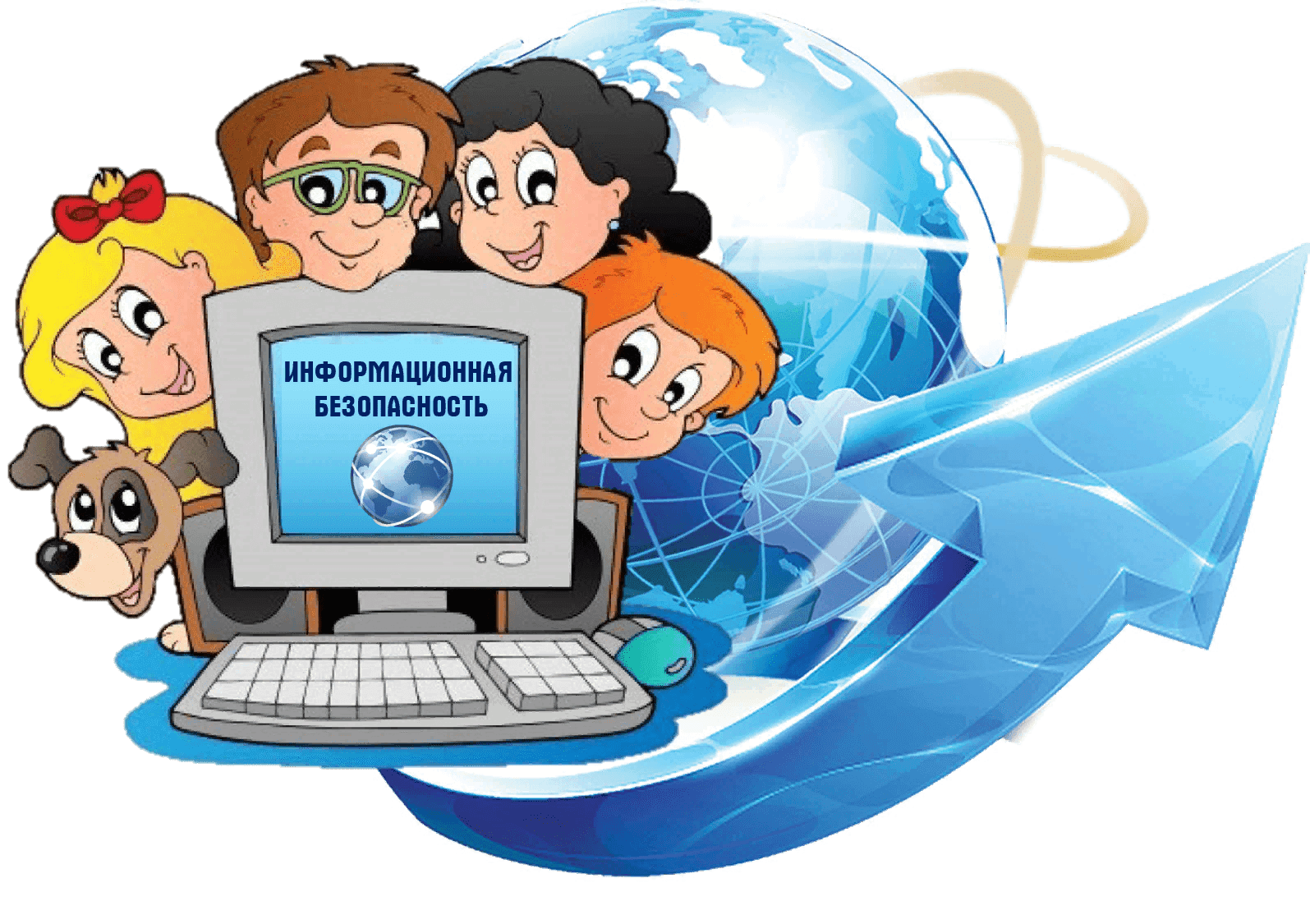
**Безопасность в интернете:**

**возрастные рекомендации для детей и подростков**

В наши дни мы все проводим много времени в интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг (травля), неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков.

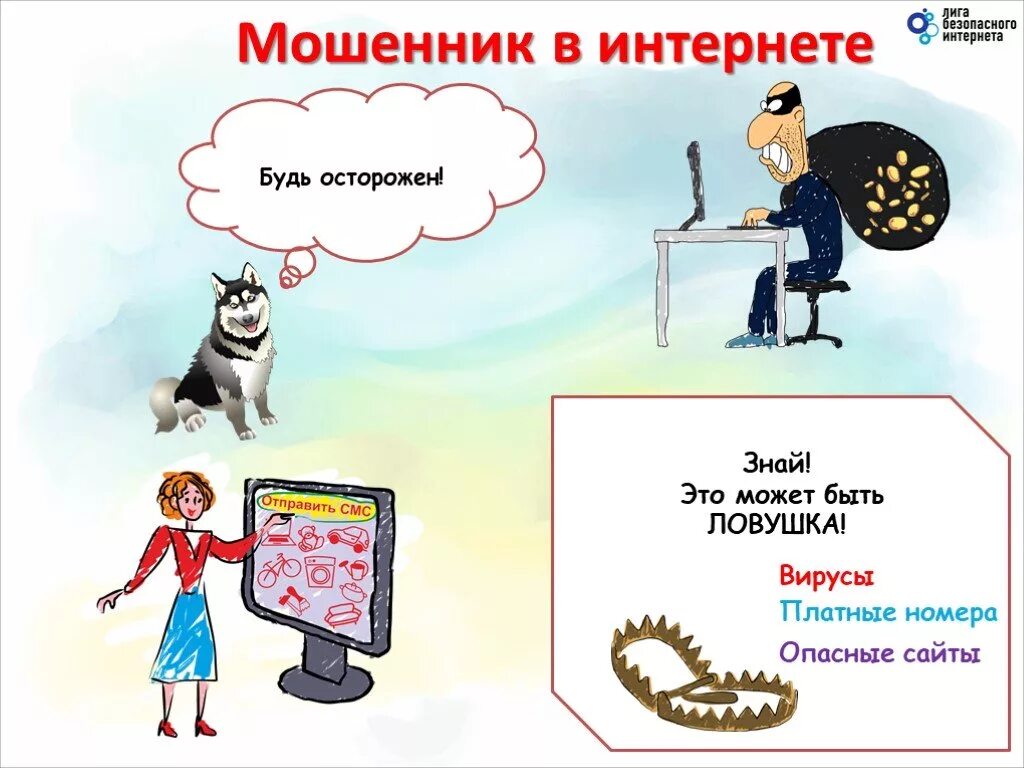
Интернет - это прекрасное место для обучения и общения. Но родители должны быть в курсе того, что их дети видят и слышат в Интернете, с кем общаются и что рассказывают о себе. Ниже приведено несколько рекомендаций, которые помогут обеспечить безопасность детей в интернете.

**Общие рекомендации**

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

**Храните имена пользователей и пароли в безопасности**

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. Убедитесь, что дети знают, что эту информацию нельзя передавать никому, даже друзьям. Возможно, никто не хочет причинить ребенку никакого вреда, но даже в розыгрышах из лучших побуждений что-то может пойти не так и доставить неприятности. Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.



**Не разглашайте личную информацию в интернете**

Дети и подростки не должны сообщать никому в интернете свое полное настоящее имя, адрес, район проживания, номер телефона и прочие данные. Общее правило: никогда не сообщать информацию, которая могла бы помочь интернет-хищникам найти их. Даже небольших деталей, таких как название школы или спортивной команды, достаточно, чтобы раскрыть личность. Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.



**Будьте внимательны в социальных сетях**

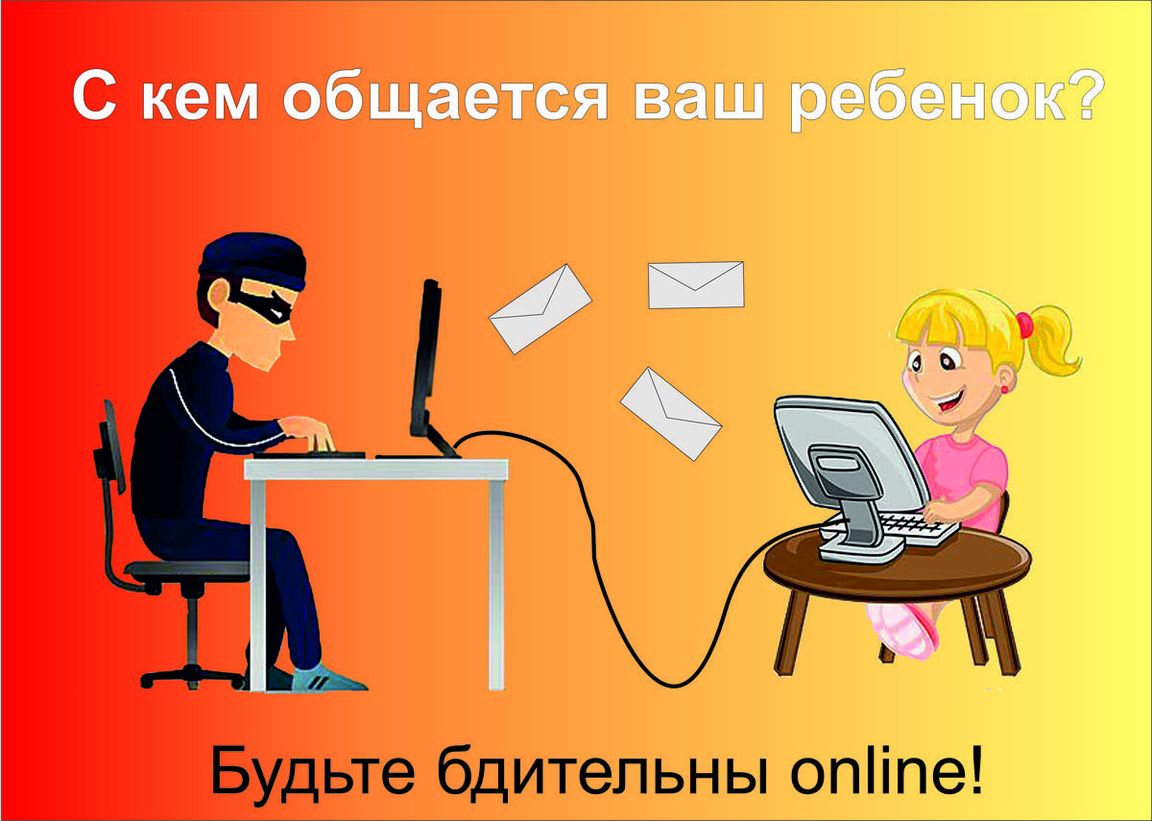
Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. Напомните детям, что все опубликованное в интернете сразу становится общедоступным, и любой может увидеть это. Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

**Проверяйте возрастные ограничения**

Многие приложения и веб-сайты имеют собственные возрастные ограничения для создания учетных записей, просмотра и регистрации. Но проблема в том, что на большинстве таких сайтов фактически нет функции проверки возраста.

**Объясните опасность передачи геоданных**

Почти все современные приложения и веб-сайты имеют функции отметки геопозиции или передачи данных о местоположении. Дети и подростки должны знать, чем опасно сообщать о своем местоположении, и что не следует неосознанно соглашаться с таким условием во всплывающих окнах приложений. Публичная демонстрация данных о местоположении подвергает детей различным опасностям: от сетевых интернет-хищников, которые могут найти их, до риска кражи личных данных. Убедитесь, что дети понимают, что означает, когда в приложении спрашивается, можно ли передавать данные о местоположении.



**Создайте список правил использования интернета**

Один из лучших способов управлять использованием интернета детьми всех возрастов – это сесть и совместно составить список правил использования интернета в соответствии с их потребностями. Вы можете показать ребенку сайты для детей и подростков, поговорить о том, почему важно установить правила, и попросить их поделиться, если он чувствуют себя некомфортно или ему угрожает что-то, найденное в интернете, и т. д.

**Установите родительский контроль**

Настройте и пересмотрите параметры родительского контроля на всех своих устройствах в соответствии с возрастом ваших детей. Это поможет защитить детей от доступа к неприемлемому контенту в интернете. Параметры контроля можно настроить несколькими способами, например, обеспечить доступ детей только к соответствующему их возрасту контенту, установить время использования устройства, контролировать активность и запретить передачу личной информации.

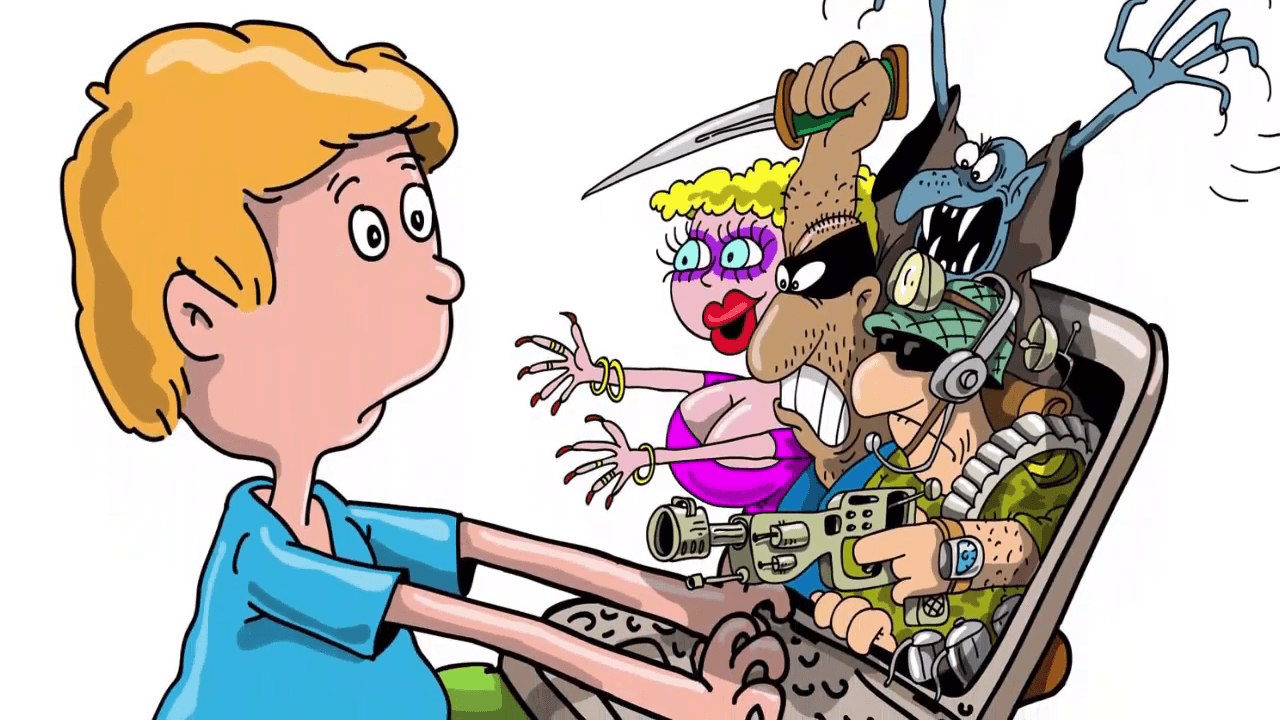


**Используйте антивирусные программы**

Помимо родительского контроля, используйте на всех устройствах антивирусные программы. Они защищают подключенные к интернету устройства от входящих угроз, а также выявляют, уничтожают и предупреждают о возможных угрозах для системы. Антивирусные программы не отстают от современных угроз и помогают обнаруживать новые постоянно появляющиеся вирусы.

**Объясните детям об опасности личных встреч с незнакомцами**

Дети никогда не должны лично встречаться с незнакомцами, с которыми они общались в интернете, если за такой встречей не наблюдает родитель. Объясните детям и подросткам, что не следует общаться с незнакомцами лично. Интернет-хищники или участники кибербуллинга (травли) могут скрываться, чтобы ребенок не понял, что общается с кем-то из интернета.



**Возрастные рекомендации**

В дополнение к общим, существуют также возрастные рекомендации, которые следует учитывать при использовании интернета детьми.

**2 – 4 года**

* Не допускайте самостоятельного времяпрепровождения в интернете.
* Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.
* Не позволяйте детям переходить по ссылкам.
* Ограничьте время, проводимое за компьютером.
* Прививайте базовые навыки работы с компьютером с помощью соответствующих возрасту игр и образовательных программ.

**5 – 7 лет**

* Не допускайте самостоятельного времяпрепровождения в интернете или с телефоном.
* Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.
* Не позволяйте детям переходить по ссылкам.
* Используйте удобные для детей поисковые системы с родительским контролем.
* Настройте фильтры по возрасту.
* Ограничьте время, проводимое в интернете.
* Ограничьте детей списком любимых сайтов, который вы составите вместе.
* Убедитесь, что подключенные к интернету устройства находятся в открытом доступе, где вы можете их наблюдать.
* Заблокируйте использование средств обмена мгновенными сообщениями, электронной почты, чатов, мобильного интернета, обмена текстовыми, графическими и видео сообщениями, а также доступ к доскам сообщений.
* Научите детей никогда не разглашать личную информацию в интернете.

**8 – 10 лет**

* Обсудите с детьми, что им интересно в интернете.
* Расскажите детям об опасностях, скрывающихся в интернете.
* Научите детей никогда не разглашать личную информацию.
* Избегайте пугающих образов.
* Объясните детям, как правильно общаться с друзьями в интернете.
* Попросите детей рассказывать вам о случаях, когда они сталкиваются в интернете с чем-то, что вызывает у них чувство неловкости.
* Проводите время в интернете совместно с детьми или ограничьте им доступ только набором одобренных сайтов.
* Размещайте подключенные к интернету устройства в открытой общей зоне.
* Установите родительский контроль, соответствующий возрасту ребенка.
* Используйте инструменты фильтрации и мониторинга.
* Используйте удобные для детей поисковые системы.
* Запретите использование средств обмена мгновенными сообщениями, чатов и сайтов социальных сетей, предназначенных для более взрослой аудитории.
* Попросите ребенка использовать тот же адрес электронной почты, который используете вы сами, или специальный адрес, к которому у вас есть доступ.
* Просите детей открыто рассказывать о своих действиях в интернете.

Безопасность в интернете достигается постоянными разговорами с детьми о том, как и для чего используется интернет, и знанием, как обеспечить их защиту. Понимание того, почему дети выходят в интернет, с кем они там взаимодействуют и какие сайты посещают, очень важно для обеспечения их безопасности. Также крайне важно информировать их о рисках, связанных интернетом, о безопасном и вежливом общении в интернете и о действиях в случае, если они столкнулись с чем-то неуместным.

