Участвуйте безопасно и ответственно онлайн

26 минут

В этом пути обучения, вы будете введены в опасности безопасности вы можете столкнуться при использовании Интернета. Вы узнаете об онлайн-мошенничестве и о том, как их избежать. Вы также узнаете о рекомендациях по обмену информацией в Интернете. Кроме того, вы познакомитесь с киберзапугиванием.

# Безопасность и конфиденциальность в Интернете

17 минут 8 единиц

В этом модуле вы узнаете о некоторых рисках безопасности, которые могут повлиять на вас при использовании Интернета, и советы для обеспечения безопасности и сохранения конфиденциальности вашей информации в Интернете.

## Защитите себя от фишинга

3 минуты

### Защитите себя от фишинга

Хотя Есть много положительных вещей, которые мы можем сделать в Интернете, мы всегда должны быть осведомлены о рисках безопасности. Есть много мошенников, которые онлайн-хищники используют для доступа к информации людей в Интернете.

Вы должны быть в курсе этих мошенников, так что вы можете сделать все возможное, чтобы избежать их. **Фишинг**  является общей онлайн-мошенничества, что вы должны быть в курсе.

**Смотреть следующее видео, чтобы узнать больше о фишинг и как защитить себя от этой онлайн-мошенничества.**

### Видео: Защитите себя от фишинга

Интернет обеспечивает нам множество возможностей. Мы можем общаться с людьми, делать покупки онлайн и вести свой бизнес из одного места. Но такое онлайн-взаимодействие не всегда безопасно. Давайте поговорим о распространенных способах мошенничества в Интернете, о которых вам следует знать. Обычно чтобы поймать рыбу, на крючок вешают наживку, которую рыба хочет съесть. Когда рыба кусает наживку, она попадает на крючок. Принцип интернет-мошенничества, называемого «фишингом» (по-английски «рыбалка), такой же самый. Люди, которые хотят украсть вашу информацию, подобны рыбакам. Они отправляют вам электронное письмо или мгновенное сообщение через сайт социальной сети или онлайн-игру. Они часто выдают себя за тех, кем не являются, и запрашивают у вас личную информацию или просят нажать гиперссылку, чтобы вы могли завершить важное дело. Если вы предоставите им эту информацию или нажмете гиперссылку, вы попадете на крючок. Но не волнуйтесь. Я дам вам четыре совета, которые помогут вам защититься от фишинг-мошенничества. Совет номер один: будьте осторожны с подозрительными сообщениями. Чтобы войти к вам в доверие, мошенники придают своим сообщениям официальный и узнаваемый вид. Если вы получили подозрительное сообщение, подумайте дважды и не предоставляйте личную информацию в сообщении или электронном письме. К такой информации относится домашний адрес, банковская информация, пароли и прочее. Не нажимайте ссылку и не загружайте файл, если вы не знаете отправителя или не доверяете ему. Совет номер два: ищите признаки того, что веб-страница является безопасной. Прежде чем предоставлять информацию о кредитной карте, вводить пароль или отправлять другую личную информацию, убедитесь, что вы находитесь на надежном и безопасном веб-сайте. Большинство безопасных веб-сайтов имеют префикс https перед URL-адресом в адресной строке веб-браузера. Также убедитесь, что вы находитесь на нужной вам веб-странице. Мошенники часто пытаются заманить вас на веб-страницы, которые кажутся официальными, но содержат ошибку в названии компании, чтобы вас обмануть. [www.microsoft.net](http://www.microsoft.net) — не то же самое, что официальный веб-сайт корпорации Microsoft по адресу [www.microsoft.com](http://www.microsoft.com). Всегда проверяйте URL-адрес, чтобы убедиться, что вы находитесь на нужной вам веб-странице. Совет номер три: регулярно обновляйте веб-браузер и операционную систему. Вы можете включить автоматические обновления, чтобы обеспечить автоматическую установку последних версий программного обеспечения на свой компьютер. Регулярные обновления программного обеспечения устройства обеспечат получение последних обновлений безопасности, которые помогут защитить ваш компьютер. Совет номер четыре: установите на своих устройствах проверенное антивредоносное программное обеспечение. Это специальное программное обеспечение, предназначенное для защиты компьютера от вредных программ и хакеров. Не будьте следующей рыбой, которая попадется на крючок. Используя Интернет, Используя Интернет, всегда думайте перед тем, как что-либо нажимать, загружать или предоставлять информацию. Так вы защитите себя от онлайн-фишинга.

## Безопасное общение в Интернете

2 минуты

### Безопасное общение в Интернете

Интернет позволяет нам общаться с другими людьми по-новому. Тем не менее, это не всегда безопасно общаться с другими людьми в Интернете. Вы не всегда знаете наверняка, кто вы говорите, когда вы находитесь в Интернете, так что вы должны быть осторожны, чтобы оставаться в безопасности.

**Посмотрите следующее видео, чтобы научиться безопасно общаться в Интернете.**

### Видео: Общайтесь безопасно онлайн

Интернет обеспечивает новые способы общения с людьми по всему миру. Он дает множество преимуществ, но есть и некоторые опасности. Существуют онлайн-злодеи, которые каждый день используют Интернет в своих целях. Они часто притворяются теми, кем не являются. Поэтому вам может быть сложно понять, кто общается с вами по ту сторону экрана. Вот три совета, которые помогут вам обезопасить себя от онлайн-злодеев при общении в Интернете. Совет номер один: прислушивайтесь к своей интуиции. Если кто-то заставляет вас нервничать или чувствовать себя неловко, прекратите общение с этим человеком и сразу же расскажите о ситуации тому, кому вы доверяете. Большинство веб-сайтов и сайтов социальных сетей предлагают инструменты для уведомления о подозрительной активности. Совет номер два: ограничьте информацию, которую вы предоставляете в Интернете. Онлайн-злодеи часто пытаются заставить вас отправить им вашу личную информацию в электронных письмах или сообщениях. Не делитесь своей личной информацией с онлайн-незнакомцами. Совет номер три: держите дистанцию. Подумайте дважды перед тем, как отправляться на встречу с кем-то, с кем вы общались только в Интернете. Онлайн-злодеи часто используют социальные сети, чтобы выдавать себя за других людей. Они создают фальшивые профили с чужими фотографиями. Даже если кто-то кажется дружелюбным, может быть сложно определить, кто же говорит с вами на самом деле. Всегда сообщайте родителям или кому-то, кому доверяете, если онлайн-незнакомец просит вас о личной встрече. Так вы избежите опасной ситуации. Многие онлайн-злодеи используют хитрые тактики, чтобы заманить вас и подвергнуть опасности, но вы можете быть умнее. Помните про эти риски и советы, чтобы обезопасить себя при общении в Интернете.

## Создание надежных паролей

2 минуты

### Создание надежных паролей

Большая часть безопасности и конфиденциальности вашей информации в Интернете защищает вашу информацию, ваши учетные записи и компьютер с помощью надежных паролей.

**Посмотрите следующее видео, чтобы узнать, как создавать надежные и эффективные пароли, которые могут защитить вашу информацию.**

### Видео: Создание надежных паролей

Пароли помогают защитить вашу личную информацию и учетные записи от других людей. Пароль так же важен, как замок на двери. Вы предпочитаете иметь прочный замок, который трудно взломать и который не даст опасным людям проникнуть в ваш дом. Вы также не хотите, чтобы кто-нибудь нашел ключи от вашего замка. Надежный пароль похож на прочный замок от вашей учетной записи. Он должен быть таким, чтобы его сложно было отгадать. Он также должен храниться в надежном месте, чтобы его не нашли другие люди. Следуйте этим советам, чтобы создать надежные пароли и обеспечить их безопасность. Совет номер один: пароль должен быть комбинацией букв, цифр и символов. Использование комбинации букв верхнего и нижнего регистра, символов и цифр может повысить надежность пароля. Совет номер два: избегайте использования в пароле общераспространенных слов, например слов «пароль» и «веб-сайт», также не используйте личные ключевые слова, например дату вашего рождения, ваше имя или родной город. Хакеры могут легко угадать пароль с этими словами. Уникальное сочетание символов и цифр обеспечивает более надежный пароль. Совет номер три: используйте разные пароли для разных учетных записей. Если кто-то угадает пароль от вашей электронной почты и тот же пароль используется для банковского счета, ваша безопасность и конфиденциальность окажутся под угрозой. Поэтому используйте разные пароли для всех своих учетных записей онлайн. Совет номер четыре: ваш пароль предназначен только для вас. Если вы сообщаете его другим людям, даже друзьями или семье, повышается вероятность того, что им воспользуется кто-то еще и безопасность будет нарушена. Не сообщайте никому свои пароли. Всегда выходите из учетных записей по окончанию работы и не сохраняйте информацию для входа на общедоступном компьютере. Кроме того, постарайтесь не заниматься личными делами на общедоступных компьютерах и в общественных сетях. Это облегчает хакерам доступ к вашей информации. Помните, когда вы используете надежные пароли и надежно их храните, вы заботитесь о своей безопасности и конфиденциальности в Интернете. Не забудьте про эти советы, когда будете создавать новый пароль.

## Опишите лучшие практики для обмена информацией в Интернете

2 минуты

### Будьте умны, когда вы разделяете

Когда мы выходим в Интернет, мы часто можем делать много вещей, которые угрожают нашей безопасности, не думая много об этом. Важно дважды подумать о том, что вы разделяете в Интернете, и иметь в виду вашу безопасность.

**Смотреть следующее видео, чтобы узнать больше о рисках совместного использования в Интернете.**

### Видео: Oversharing онлайн

Интернет и Всемирная паутина позволяют нам оставаться на связи с друзьями и семьей из разных уголков мира. Мы можем использовать социальные сети и другие платформы, чтобы наблюдать за тем, что происходит в жизни наших друзей, делиться личными новостями и поддерживать социальные связи. Однако предоставление информации о себе в Интернете не всегда безопасно. Рассмотрим следующий сценарий. У Гарольда новая машина, и он хочет показать ее своим друзьям. Поэтому он публикует фотографию машины в социальных сетях. Можно подумать, что все нормально, но на фотографии много личной информации о Гарольде. Любой может увидеть его номерной знак, какой у него автомобиль и где он живет. Вполне нормально, если это видят друзья, и опасно, если человек, который получит эту информацию, захочет использовать ее со злым умыслом. Публикуя информацию в Интернете, важно помнить о конфиденциальности и безопасности. Настраивая профили на веб-сайтах социальных сетей, не забудьте просмотреть настройки конфиденциальности своей учетной записи. Если ваша учетная запись общедоступная, любой человек может видеть вашу информацию и то, чем вы делитесь. Рекомендуем делать учетные записи частными, чтобы то, чем вы делитесь, было видно только вашим личным контактам. Также будьте избирательными, когда принимаете приглашения в друзья через социальные сети. Большинство платформ социальных сетей позволяют принимать и отклонять запросы от потенциальных друзей или подписчиков. Как только вы принимаете запрос от человека, вы открываете ему прямой доступ к вашему профилю и информации, которой вы делитесь. Имейте это в виду, когда получаете запрос, и убедитесь, что взаимодействуете только с теми люди, которых знаете и которым доверяете. Даже если вы контролируете, кто имеет доступ к вашим профилям и учетным записям, вы не можете контролировать то, что они делают с вашей информацией. Поделившись чем-нибудь в Интернете, вы не сможете это стереть. Никогда не выкладывайте онлайн то, что вы бы не хотели показывать незнакомцам и общественности. Всегда подумайте, прежде чем делиться чем-нибудь в Интернете. Помните про свою безопасность и принимайте взвешенные решения относительно своих онлайн-публикаций.

### Попробуйте сами

Что вы узнали из этого видео? Запишите 1-3 вещи, которые вы будете иметь в виду, когда вы делитесь личной информацией в Интернете.

## Опишите важность управления цифровым следом

3 минуты

### Ваш цифровой след

Мы можем многое сделать в Интернете, от просмотра веб-страниц до обмена обновлениями в социальных сетях, до совершения покупок в Интернете. Вы должны иметь в виду, что все, что вы делаете в Интернете становится частью вашей истории онлайн, или ваш **цифровой след**.

Вы должны думать о своем цифровом следе, когда вы делитесь информацией или делаете вещи в Интернете, потому что вещи, которые происходят в Интернете, трудно стереть.

**Посмотрите следующее видео, чтобы узнать больше о вашем цифровом следе и о том, как им управлять.**

### Видео: Управление цифровой след

Если вы используете Интернет, то должны знать, что оставляете цифровой след. Подобно физическим следам, которые остаются, когда кто-то проходит по грязной дороге, ваш цифровой след — это история всей вашей активности в Интернете. Любые ваши публикации в социальных сетях, любые веб-сайты, которые вы посещаете, и любая информация, которой вы делитесь онлайн — все это формирует ваш цифровой след. Как только вы опубликовали что-то в Интернете, это уже нельзя стереть. Поэтому ваш цифровой след может быть вечным. Хорошо, если ваш цифровой след обеспечивает вам положительную репутацию в Интернете. В этом случае он может помочь вам строить ваш личный бренд. Ваша онлайн-история также помогает приложениям, которые вы используете, лучше узнавать вас. Они могут использовать эту информацию для повышения качества предоставляемых вам услуг посредством адаптации под ваши предпочтения и ежедневные привычки. Но они также могут использовать эту информацию неправильно и делиться ей с другими людьми. Следующие советы помогут вам управлять своим цифровым следом в Интернете. Совет номер один: знайте, что говорит о вас ваш цифровой след. Люди могут судить о вас по вашему цифровому следу. Например, это могут делать работодатели, когда вы пытаетесь устроиться на работу, или члены отборочной комиссии, когда вы подаете заявку на участие в академических программах. Важно понимать, что говорит о вас ваш цифровой след и как используется ваша информация. Чтобы узнать, что представляет собой ваш личный бренд в Интернете, можно поискать информацию о себе. Введите свое имя в поисковой системе Bing и посмотрите, какие результаты отобразятся. Если эти результаты отличаются от того, что вы желаете видеть, подумайте, чем вы делитесь в Интернете и какую информацию позволяете видеть другим людям. Совет номер два: настройте свои параметры конфиденциальности. Вы можете изменить параметры конфиденциальности в большинстве социальных сетей и онлайн-приложений, которые используете. Так вы сможете контролировать, кто видит, чем вы делитесь, и какая информация появляется, когда кто-то ищет вас в Интернете. Совет номер три: управляйте своими файлами cookie. Файлы cookie — это примечания, которые получает ваш веб-браузер, когда вы заходите на веб-страницы. Эти файлы cookie помогают приложениям отслеживать информацию, связанную с использованием вами приложения. Она помогает приложению улучшать ваш пользовательский опыт. Однако эти данные также оставляют ваш цифровой след. В настройках браузера можно ограничить или блокировать использование файлов cookie на некоторых веб-сайтах. Совет номер четыре: подумайте перед тем, как делиться какой-либо информацией. Как только вы поделились чем-то в Интернете, это уже нельзя удалить. Убедитесь, что вы нормально относитесь к тому, что информация, которую вы собираетесь опубликовать, станет частью вашего публичного цифрового следа, и только потом публикуйте. Ваш цифровой след может быть вечным. Пользуйтесь этими советами, и вы будете довольны своим цифровым следом и его использованием.

Проверка знаний

3 минуты

1. Какой из следующих компонентов вы должны искать в URL веб-страницы, чтобы убедиться, что вы находитесь на безопасном сайте?

* http
* Безопасный
* **https - Правильно! "https" означает, что веб-страница является безопасной.**
* Ssh

1. Какой из этих паролей является самым сильным?

* **John@453 - Правильно! Этот пароль содержит верхний регистр, нижний регистр, специальный символ и номера.**
* john500
* JoHn300
* 125893

1. Ваш цифровой след:

* Размер информации в ваших онлайн-аккаунтах.
* Количество людей, к которых вы подключены в Интернете.
* **Запись всего, что вы делаете и говорите в Интернете. - Правильно! Цифровой след позволяет легко отслеживать ваши действия в Интернете.**
* Ваше имя пользователя в Интернете.
* r с использованием надежных паролей.

## Сводка

1 минута

Поздравляю!

Вы завершили модуль безопасности и конфиденциальности в Интернете и теперь можете ответить на следующие вопросы самостоятельно:

1. Каковы некоторые опасности использования Интернета и Интернета?
2. Каковы некоторые признаки риска для безопасности и мошенничества в Интернете?
3. Какие шаги вы можете предпринять, чтобы оставаться в безопасности при использовании Интернета?
4. Как вы можете управлять своим цифровым следом?

**следующее видео,** чтобы узнать, как создать сильные, эффективные пароли, которые

# Онлайн вежливость

9 минут 5 единиц

В этом модуле вы узнаете больше о правах и рекомендациях по использованию информации в Интернете. Вы также узнаете о киберзапугивания.

Введение

1 минута

Мы можем использовать Интернет для доступа к большому количеству информации и общаться с другими, но мы должны убедиться, что мы веем себя как ответственные цифровые граждане.

В этом уроке, вы узнаете, как ответственно использовать Интернет и Интернет.

**К концу этого урока вы сможете:**

1. Опишите права, которые люди имеют на информацию и контент, распространяемый в Интернете.
2. Опишите лучшие практики использования информации, найденной в Интернете.
3. Опишите последствия плохого отношения к другим людям в Интернете.
4. **защитить вашу информацию.**

## Опишите лучшие практики использования информации, найденной в Интернете

2 минуты

### Ответственно используйте информацию

Хотя доступ к информации легко в цифровом мире, Есть некоторые правила, чтобы иметь в виду, когда вы хотите использовать информацию, вы найдете в Интернете.

**Посмотрите следующее видео, чтобы узнать некоторые рекомендации по использованию информации, которую вы найдете в Интернете.**

### Видео: Используйте информацию ответственно

Интернет дает нам неограниченное количество информации и возможностей. Мы можем найти все: от смешных видео до любимых песен и подсказок, как решить домашнее задание, но мы должны ответственно подходить к информации, которую находим в Интернете. Давайте рассмотрим такой сценарий. Гарольд хочет написать поваренную книгу и продавать ее в онлайн-магазинах. Он не умеет фотографировать, поэтому ищет фотографии в Интернете. Он загружает изображения различных блюд и включает их в свою книгу. Такое поведение может показаться нормальным, ведь это очень просто сделать, но оно не является честным и ответственным способом использования информации из Интернета. Когда кто-то публикует свою оригинальную работу онлайн, включая тексты, изображения, видео, музыку и прочее, он становится владельцем этой работы. Как владелец он имеет определенные права, которые обычно называются авторскими правами. Эти права позволяют решать, как можно использовать данное содержимое. Если вы используете чужие тексты или работы как свои собственные, это считается плагиатом. Это нечестно по отношению к автору и может доставить вам неприятности. Если вы хотите использовать чью-то работу в своей работе, не забудьте сослаться на автора этой работы. Чтобы использовать чью-то работу в продукте, который вы будете продавать, сначала нужно получить разрешение от автора работы. Возможно, вам также придется заплатить за лицензию на использование этой работы. Иногда авторы работ позволяют использовать их бесплатно. В поисковых системах, например в Bing, можно искать изображения, файлы мультимедиа и другие типы содержимого, которое доступно для бесплатного использования. Если вы используете информацию из Интернета, убедитесь, что поступаете честно и ответственно.

## Опишите последствия плохого отношения к другим в Интернете

3 минуты

### Киберзапугивание

Интернет позволяет нам общаться с другими онлайн со всего мира. К сожалению, люди не всегда относятся друг к другу красиво в Интернете.

**Киберзапугивание** является одним из видов издевательств, что происходит через Интернет. Это может быть легко отправить средние сообщения или распространять негативные слухи о других людях, но это может быть опасно для человека, который является мишенью.

**Смотреть следующее видео, чтобы узнать советы по предотвращению киберзапугивания и быть цифровым гражданином.**

### Видео: Относитесь к другим с уважением онлайн

### Интернет и социальные сети обеспечивают новые способы поддерживать связь с друзьями, семьей и коллегами. Иногда люди используют эти платформы для распространения негативной информации о других пользователях.

### Кибербуллинг, или травля в Интернете, это так же плохо, как и травля в обычной жизни. В Интернете люди могут отправлять злые сообщения, распространять неправдивые слухи и выкладывать чью-то личную информацию без разрешения. Когда кто-то становится объектом кибербуллинга, его чувства могут быть задеты, а репутация испорчена. Вы не всегда можете предотвратить кибербуллинг, но вы можете помочь сделать Интернет более дружелюбной и безопасной средой для каждого.

### Далее несколько советов, которые можно использовать для продвижения цифровой культуры. Живите по золотому правилу:

* относитесь к другим так, как вы хотите, чтобы относились к вам. Это применимо как в личном взаимодействии, так и в Интернете.
* Воздержитесь от отправки негативных сообщений и участия в действиях, которые могут кого-то ранить.
* Уважайте различия. Мы все разные во многих аспектах. Взаимодействуя с людьми в Интернете, уважайте различия в мнениях, опыте и культуре. Даже если вы не согласны с чем-то, чем другой человек делится онлайн, вы все равно должны относиться к нему с уважением и стараться сделать Интернет дружественным пространством для общения. Сделайте паузу перед ответом.
* Перед тем, как поделиться чем-нибудь в Интернете, всегда остановитесь и подумайте о последствиях. Может ли ваше сообщение причинить боль кому-нибудь? Повредит ли это вашей репутации, или безопасности или репутации других людей?
* Подумайте дважды, прежде чем публиковать что-либо онлайн. Защищайте себя и других. Если вы не чувствуете себя в безопасности в Интернете, вы можете спокойно покинуть ситуацию и сообщить об этом кому-то, кому вы доверяете.
* Если вы наблюдаете жестокие или опасные действия в Интернете, предложите поддержку тем, на кого они направлены, и сообщите об инциденте тому, кому доверяете. Вместе мы можем сделать Интернет безопасным и дружественным местом для каждого человека.
* Внесите свой вклад, ведите себя онлайн как ответственный цифровой гражданин.

## Проверка знаний

2 минуты

1. Какое из этих действий не нарушает авторских прав?

* Использование чьих-то изображений в книге, которую вы публикуете без ихразрешения.
* **Цитируя абзац из чьей-то книги и ссылки на них - Правильно! Вы соблюдаете авторские права, когда ссылаетесь на владельца.**
* Продажа чьего-то видео под вашимименем.
* Продажа чьей-то книги безлицензии.

1. Киберзапугивание может иметь место:

* Только на социальных медиа-платформах.
* Только через электронную почту.
* Только по SMS.
* **На платформах социальных сетей и SMS, а также через электронную почту. - Правильно! Киберзапугивание может иметь место в любом типе онлайн-коммуникаций.**

## Сводка

1 минута

Поздравляю!

Вы завершили модуль онлайн-вежливости и теперь можете ответить на следующие вопросы самостоятельно:

1. Что делать, если вы хотите использовать информацию, которую вы найдете в Интернете?
2. Что вы можете сделать, чтобы предотвратить или положить конец киберзапугивания?

# Печать сертификата

2 минуты 2 единицы

Вы должны заполнить все модули в этом курсе, чтобы получить сертификат.

## Получение кредита

1 минута

### Полный

Поздравляем с завершением Участие безопасно и ответственно онлайн. Выберите **Получить кредит,** чтобы пройти курс и получить сертификат.

### Кредит получен

Поздравляем с завершением Участие безопасно и ответственно онлайн.

В поле ниже, пожалуйста, введите свое имя, как вы хотите, чтобы он появился на сертификате, а затем выберите **Сертификат Просмотра.**