# Что надо знать о медиабезопасности?

**автор Фандеева Т.В.**

Согласно российскому законодательству **информационная безопасность детей** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").
**Медиа-грамотность** определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.
На **сайте «Дети онлайн»** вы можете найти рекомендации, которые помогут вам обеспечить свою медиабезопасность в сетях Интернет и мобильной (сотовой) связи.

## Правила безопасного поведения в Интернет для обучающихся:

Вы должны это знать:
1. Не желательно размещать персональную информацию в Интернете.
**Персональная информация** — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей, или другая личная информация о вас, например, место учёбы, любимое место прогулок и т.п.
Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
2. Не отвечайте на спам (нежелательную электронную почту).
3. Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием. Не проходите по ссылкам, присланным Вам незнакомыми людьми, это может быть опасно для Вашего компьютера.
**Помните золотое правило:** то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в Сети.
4. Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
5. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают. Если вы желаете встретиться с новым интернет-другом, следует настоять на том, что вы придёте в сопровождении родителей на эту встречу.

6. Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Не сплетничайте, не хулиганьте, никому не угрожайте при общении в Интернете.
7. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
8. Никогда не поздно рассказать взрослым, если вас кто-то обидел или угрожает через Интернет.
9. Далеко не всё, что Вы читаете или видите в Интернете – правда. Всегда советуйтесь с родителями, если в чём то не уверены.
10. Уважайте чужую собственность. Незаконное копирование музыки, игр, фильмов, программ и иного – кража.
11. Используйте и регулярно обновляйте антивирусное ПО.

**Рекомендации абонентам сотовой связи:**

1. Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.
2. Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученных посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию.
3. Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.
4. Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.
5. Не торопитесь давать телефон на «1 звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.
6. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения - то и от известных. С развитием функциональности мобильных телефонов, КПК и коммуникаторов хакеры стали уделять больше внимания созданию вредоносного ПО для этих устройств. По возможности, установите на мобильное устройство одну из многих антивирусных программ, которые вы можете найти на сайтах известных производителей антивирусного ПО.
7. Для разблокировки компьютера от вирусов используйте антивирусное ПО известных разработчиков, в том числе, бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от

вируса или исчезновение интернет-баннера при отправке смс на короткий номер.