

## Текст лекции к презентации на тему «Безопасные сайты – Как определить, что сайт безопасен»

### Слайд 1: Титульный слайд

Ребята, сегодня мы с вами отправимся в важное путешествие по просторам интернета! Но не просто так, а чтобы научиться отличать безопасные сайты от опасных. Представьте, что интернет - это большой город: здесь есть полезные места, как библиотеки и парки, но есть и темные переулки, куда лучше не ходить. Мы узнаем, как заметить опасность заранее, какие знаки подскажут, что сайту можно доверять, и что делать, если вы попали на подозрительную страницу. В конце урока вы станете настоящими экспертами по интернет-безопасности! Давайте начнем наше важное расследование.

### Слайд 2: Что такое безопасный сайт?

Безопасный сайт - это как надежный друг: он честен с вами, не просит того, чего не стоит давать, и точно не причинит вреда. Такие сайты создают добросовестные компании или организации для полезных целей: обучения, игр, общения. Они не содержат вирусов, не пытаются обмануть посетителей и не крадут личные данные. Опасные же сайты - как незнакомцы, предлагающие конфету: могут казаться привлекательными, но таят угрозу. Они могут заразить ваш гаджет вирусами, украсть ваши пароли или показать неприятный контент. Помните: если сайт вызывает у вас чувство тревоги или что-то в нем кажется странным - лучше сразу его закрыть.

### Слайд 3: Проверяем адрес сайта (<https://> и замок)

## Школьники в цифровом мире: **безопасность и познавательный интерес**

Давайте научимся проверять сайты как настоящие детективы! Первая подсказка - адресная строка. Видите в начале адреса 'https://' и маленький замок? Это как печать качества - значит, сайт защищен специальным шифрованием. Буква 's' в 'https' - от слова 'secure', то есть безопасный. А замок показывает, что ваши данные (например, пароль) нельзя перехватить. Если же стоит просто 'http://' без 's' и замка - будьте осторожны! Особенно когда нужно вводить личную информацию. Кстати, некоторые браузеры даже пишут Не защищено рядом с такими адресами - это серьезное предупреждение!

### Слайд 4: Опасные ссылки (как их распознать?)

Ох, сколько неприятностей могут принести эти коварные ссылки! Они маскируются под что-то интересное: Кликни, чтобы получить 1000 рублей!, Ты выиграл приз!, Только сегодня - бесплатно!. Но поверьте, ничего бесплатного в интернете не бывает. Такие сообщения - как конфеты с сюрпризом внутри, только сюрприз очень неприятный. Нажав на них, вы можете скачать вирус или попасть на страницу, которая украдет ваши данные. Особенно опасны ссылки в письмах от незнакомцев или всплывающие окна в играх. Правило простое: если предложение выглядит слишком хорошим, чтобы быть правдой - скорее всего, это обман. Лучший вариант - закрыть такое окно, даже не начиная читать.

### Слайд 5: Вирусы и вредоносные программы

Вирусы в компьютере - совсем как болезнь у человека: мешают работать, портят информацию и могут даже убить устройство. Они попадают к нам разными путями: через опасные сайты, скачанные файлы или даже флешки. Некоторые вирусы воруют пароли, другие показывают назойливую рекламу, третьи просто разрушают систему. Представьте, что все ваши фото, сохраненные игры или проекты могут исчезнуть в один момент! Как защититься? Во-первых, не качайте файлы с подозрительных сайтов. Во-вторых, используйте антивирус -

# Школьники в цифровом мире: **безопасность и познавательный интерес**

это как прививка для компьютера. И главное - будьте внимательны к тому, куда нажимаете в интернете.

## Слайд 6: Фишинговые сайты (поддельные страницы)

Фишинг - это когда мошенники создают точную копию известного сайта, например, страницы ВКонтакте или онлайн-игры, чтобы украсть ваши данные. Они могут прислать ссылку якобы для восстановления пароля или получения бонуса. Различить подделку можно по адресу: вместо vk.com будет что-то вроде vk-id123.ru. Также обратите внимание на дизайн - на фальшивых сайтах часто кривые логотипы, плохие картинки. Если вы уже ввели пароль на таком сайте - срочно поменяйте его на настоящем сайте и скажите взрослым. Помните: настоящие сервисы никогда не просят прислать пароль в сообщении или письме!

## Слайд 7: Как проверить сайт перед входом?

Давайте выработаем полезную привычку - быструю проверку сайта. Первое - смотрим на адрес: он должен быть знакомым, без лишних символов. Например, сайт школы должен заканчиваться на .edu или .gov. Второе - оцениваем внешний вид: много ли всплывающих окон, навязчивой рекламы, странных картинок? Третье - читаем предупреждения браузера: если он пишет Опасный сайт - значит, его уже ловили на вредоносной активности. Еще можно поискать отзывы о сайте в интернете. И никогда не игнорируйте свою интуицию - если что-то кажется подозрительным, даже если вы не можете объяснить почему, лучше перестраховаться.

## Слайд 8: Опасные баннеры и реклама

Эти яркие мигающие баннеры с надписями Выбери приз! или Твой компьютер заражен! созданы специально, чтобы привлечь внимание. Они используют психологические уловки: ограничение времени (Осталось 10 секунд!), мнимую бесплатность, угрозы. На

## Школьники в цифровом мире: **безопасность и познавательный интерес**

самом деле, никаких проверок системы они не делают, а кнопка **Закреть** часто ведет... на ту же рекламу! Настоящие антивирусы так не работают. Что делать? Воспользуйтесь сочетанием клавиш **Alt+F4**, чтобы закрыть окно, или вообще выключите браузер через диспетчер задач (**Ctrl+Shift+Esc**). А лучше - установите блокировщик рекламы, который будет фильтровать такие баннеры.

### Слайд 9: Что делать, если попал на опасный сайт?

Если вы поняли, что зашли на опасный сайт, главное - не паниковать! Первым делом закройте вкладку. Если окно не закрывается - закройте весь браузер. Ничего не скачивайте и тем более не вводите никакие данные. После этого расскажите о ситуации взрослым - они помогут проверить компьютер антивирусом. Если вы успели что-то ввести (например, пароль) - немедленно поменяйте его на настоящем сайте. Хорошая привычка - очищать историю браузера и кэш после таких случаев. И помните: даже опытные пользователи иногда попадают на опасные сайты, поэтому не стесняйтесь просить помощи!

### Слайд 10: Итоги - правила безопасности

Давайте повторим главные правила интернет-безопасности, которые стоит запомнить как таблицу умножения:

1. Всегда проверяйте адрес сайта - ищите **https://** и замок.
2. Никогда не переходите по подозрительным ссылкам, даже от друзей (их аккаунт могли взломать).
3. Не скачивайте файлы с неизвестных сайтов.
4. Используйте сложные пароли и никому их не сообщайте.
5. Рассказывайте взрослым о любых странностях в интернете.

Заведите привычку - прежде чем что-то кликнуть, спросите себя: А точно ли это безопасно? Всего пять простых правил помогут вам избежать 99% проблем в сети!

# Школьники в цифровом мире: **безопасность и познавательный интерес**

---



ПРОЕКТ  
**ЦЕНТРА  
КОМПЬЮТЕРНОГО  
ОБУЧЕНИЯ «ТУРБО»**



ПРИ ПОДДЕРЖКЕ  
**ГРАНТОВ  
РЕСПУБЛИКИ  
АДЫГЕЯ**