода подтверждающего кода будет оформлена платная подписка, и с вашего счета будут регулярно списываться деньги. (правильный ответ)

г) Номер телефона и подтверждение нужны, чтобы оставить на сайте свой отзыв о фильме.

*Часто недобросовестные владельцы подобных сервисов таким образом навязывают платные услуги или используют данные пользователей в корыстных целях.*

# Вопрос № 14

**Ты нашел любимую песню в сети, бесплатно скачал ее на компьютер и затем обнаружил, что это не музыкальный файл (например, «название-песни.mp3»), а архив (например, «название-песни.rar»). Твои действия?**

а) Открою файл. Какая разница какой формат?

б) Перешлю файл друзьям, пусть сначала откроют они.

в) Сначала проверю файл антивирусной программой, которую заранее обновлю. (правильный ответ)

г) Обращусь в поддержку сайта, чтобы мне прислали файл без архива.

*В архивах могут прятаться вирусы, поэтому лучше проверить антивирусом, а еще лучше не скачивать файлы из непроверенных источников.*

# Вопрос № 15

**В сети ты увидел заманчивое предложение - пройти простой тест, в котором надо ответить на несколько вопросов и получить за это денежное вознаграждение. В финале теста тебя просят ввести данные карты для получения вознаграждения. Как следует поступить?**

а) Введу данные карты, чтобы забрать положенное вознаграждение.

б) Введу только номер карты.

в) Не буду вводить данные! Так действуют мошенники! (правильный ответ)

г) Попробую найти контакты организаторов, чтобы получить приз наличными.

*Часто используемый способ обмана, не стоит посещать такие сайты. За подобными предложениями стоят злоумышленники, которые хотят заполучить данные банковской карты. Подобные сервисы также могут предложить оплатить комиссию за перечисление выигрыша или страховку, после чего обещают сразу отправить приз, но, разумеется, никаких денег и других призов ты не получишь.*