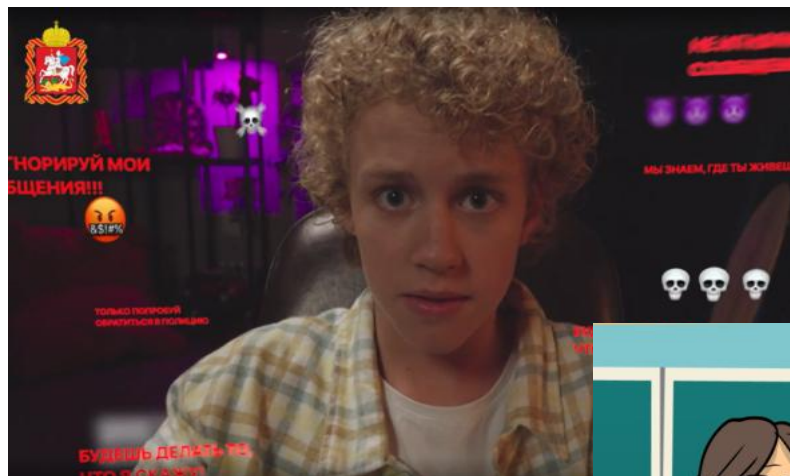




# Цифровая и телефонная безопасность

Возрастная группа: 8-9 классы

# О чем мы сегодня говорим?



<https://clck.ru/3NQYFY>



<https://clck.ru/3NQYJ5>

Отвечаем на вопросы:

О чем видеоролики?



Были ли они для вас интересны?



На что вы бы хотели обратить внимание?

Как вы думаете, о чем мы сегодня будем говорить?



# 1

## Фишинг и мошенничество

### Распознаем фишинг и мошенничество

#### Ситуации

Твой друг прислал сообщение с ссылкой на розыгрыш билетов на концерт любимой группы.  
После перехода по ссылке тебя попросили ввести пароль аккаунта

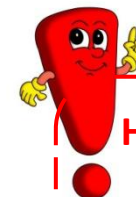
#### Вопросы

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?



**Не открывайте подозрительные письма и  
ссылки!**

**Будьте осторожны с сообщениями,  
содержащими требования передать личную  
информацию!**



## 2

### Вредоносный контент: вирусы и защита

#### Чем опасен вредоносный контент?

#### 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.

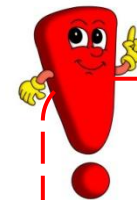
#### Вопросы

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?



**Будьте внимательны ко вложениям и  
ссылкам во входящих письмах и  
сообщениях! Будьте внимательны к  
источнику информации!**



# 3

**Безопасный  
онлайн-  
шоппинг и  
платежи**

**Почему важно 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?

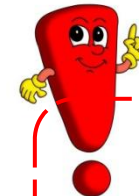
Как убедиться, что компания законна и безопасна?

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?



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



# 4

## Цифровая гигиена: защита личных данных

Защищаем 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

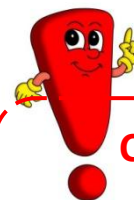
### Вопросы

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.



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

# Отвечаем на вопросы

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?

# Важно запомнить и соблюдать



Не вводить данные  
банковской карты на  
сомнительных сайтах



Не открывать письма с  
подозрительными  
вложениями



Не игнорировать  
настройки приватности



Не распространять  
контент неизвестного  
происхождения