

## 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. Страницы 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.

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

Эта 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 средства блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

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 наткнуться 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.

## 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 своего 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.

## ЧТО ТАКОЕ АВТОРСКОЕ ПРАВО

Эта памятка расскажет тебе об авторском праве

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 ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа.

Не стоит также забывать, что существуют **легальные и бесплатные программы**, которые можно найти в сети.

## 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.



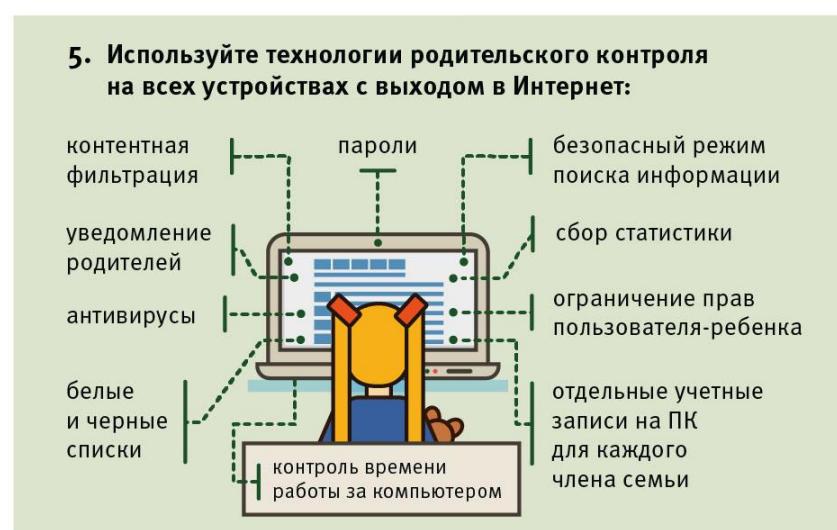
1. Обращайте внимание на то, какие сайты посещает Ваш ребенок



2. Учите ребёнка избирательно относиться к информации, которую он получает в Интернете и проверять её



3. Объясните ребенку, как правильно реагировать на возможного агрессора и конфликтные ситуации в Интернете



4. РАССКАЖИТЕ РЕБЕНКУ О ТОМ, КАКОЮ ИНФОРМАЦИЮ РАЗМЕЩАТЬ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ ОПАСНО:



о своём местоположении



о планах на длительные поездки



фото дорогих вещей и подарков



фото квартир или дома



свой домашний адрес



фото личных документов и банковских карт



## Информационная безопасность детей

состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию

(Федеральный закон от 29.01.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию")

