Редакция от 25 мая 2018

Как защититься от фишинга

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Эта памятка поможет тебе защитить личные данные

Обычной кражей денег и документов никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг (от английского слова fishing – рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей.

Советы по борьбе с фишингом

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
2. Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будут рассылаться спам и ссылки на фишинговые сайты.
5. Установи надежный пароль (PIN) 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. Лучше уточни у них, отправляли ли они тебе эти файлы.

Редакция от 25 мая 2018

Как безопасно пользоваться смартфоном, планшетом

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СМАРТФОНОМ, ПЛАНШЕТОМ

Эта памятка поможет тебе безопасно пользоваться мобильными устройствами

Смартфоны и планшеты содержат в себе взрослый функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока 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.

Советы по безопасному использованию мобильных устройств

1. Ничего 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 SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего 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.

Редакция от 25 мая 2018

Как безопасно пользоваться электронной почтой

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

Эта памятка поможет тебе безопасно пользоваться электронной почтой

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Меры защиты электронной почты

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 «рок2018@» вместо «андрей2005@».
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.
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. Лучше 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».

Редакция от 25 мая 2018

Как безопасно общаться в социальных сетях

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ОБЩАТЬСЯ В СОЦИАЛЬНЫХ СЕТЯХ

Эта памятка поможет тебе безопасно общаться в социальных сетях

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой 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.

Советы по безопасному общению 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 твоего 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: имя, 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 8.
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 ко всем сразу.

Редакция от 25 мая 2018

Как безопасно пользоваться сетью Wi-Fi

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СЕТЬЮ WI-FI

Эта памятка поможет тебе безопасно пользоваться сетью Wi-Fi.

Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi – аббревиатура от английского словосочетания Wireless Fidelity, что дословно переводится как беспроводная точность. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но общедоступные сети Wi-Fi не являются безопасными.

Советы по безопасному использованию 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 брандмауер. 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 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.

Редакция от 25 мая 2018

Как защититься от компьютерных вирусов

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК ЗАЩИТИТЬСЯ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Эта памятка поможет тебе безопасно находиться в сети

Компьютерный вирус – это программа, отличительной особенностью которой является способность к размножению. 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 распространяются вирусы через интернет.

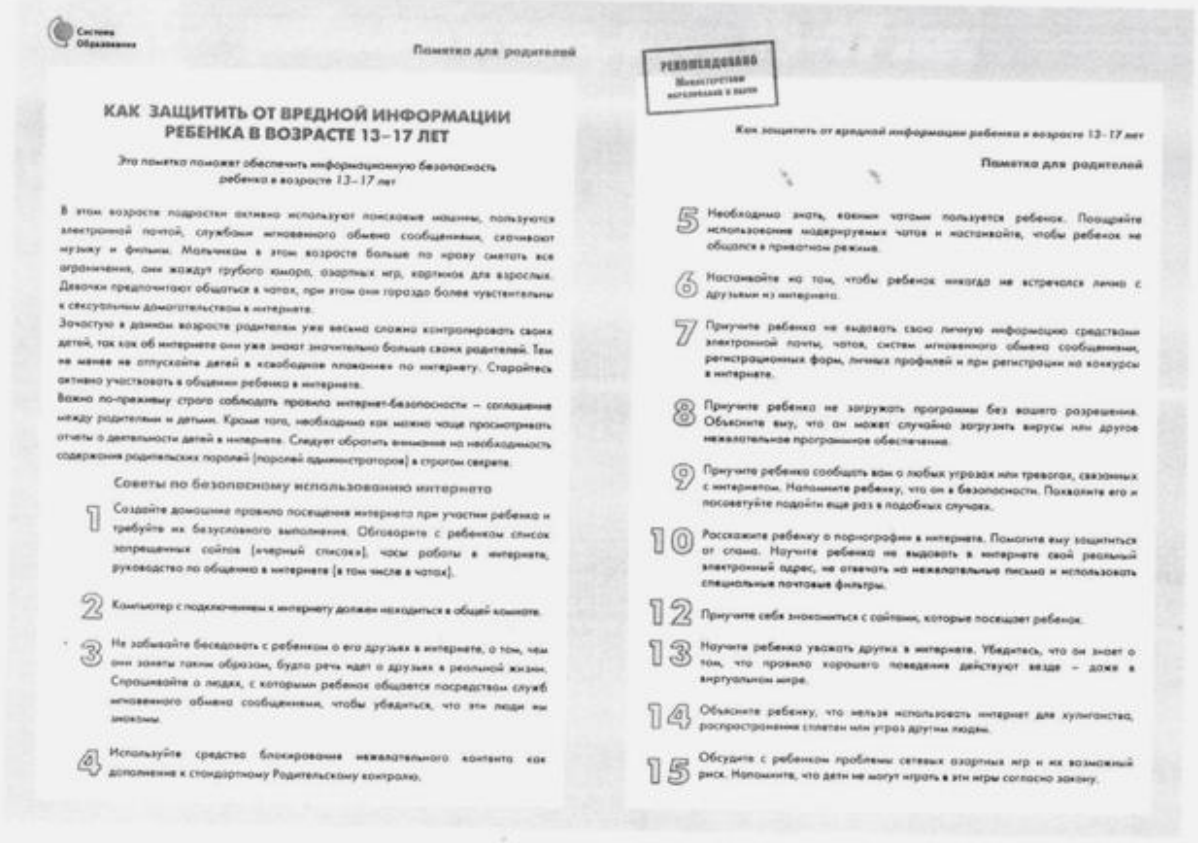
Методы защиты от вредоносных программ

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.
2. Постоянно устанавливай патчи (цифровые заплатки для программ) 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. Лучше уточни у него, отправлял ли он тебе их.

Редакция от 25 мая 2018

Как защитить от вредной информации ребенка в возрасте 13–17 лет

Виктория Ярцева, юрист-редактор справочной системы «Образование»



Система Образования

Памятка для родителей

КАК ЗАЩИТИТЬ ОТ ВРЕДНОЙ ИНФОРМАЦИИ РЕБЕНКА В ВОЗРАСТЕ 13–17 ЛЕТ

Это памятка поможет обеспечить информационную безопасность ребенка в возрасте 13–17 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 уже весьма сложно контролировать своих детей, так как об интернете они уже знают значительно больше своих родителей. Тем не менее не отпускайте детей в «свободное плавание» по интернету. Старайтесь активно участвовать в общении ребенка в интернете.

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

Советы по безопасному использованию интернета

1. Создайте домашние правила посещения интернета при участии ребенка и требуйте их безусловного выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в интернете, руководство по общению в интернете (в том числе в чатах).
2. Компьютер с подключением к интернету 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 им знакомы.
4. Используйте средство блокирование нежелательного контента как дополнение к стандартному Родительскому контролю.

РЕКОМЕНДОВАНО Министерством образования и науки

Как защитить от вредной информации ребенка в возрасте 13–17 лет

Памятка для родителей

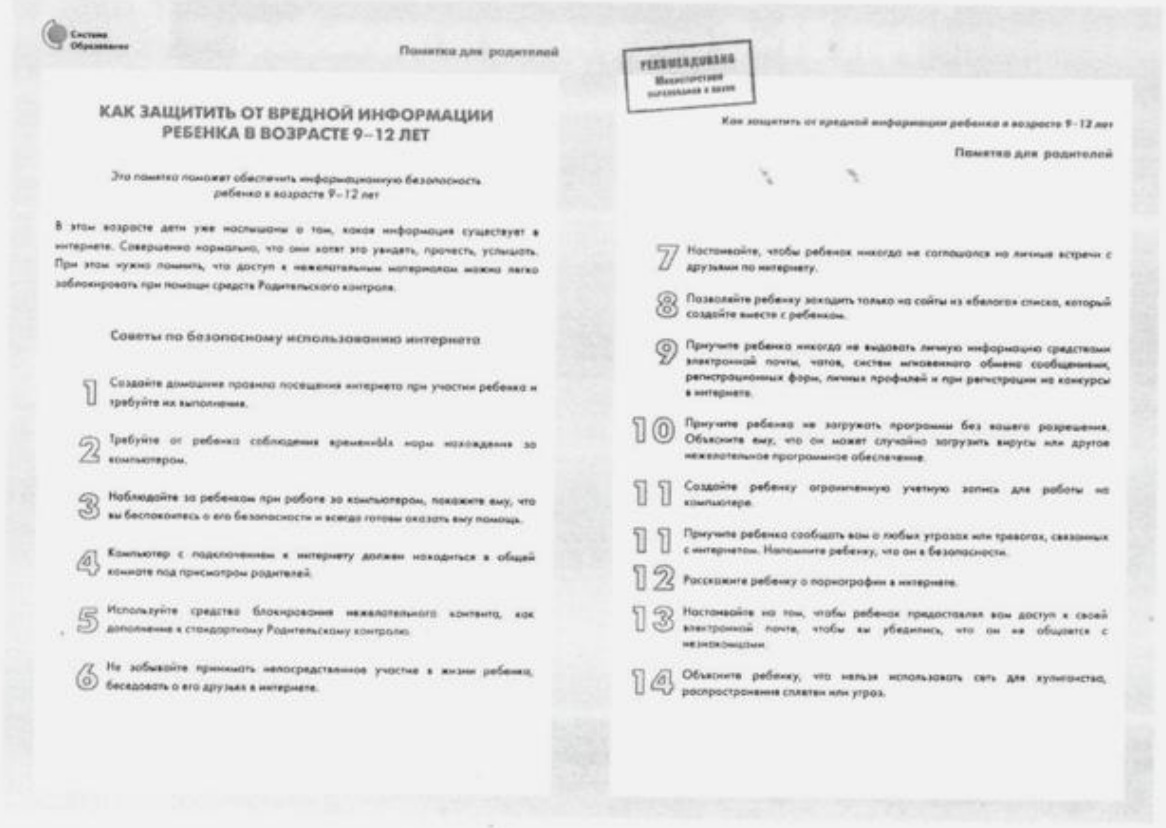
5. Необходимо знать, какими чатами пользуется ребенок. Поощряйте использование модерируемых чатов и настаивайте, чтобы ребенок не общался в приватном режиме.
6. Настаивайте на том, чтобы ребенок никогда не встречался лично с друзьями из интернета.
7. Приучите ребенка не выдавать свою личную информацию 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 ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните ребенку, что он в безопасности. Похвалите его и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите ребенку о порнографии в интернете. Помогите ему защититься от спама. Научите ребенка не выдавать в интернете свой реальный электронный адрес, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
12. Приучите себя знакомиться с сайтами, которые посещает ребенок.
13. Научите ребенка уважать других в интернете. Убедитесь, что он знает о том, что правило хорошего поведения действуют везде – даже в виртуальном мире.
14. Объясните ребенку, что нельзя использовать интернет для хулиганства, распространения сплетен или угроз другим людям.
15. Обсудите с ребенком проблемы сетевых азартных игр и их возможный риск. Напомните, что детям не могут играть в эти игры согласно закону.

Из рекомендации «Изменились требования к школьному сайту. Срочно разместите 15 новых памяток»

Редакция от 25 мая 2018

Как защитить от вредной информации ребенка в возрасте 9–12 лет

Виктория Ярцева, юрист-редактор справочной системы «Образование»



Памятка для родителей

КАК ЗАЩИТИТЬ ОТ ВРЕДНОЙ ИНФОРМАЦИИ РЕБЕНКА В ВОЗРАСТЕ 9–12 ЛЕТ

Эта памятка поможет обеспечить информационную безопасность ребенка в возрасте 9–12 лет

В этом возрасте дети уже наслышаны о том, какая информация существует в интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасному использованию интернета

1. Создайте домашние правила посещения интернета при участии ребенка и требуйте их выполнения.
2. Требуйте от ребенка соблюдения временны́х норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе 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 о его друзьях в интернете.

РЕКОМЕНДОВАНО Министерством образования и науки

Как защитить от вредной информации ребенка в возрасте 9–12 лет

Памятка для родителей

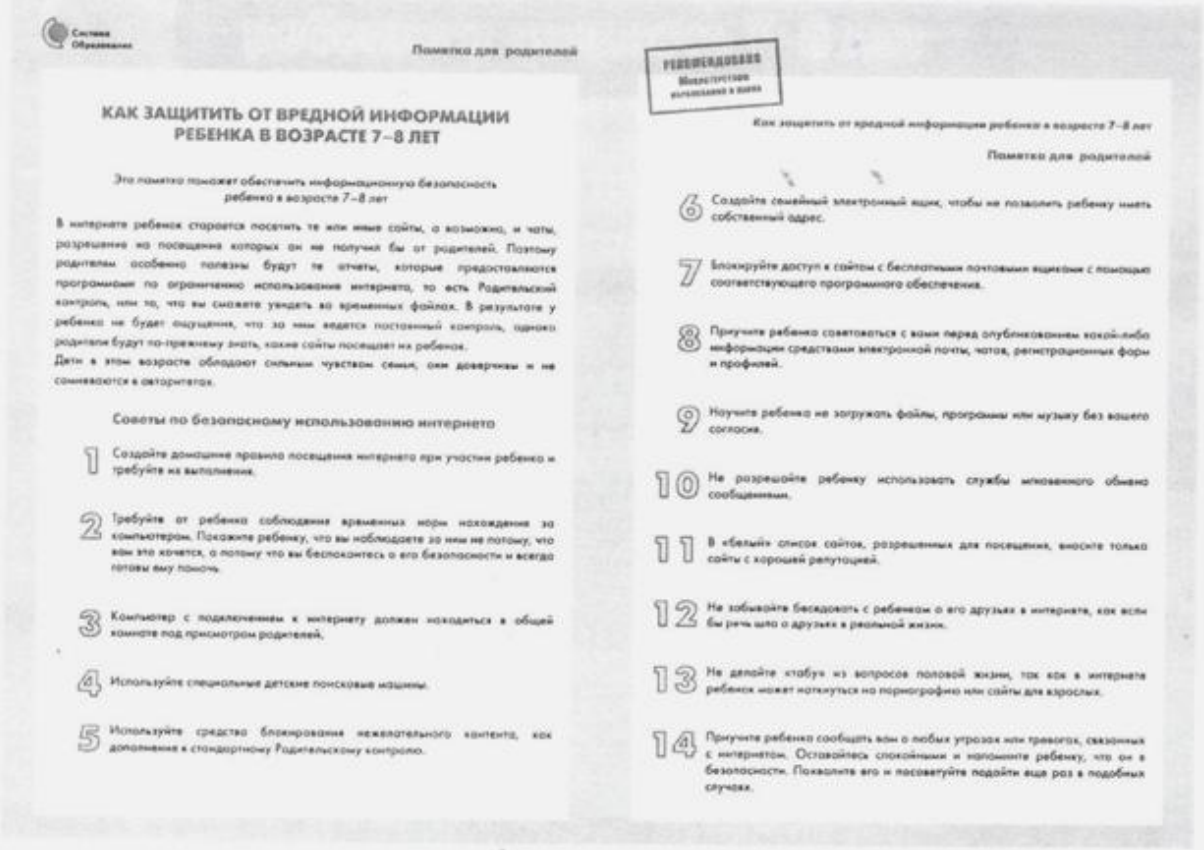
7. Настаивайте, чтобы ребенок никогда не соглашался на личные встречи с друзьями по интернету.
8. Позволяйте ребенку заходить только на сайты из «белого» списка, который создайте вместе с ребенком.
9. Приучите ребенка никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в интернете.
10. Приучите ребенка не загружать программы без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте ребенку ограниченную учетную запись для работы на компьютере.
11. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните ребенку, что он в безопасности.
12. Расскажите ребенку о порнографии в интернете.
13. Настаивайте на том, чтобы ребенок предоставлял вам доступ к своей электронной почте, чтобы вы убедились, что он не общается с незнакомцами.
14. Объясните ребенку, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Из рекомендации «Изменились требования к школьному сайту. Срочно разместите 15 новых памяток»

Редакция от 25 мая 2018

Как защитить от вредной информации ребенка в возрасте 7–8 лет

Виктория Ярцева, юрист-редактор справочной системы «Образование»



Система Образование

Памятка для родителей

КАК ЗАЩИТИТЬ ОТ ВРЕДНОЙ ИНФОРМАЦИИ РЕБЕНКА В ВОЗРАСТЕ 7–8 ЛЕТ

Это памятка поможет обеспечить информационную безопасность ребенка в возрасте 7–8 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 вы сможете увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут по-прежнему знать, какие сайты посещает их ребенок.

Дети в этом возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах.

Советы по безопасному использованию интернета

1. Создайте домашние правила посещения интернета при участии ребенка и требуйте их выполнения.
2. Требуйте от ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому, что вам это 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 средство блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

РЕКОМЕНДОВАНО Министерством образования и науки

Как защитить от вредной информации ребенка в возрасте 7–8 лет

Памятка для родителей

6. Создайте семейный электронный ящик, чтобы не позволить ребенку иметь собственный адрес.
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. Научите 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 ребенок может натолкнуться на порнографию или сайты для взрослых.
14. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Оставайтесь спокойными и напомните ребенку, что он в безопасности. Похвалите его и посоветуйте подойти еще раз в подобных случаях.

Из рекомендации «Изменились требования к школьному сайту. Срочно разместите 15 новых памяток»

Редакция от 25 мая 2018

Как обеспечить информационную безопасность ребенка

Виктория Ярцева, юрист-редактор справочной системы «Образование»

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕБЕНКА

Эта памятка поможет обеспечить информационную безопасность вашего ребенка

Общие правила:

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 другие), 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 содержать и ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).

4. Поощряйте вашего ребенка сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда он это делает (из-за опасения потерять доступ к интернету дети не говорят родителям о проблемах, а также могут начать использовать интернет вне дома и школы).

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