Ситуационные задачи по кибермошенничеству для подростков

1. Фишинг в соцсетях

Ситуация: В «ВКонтакте» тебе пишет «друг», утверждает, что попал в беду (например, задержан полицией) и просит срочно перевести 50 рублей на номер телефона, чтобы его «отпустили».

Вопросы:

- Как проверить, действительно ли это твой друг?
- Какие действия предпринять, чтобы не стать жертвой мошенников?

Правильный ответ:

- Позвонить другу или связаться через другой канал (например, голосовой звонок).
- Не переводить деньги без подтверждения личности. Сообщить взрослым или в правоохранительные органы .

2. Фейковый выигрыш

Ситуация: На почту приходит письмо: «Поздравляем! Вы выиграли iPhone 15! Перейдите по ссылке и введите данные карты для получения приза».

Вопросы:

- Почему это мошенничество?
- Что делать с таким письмом?

Правильный ответ:

- Настоящие конкурсы не требуют данных карты. Это фишинг для кражи денег.
- Не переходить по ссылке, удалить письмо, проверить адрес отправителя (часто он не соответствует официальному домену компании).

3. Поддельный звонок из «банка»

Ситуация: Тебе звонит «сотрудник банка», говорит, что твоя карта взломана, и просит назвать код из SMS для «блокировки».

Вопросы:

- Почему нельзя называть код из SMS?
- Как проверить подлинность звонка?

Правильный ответ:

- Код из SMS — это доступ к деньгам. Банки никогда не спрашивают его по телефону.
- Прервать разговор, перезвонить в банк по официальному номеру с сайта или карты.

4. Взлом аккаунта через слабый пароль

Ситуация: У Ани пароль «Persik1234» (имя кота + цифры). Через 254 часа его взломали, и мошенники рассылают спам от ее имени.

Вопросы:
- Почему этот пароль ненадежный?
- Как создать надежный пароль?
Правильный ответ:
- Простые комбинации (имя + цифры) легко взломать брутфорсом.
- Использовать спецсимволы, заглавные/строчные буквы и случайные комбинации (например, «A!-7l9aj234» — взлом за 544 770 лет) .

5. Шантаж из-за личных фото

Ситуация: Незнакомец в Telegram пишет: «У меня твои фото из переписки. Заплати 100$, или я выложу их в сеть».
Вопросы:
- Почему нельзя платить?
- Куда обратиться за помощью?
Правильный ответ:
- Мошенники не удалят фото после оплаты, а потребуют еще.
- Сообщить родителям, заблокировать шантажиста, обратиться в киберполицию (например, в Отделение по противодействию киберпреступности) .

6. Поддельный Wi-Fi в кафе

Ситуация: В кафе есть открытая сеть «Free_Cafe_WiFi». После подключения начали приходить странные SMS с кодами.
Вопросы:
- В чем опасность публичных Wi-Fi?
- Как защититься?
Правильный ответ:
- Мошенники могут перехватывать данные (логины, пароли) через фальшивые точки доступа.
- Не подключаться к сомнительным сетям, использовать VPN или мобильный интернет.
Дополнительные рекомендации:
- Для занятий можно использовать интерактивные форматы: тесты на Kahoot (пример в), ролевые игры (например, «пользователь vs мошенник»).
- Разбирать реальные случаи из новостей (например, схемы с дипфейками или вишингом).
Эти задачи помогут подросткам распознать типичные схемы обмана и отработать алгоритмы безопасного поведения. Для большего эффекта сочетайте их с видеоразборами (например, ролики школьного TV) и гостевыми лекциями сотрудников МВД.