



Цифровая и телефонная безопасность

Сценарий

Возрастная группа: 8-9 классы

Цель проведения занятия

Формирование у учащихся представления о ключевых правилах осознанного и безопасного поведения при использовании компьютера и телефона путем развития критического мышления, умения распознать онлайн-угрозы, защищать личные данные

Задачи

Развивающие

- ✓ сформировать умение анализировать ситуации и принимать адекватные решения
- ✓ отработать умение формулировать правила и рекомендации для себя и других

Воспитательные

- ✓ помочь научиться вести себя вежливо и ответственно
- ✓ способствовать формированию привычки заботиться о своей и безопасности других

Образовательные

- ✓ познакомить с понятиями «цифровая гигиена», «фишинг», «дропперство»
- ✓ объяснить, какие действия могут быть опасными и почему

Планируемые результаты учащихся

Предметные

- ✓ освоить основные правила безопасного поведения
- ✓ узнать как действовать при той или иной угрозе

Метапредметные

- ✓ научиться распознавать признаки опасных ситуаций
- ✓ уметь применить правила безопасного поведения в реальных ситуациях

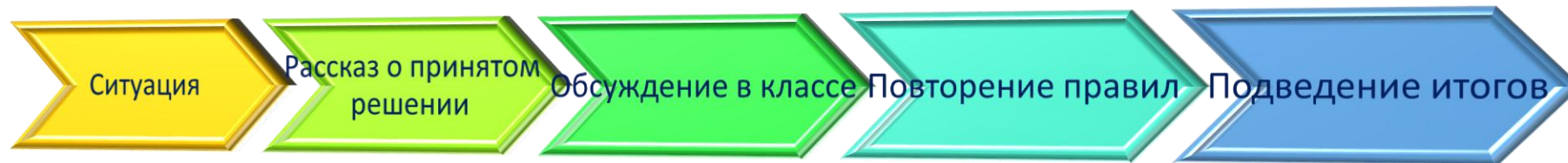
Личностные

- ✓ осознать свою ответственность за действия в интернете
- ✓ сформировать позитивное отношение к безопасному и уважительному онлайн-общению

Используемые методы и схема работы

Методы: беседа, интерактив

Схема проведения занятия



Примерная структура занятия

Этапы

- вступление (5 мин)
- просмотр видеоролика (3 мин)
- тематические блоки, мини-беседы (6 мин)
- игра «Правильно – неправильно» (8 мин)
- опрос (5 мин)
- заключение (3 мин)

Содержание

- знакомство с темой, мотивация на работу, просмотр видеоролика
- ситуации, задания, решения, обсуждение
- выводы, тест

Работа с заданиями

Использование интерактивных карточек [Учи.ру](https://uchi.ru)

- 1) Зайдите в личный кабинет на платформе;
- 2) Откройте по прямой ссылке или указанному пути адаптивную карточку;
- 3) Выведите ее на экран для демонстрации классу.

Также можно выдать задания в конце урока, чтобы учащиеся закрепили знания дома

Введение в тему

Обеспечение заинтересованности учащихся, вводные вопросы для привлечения и вовлечения

Решаемая задача

Способы подачи

Просмотр видеоролика и его обсуждение

«Чем вас привлекает интернет?», «Сталкивались ли вы или ваши знакомые с неприятностями при использовании интернета?»

Мотивация учащихся на ответы на вопросы, плюсы и минусы использования интернета

«Сколько времени вы проводите в интернете?» — выведение на доску статистики

«Мы все каждый день пользуемся интернетом. Но в нем, как и в жизни, есть правила, которые помогают нам быть в безопасности».
«Вы бы доверили ключи от своей квартиры незнакомцу? Почему же тогда многие рассказывают в интернете важные вещи?»

Переход по ссылке, где размещен видеоролик;
просмотр видеоролика;
Наводящие вопросы, мини-беседа по результатам просмотра видеоролика: «О чем видеоролик?», «Был ли он для вас интересен?», «На что вы бы хотели обратить внимание?», «Как вы думаете, о чем мы сегодня будем говорить?»

Разбор ситуаций

Блок 1. Фишинг и мошенничество

Необходимо научить учащихся распознавать фишинг (метод онлайн-мошенничества, при котором злоумышленники пытаются обмануть пользователей, заставляя их добровольно раскрыть конфиденциальную информацию, такую как пароли, номера банковских карт или личные данные)

Ситуации	Твой друг прислал сообщение с ссылкой на розыгрыш билетов на концерт любимой группы. После перехода по ссылке тебя попросили ввести пароль от аккаунта.
Вопросы	Почему нельзя вводить пароль? Что нужно сделать при виде такого сообщения?
«Правильно – неправильно»	Вы получили смс-сообщение с информацией о грандиозной скидке на товары популярного бренда электроники. Сообщение содержит ссылку, по которой нужно зарегистрироваться, введя свои контактные данные и банковскую карту. Ваши действия?

Задание на Учи.ру для закрепления (<https://distant.uchi.ru/page61091567html>)

Правило!

Не открывайте подозрительные письма и ссылки!
Будьте осторожны с сообщениями, содержащими требования передать личную информацию!

Блок 2.
Вредоносный
контент: вирусы и
защита

Необходимо помочь учащимся понять, что такое вредоносный контент и чем он опасен, способы распространения вирусов и методы защиты от них

Ситуации	Василий получил письмо от знакомого адреса, но содержание показалось странным. Письмо гласит: «Привет, посмотри прикольный ролик!» Далее идет прикрепленный файл с расширением .exe.
Вопросы	Можно ли запускать исполняемые файлы (.exe) из вложений писем? Как убедиться, что письмо реально отправлено знакомым человеком? Какой риск возникает при открытии файла .exe?
«Правильно – неправильно»	Катя увидела яркую баннерную рекламу, обещающую бесплатный iPhone. Чтобы поучаствовать в конкурсе, ей предложили заполнить анкету с персональными данными. Что нужно сделать Кате?

Задание на Учи.ру для закрепления

Правило!

Будьте внимательны ко вложениям и ссылкам во входящих письмах и сообщениях!

Будьте внимательны к источнику информации!

Разбор ситуаций

**Блок 3.
Безопасный
онлайн-шоппинг
и платежи**

Важно объяснить учащимся, почему необходимо соблюдать безопасность при покупках в интернете

Ситуации	Ольга решила купить подарок сестре на сайте интернет-магазина. Однако, заполнив корзину, она заметила, что оплата производится через стороннюю компанию с неясным названием
Вопросы	Является ли это поводом для беспокойства? Как убедиться, что компания законна и безопасна? Какие альтернативные варианты оплаты Ольга может рассмотреть?
«Правильно – неправильно»	Максим получил смс-сообщение с промокодом на скидку в крупном интернет-магазине. Но сам магазин он раньше не использовал и не подписывался на рассылки. Какие дальнейшие действия Максима?

Задание на Учи.ру для закрепления

Правило!
Используйте только официальные,
доверенные сервисы оплаты онлайн-
покупок!

**Блок 4. Цифровая
гигиена: защита
личных данных**

Необходимо научить учащихся защищать свою личность и личные данные в интернете

Ситуации	Анна разместила фотографию своего паспорта на странице социальной сети, отмеченную хэштегом #документы. Позже она узнала, что такая фотография стала доступной широкому кругу пользователей.
Вопросы	Какие последствия могут возникнуть после размещения документа в открытом доступе? Какие меры Анна должна предпринять немедленно? Как предотвратить повторение подобной ситуации?
«Правильно – неправильно»	Светлана опубликовала в социальной сети снимок с отметкой своего текущего местоположения. Ее подруга тут же написала комментарий: «Приходите быстрее домой, у вас открыт балкон». Какие дальнейшие действия Светланы?

Задание на Учи.ру для закрепления

Правило!

Создавайте сложные пароли! Включите двухфакторную аутентификацию! Минимизируйте публичный профиль и осмотрительно относитесь к социальным сетям!

Опрос

Закрепление материала и личные выводы учащихся

Проведение опроса по блокам

«Как отличить безопасный сайт от мошеннического?», «Сколько приватных данных открыто в вашем профиле соцсетей?», «Какие последствия могут возникнуть после размещения документа в открытом доступе?», «Почему опасно нажимать на ссылки из подозрительных писем?» и т.п.

Заключение

**Вопросы учителя,
адресованные учащимся**

**Вопросы учащихся учителю по
теме**

Обмен мнениями

Памятка учителю

Вступление

- вовлечение учащихся (метафора, вопрос, пример)
- выведение на обсуждение: в использовании компьютера и телефона есть и плюсы, и минусы

Тематические блоки

- № 1. Фишинг и мошенничество
- № 2. Вредоносный контент: вирусы и защита
- № 3. Безопасный онлайн-шоппинг и платежи
- № 4. Цифровая гигиена: защита личных данных

Заключение

- повторение правил
- проведение мини-тестов

Говорите простыми словами, адаптируйте примеры под возраст.

Используйте определенную структуру в каждом блоке:
ситуация → обсуждение → правило → задание.

Заканчивайте занятие позитивно: в интернете много полезного, это большие возможности, но нужно придерживаться правил

Желаем успехов!