**Безопасность в сети Интернет**

С каждым годом молодежи в интернете становиться больше, и как правило это одна из категорий самых активных пользователей Рунета.

Социальные сети — это один из самых востребованных ресурсов Интернета. Благодаря им  сделан огромный шаг вперёд в деле [информатизации](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.kv.by%2Fpost%2F1050286-obzor-zakonodatelstva-respubliki-belarus-v-sfere-informatizacii-za-dekabr-2016-goda) общества. Это настоящий подарок для любителей интерактивного общения. Казалось бы, чем можно навредить человеку, сидя за монитором? Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

**1 ролик «Интернет безопасность»**

**Компьютерные вирусы**
Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю. В большинстве случаев распространяются вирусы через интернет.
**Методы защиты от вредоносных программ:**
• Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
• Постоянно устанавливай обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
• Ограничь физический доступ к компьютеру для посторонних лиц;
• Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
• Работай на своем компьютере под правами пользователя, а не администратора.
• Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
• Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.
**Сети WI-FI**
Да, бесплатный интернет-доступ в общественных местах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.
**Советы по безопасности работе в общедоступных сетях Wi-fi:**• Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
• Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
• При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
• Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
• Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;
• В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.
**Социальные сети**
Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.
**Основные советы по безопасности в социальных сетях:**
• Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
• Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
• Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
• Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
• Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
• При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
• Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Видео «Шокирующая правда о социальных сетях»**

 **Электронные деньги**
Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.
**Основные советы по безопасной работе с электронными деньгами:**• Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
• Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
• Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль.
• Не вводи свои личные данные на сайтах, которым не доверяешь.
**Электронная почта**
Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Также кроме передачи простого текста, имеется возможность передавать файлы.
**Основные советы по безопасной работе с электронной почтой:**• Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
• Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;
• Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
• Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
• Если есть возможность написать самому свой личный вопрос, используй эту возможность;
• Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
• Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
• После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».
**Кибербуллинг или виртуальное издевательство**
Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.
**Основные советы по борьбе с кибербуллингом:**• Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
• Управляй своей киберрепутацией;
• Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
• Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
• Соблюдай свой виртуальную честь смолоду;
• Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
• Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
• Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.