



Онлайн-квиз «Будь на чеку в сети!»

Защита от интернет- мошенничества

Узнай, как безопасно использовать интернет и избежать ловушек.

Что такое интернет-мошенничество?



Обман и вымогательство

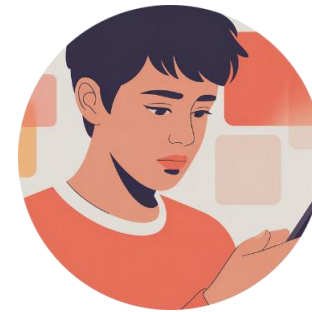
Интернет-мошенничество — это любое действие, направленное на обман пользователя с целью получения его денег или личных данных.

Мошенники используют различные уловки, чтобы заставить детей и подростков доверять им и раскрывать конфиденциальную информацию.



Фишинг: поддельные страницы

Фишинг является одной из самых распространенных форм мошенничества. Это поддельные веб-сайты и сообщения, которые выглядят как настоящие, например, страницы популярных игр, социальных сетей или интернет-магазинов. Цель фишинга — заставить пользователя ввести свои логины, пароли или данные банковских карт.



Манипуляции и шантаж

Мошенники могут использовать социальные сети и мессенджеры для вымогательства и манипуляций. Они могут угрожать раскрытием личной информации, распространением ложных слухов или шантажом, требуя деньги или выполнение определенных действий.

Реальные примеры мошенничества

1

«Помощь другу» или «выигрыш»

Дети часто получают сообщения от якобы друзей с просьбами о помощи или сообщения о выигрыше в лотерею. Это классическая ловушка: мошенники просят данные карты для «перевода выигрыша» или «срочной помощи».

2

Фальшивые игры и приложения

Множество игр и приложений обещают бесплатные бонусы или уникальные возможности. На самом деле, они созданы для кражи личных данных, паролей или даже заражения устройства вредоносным ПО.

3

Злоумышленники под видом друзей

Мошенники могут создавать фейковые аккаунты, выдавая себя за друзей или знакомых. Они входят в доверие, собирают информацию, а затем используют ее для шантажа или других мошеннических действий.

4

Приманка «бесплатным» контентом

Предложения бесплатной музыки, фильмов или программ часто скрывают вредоносные ссылки, которые ведут на фишинговые сайты или запускают загрузку вирусов.

Ответь на вопросы!

1

Почему дети часто получают сообщения от незнакомцев с просьбами о помощи или сообщениями о выигрыше в лотерею?

2

Если ты получишь сообщение от незнакомца с просьбой о помощи, как ты поступишь?

3

Как ты думаешь, что должны делать родители, чтобы защитить своих детей от мошенников в интернете?

4

Что может произойти, если ты отправишь свои данные или карты незнакомому человеку?

Прочитай следующие ситуации и определи, какие из них могут быть признаками интернет-мошенничества. Объясни, почему ты так думаешь.

Ситуация 1: Ты получаешь сообщение от незнакомого человека, который утверждает, что ты выиграл в лотерею, и просит отправить свои личные данные для получения приза.

Ситуация 2: Ты находишь в интернете сайт, который предлагает бесплатные игры, но для их загрузки нужно ввести номер телефона.

Ситуация 3: Ты получаешь письмо от "службы поддержки" известного магазина, в котором говорится, что твой аккаунт заблокирован, и нужно перейти по ссылке, чтобы его разблокировать.

Ситуация 4: Ты видишь рекламу, которая обещает "быстрые деньги" за выполнение простых заданий, но для начала нужно внести небольшую сумму.



Интернет-мошенничество — одна из главных угроз для детей в сети, требующая немедленного внимания и просвещения.

Как распознать мошенника?

- Проверь, кто пишет: всегда убеждайся в личности отправителя. Если незнакомец предлагает что-то слишком хорошее, чтобы быть правдой, это, скорее всего, ложь.
- Никогда не сообщай личные данные: никому, даже «друзьям» или «администрации», нельзя сообщать пароли, номера карт, домашний адрес или номер телефона.
- Осторожно с ссылками и вложениями: не переходи по подозрительным ссылкам и не открывай вложения в сообщениях от неизвестных отправителей.
- Обращай внимание на детали: грамматические ошибки, странный стиль общения или незнакомые домены в ссылках – верные признаки мошенничества.
- Помни о своей приватности: любая личная информация, опубликованная онлайн, может быть использована против тебя.



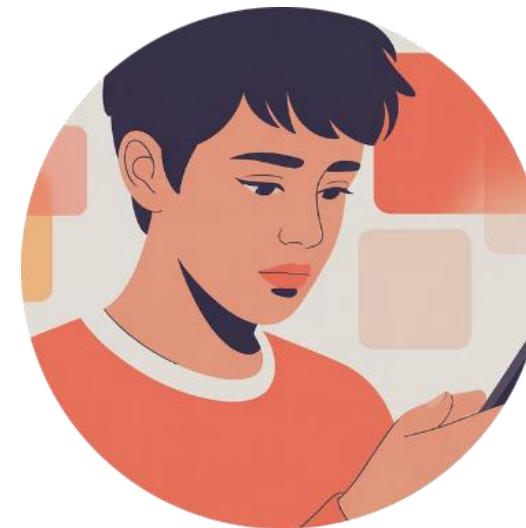
Давай проверим твои знания!

Какие личные данные нельзя указывать в социальных сетях?

- a) Имя и возраст
- b) Номер телефона и адрес проживания
- c) Любимый фильм и хобби
- d) Фотографии домашних питомцев

Что значит термин «цифровая гигиена»?

- a) Регулярная чистка компьютера от пыли
- b) Умение защищать персональные данные и ответственно пользоваться цифровыми ресурсами
- c) Установка антивирусных программ
- d) Ограничение экранного времени



Игровое задание: «Опасные сообщения»

Перед тобой несколько сообщений, которые ты можешь получить в сети.

Сообщение 1:

«Привет! Это твой друг. Мне срочно нужны деньги на новую игру. Можешь отправить 500 рублей на этот номер? Это мой новый аккаунт.»

Сообщение 2:

«Поздравляем! Ты выиграл новый смартфон! Перейди по ссылке, чтобы забрать приз: [подозрительная ссылка]»

Сообщение 3:

«Ваш аккаунт заблокирован. Чтобы разблокировать, введите свой пароль и логин здесь: [фишинговая ссылка]»

Определи, какие из этих сообщений – мошеннические. Выбери правильные действия для защиты себя и друзей.



Как правильно реагировать на негативные комментарии в интернете?

1.

Игнорировать и не вступать в конфликт.

2.

Отвечать грубо и резко.

3.

Сообщить администрации ресурса о нарушении.

4.

Варианты 1 и 3 правильные.



Будь начеку в сети!

Защищай себя и помогай друзьям

Интернет – это удивительный и полезный инструмент, если использовать его с умом и осторожностью.

- Учись распознавать угрозы: чем больше ты знаешь о мошенничестве, тем сложнее тебя обмануть.
- Действуй правильно: знай, что делать, если столкнулся с подозрительной ситуацией.
- Вместе мы сделаем сеть безопаснее: делись своими знаниями с друзьями и взрослыми, помогая им тоже быть начеку.

Твоя бдительность и ответственное поведение делают интернет безопаснее для всех!