МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

О размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет*

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», которые прошли в Совете Федерации 17 апреля 2017 года, были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет (далее – методические рекомендации).

Методические рекомендации направлены на качественное повышение уровня информационной деятельности общеобразовательных организаций и органов, осуществляющих управление в сфере образования, в части информирования учащихся, их родителей (законных представителей) и педагогических работников об основных аспектах информационной безопасности.

Методические рекомендации позволят общеобразовательным организациям и органам, осуществляющим управление в сфере образования, как актуализировать уже используемые и размещенные информационные материалы, так и подготовить их, если они отсутствуют, с учетом лучших практик и рекомендаций.

* Методические материалы рекомендованы письмом Минобрнауки России от 14 мая 2018 г. № 08-11854.

В рамках методических рекомендаций рассматриваются следующие инструменты:

1. информационные стенды;
2. официальные интернет-ресурсы;
3. средства массовой информации (школьные газеты, педагогические издания и другие).

Информационные стенды

На информационных стендах в общеобразовательных организациях, расположенных в фойе учреждений и в кабинетах, оснащенных персональными устройствами для выхода в сеть Интернет, рекомендуется разместить информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.

В приложении № 1 к методическим рекомендациям представлен образец памятки для размещения на информационных стендах.

Средства массовой информации

В средствах массовой информации, ориентированных на обучающихся, рекомендуется в течение учебного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности, а также различные памятки общего характера.

В средствах массовой информации, ориентированных на педагогическую общественность, рекомендуется в течение календарного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности и несовершеннолетних учащихся, и общеобразовательных организаций, а также различные памятки, обзоры нормативно-правового регулирования данной сферы и информацию об актуальных мероприятиях и событиях в данной сфере.

В ходе проведения Единого урока по безопасности в сети Интернет рекомендуется обеспечить тематический выпуск средства массовой информации либо серии публикаций, в том числе рассмотреть организованные мероприятия для обучающихся, их родителей (законных представителей) и педагогической общественности.

Официальные интернет-ресурсы

Общеобразовательным организациям рекомендуется на своих официальных интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела «Информационная безопасность», в рамках которого предусмотреть размещение следующей информации:

№ п/п	Раздел/подраздел	Формат представления материалов	Содержание материалов
1	Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся	Копии документов в формате *PDF	Размещаются копии документов, то есть сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие документы
2	Нормативное регулирование	Копии документов в формате *PDF	Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на соответствующие документы на сайтах органов государственной власти
3	Педагогическим работникам	Текст на странице сайта. Копии документов в формате *PDF	Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников
4	Обучающимся	Текст на странице сайта	Размещается информационная памятка (приложение № 2) и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся
5	Родителям (законным представителям) обучающихся	Текст на странице сайта	Размещается информационная памятка (приложение № 3)
6	Детские безопасные сайты	Текст на странице сайта	Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов

Органам, осуществляющим управление в сфере образования, рекомендуется на своих официальных интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела «Информационная безопасность», в рамках которого предусмотреть размещение информации согласно приложениям № 1, 2, 3.

Приложение № 1

Памятка для обучающихся об информационной безопасности детей

НЕЛЬЗЯ

1. Не сообщай всем подряд свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также не предоставляй фотографии свои, своей семьи и друзей).

2. Не открывай вложенные файлы электронной почты, когда не знаешь отправителя.

3. Не груби, не придирайся, не оказывай давление – не веди себя невежливо и агрессивно.

4. Не распоряжайся деньгами своей семьи без разрешения старших – всегда спрашивай родителей.

5. Не встречайся с интернет-знакомыми в реальной жизни – посоветуйся с взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете – сообщи об этом своим родителям или опекунам.

2. Приглашают переписываться, играть, обмениваться – проверь, нет ли подвоха.

3. Незаконное копирование файлов в Интернете – это воровство.

4. Всегда рассказывай взрослым о проблемах в Сети – они обязательно помогут.

5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и на других порталах.

МОЖНО

1. Уважай других пользователей.

2. Пользуешься интернет-источником – делай ссылку на него.

3. Открывай только те ссылки, в которых уверен.

4. Обращайся за помощью к взрослым – родители, опекуны и администрация сайтов всегда помогут.

5. Пройди обучение на сайте «Сетевичок» и получи паспорт цифрового гражданина!

Приложение № 2

Информационная памятка для обучающихся для размещения на официальных интернет-ресурсах

С каждым годом молодежи в Интернете становится больше, а школьники – одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, Интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в Сети.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. Кроме того, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев вирусы распространяются через Интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.

2. Постоянно устанавливай патчи (цифровые «заплатки», которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.

4. Используй антивирусные программные продукты известных производителей с автоматическим обновлением баз.

5. Ограничь физический доступ к компьютеру для посторонних лиц.

6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников.

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Сначала уточни у него, отправлял ли он тебе их.

Сети Wi-Fi

Аббревиатура Wi-Fi происходит от словосочетания Wireless Fidelity, которое переводится как «беспроводная точность». Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Сегодня термином Wi-Fi называют технологию передачи данных по безпроводным сетям.

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные сети Wi-Fi не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-Fi:

1. Не передавай свою личную информацию через общедоступные сети Wi-Fi. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.

2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.

3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или входа в электронную почту.

5. Используй только защищенное соединение через HTTPS, а не HTTP, то есть при наборе веб-адреса вводи именно «https://».

6. 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, а в Facebook уже зарегистрирован миллиард человек, что составляет одну седьмую всех жителей планеты. 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:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату своего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. 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.

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информацию: место жительства, место учебы и прочее.

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр, и с количеством знаков не менее восьми.

7. 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.

Электронные деньги

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно, и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют, и о них уже прописано в законе, где их разделяют на анонимные и неанонимные. Разница в том, что анонимными разрешается проводить операции без идентификации пользователя, а при операциях с неанонимными электронными деньгами идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. 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.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли – это пароли, которые содержат не менее восьми знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, таких как знак доллара, фунта, восклицательный знак и т. п. Например, $tR0ng!.

4. 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. Обычно адрес электронного почтового ящика выглядит следующим образом: имя_пользователя@имя_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по СМС.

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Сначала уточни у них, отправляли ли они тебе эти файлы.

8. 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:

1. Не бросайся в бой. Лучший способ: посоветоваться, как себя вести, а если нет того, к кому можно обратиться за советом, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. Управляй своей киберрепутацией.

3. Анонимность в Сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Соблюдай свою виртуальную честь смолоду.

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

8. Если ты свидетель кибербуллинга, выступи против преследователя, покажи ему, что его действия оцениваются негативно, поддержи жертву, которой нужна психологическая помощь, сообщи взрослым о факте агрессивного поведения в Сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Ничто не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

2. Думай, прежде чем отправить СМС-сообщение, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему смартфона.

4. Используй антивирусные программы для мобильных телефонов.

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

7. Периодически проверяй, какие платные услуги активированы на твоем номере.

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Онлайн-игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на обеспечение безопасности: совершенствуются системы авторизации, выпускаются новые патчи (цифровые «заплатки» для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.

3. Не указывай личную информацию в профайле игры.

4. Уважай других участников игры.

5. Не устанавливай неофициальные патчи и моды.

6. Используй сложные и разные пароли.

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг, или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в Интернет и продолжают заниматься «любимым» делом.

Так появилась новая угроза – интернет-мошенничество, или фишинг, главная цель которого состоит в получении

конфиденциальных данных пользователей – логинов и паролей. На английском языке phishing читается как «фишинг» (от fishing – рыбная ловля).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить об этом администраторам ресурса как можно скорее.

2. Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.

3. Используй сложные и разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в Сети, а не ко всем.

4. Если тебя взломали, предупреди всех знакомых, которые добавлены у тебя в друзьях, что по этой причине, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.

5. Установи надежный пароль (ПИН) на мобильный телефон.

6. Отключи сохранение пароля в браузере.

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Сначала уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация – это негативная или позитивная информация в Сети о тебе. Компрометирующая информация, размещенная в Интернете, может серьезным образом отразиться на твоей реальной жизни. Цифровая репутация – это твой имидж, который формируется из информации о тебе в Интернете.

Данные о твоем месте жительства, учебы, твоем финансовом положении, особенностях характера и рассказы о близких – все это накапливается в Сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная пять лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь.

Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли, а главное – что подумают о тебе окружающие люди, которые найдут и увидят ее. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети.

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей».

3. Не размещай и не указывай информацию, которая может кого-либо оскорбить или обидеть.

Авторское право

Современные школьники – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных доступа к твоим аккаунтам до блокировки твоего устройства, на котором

установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в Сети.

О портале

Сетевичок.рф – твой главный советчик в Сети. Здесь ты можешь узнать информацию о безопасности в Сети, изложенную понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Приложение № 3

Памятка для родителей об информационной безопасности детей

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующем отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону, информационная безопасность детей – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Согласно Федеральному закону № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

- информация, запрещенная для распространения среди детей;
- информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится информация:

– побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе причинению вреда своему здоровью, самоубийству;

– способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе,

принять участие в азартных играх, заняться проституцией, бродяжничеством или попрошайничеством;

– обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

– отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

– оправдывающая противоправное поведение;

– содержащая нецензурную брань;

– содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится информация:

– представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

– вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

– представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

– содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку – главный метод защиты.

2. Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т. п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, на порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).

4. Поощряйте ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети порой не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь, кто его друзья в Интернете, так же, как интересуетесь реальными друзьями.

Возраст детей от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, то есть «Родительский контроль», или то, что можно увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7–8 лет:

1. Создайте список домашних правил посещения Интернета при участии ребенка и требуйте их выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому, что вам так хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите ребенка советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Приучите ребенка не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте ребенку использовать службы мгновенного обмена сообщениями.

11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с ребенком о его друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте табу из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

14. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. В случае инцидента оставайтесь спокойным и напомните ребенку, что он в безопасности, если сам рассказал вам о своих тревогах. Похвалите и посоветуйте подходить всякий раз в подобных случаях.

Возраст детей от 9 до 12 лет

В этом возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят все увидеть, прочесть, услышать. Поэтому нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств «Родительского контроля».

Советы по безопасности в Интернете для детей от 9 до 12 лет:

1. Создайте список домашних правил посещения Интернета при участии ребенка и требуйте их выполнения.

2. Требуйте от вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком, когда он работает за компьютером, покажите ему, что вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с ним о его друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте ребенку заходить только на сайты из «белого» списка, который создайте вместе с ним.

9. Приучите ребенка никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

10. Приучите ребенка не загружать программы без вашего разрешения. Объясните, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомнайте ребенку, что он в безопасности, если сам рассказал вам о своих тревогах и опасениях.

13. Расскажите ребенку о порнографии в Интернете.

14. Настаивайте на том, чтобы ребенок предоставлял вам доступ к своей электронной почте, чтобы вы убедились, что он не общается с незнакомцами.

15. Объясните ребенку, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее не отпускайте ребенка в «свободное плавание» по Сети. Старайтесь активно участвовать в его общении в Интернете.

Важно по-прежнему строго соблюдать правила интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности ребенка в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете.

Советы по безопасности в Интернете для подростков от 13 до 17 лет:

1. Создайте список домашних правил посещения Интернета при участии ребенка и требуйте безусловного их выполнения. Обговорите с ним список запрещенных сайтов (черный список), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с ребенком о его друзьях в Интернете, о том, чем они заняты, таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми ребенок общается посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди ему знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».

5. Необходимо знать, какими чатами пользуется ваш ребенок. Поощряйте использование модерируемых чатов и настаивайте, чтобы ребенок не общался в приватном режиме.

6. Настаивайте на том, чтобы ребенок никогда не встречался лично с друзьями из сети Интернет.

7. Приучите ребенка не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите ребенка не загружать программы без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. В случае инцидента напомните ребенку, что он в безопасности, если сам рассказал вам об угрозах или своих тревогах. Похвалите и посоветуйте подходить каждый раз в подобных случаях.

10. Расскажите ребенку о порнографии в Интернете. Помогите ему защититься от спама. Научите не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещает ребенок.

12. Научите ребенка уважать других в Интернете. Убедитесь, что он знает о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

13. Объясните, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с ребенком проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление вашей родительской ответственности и заботы.