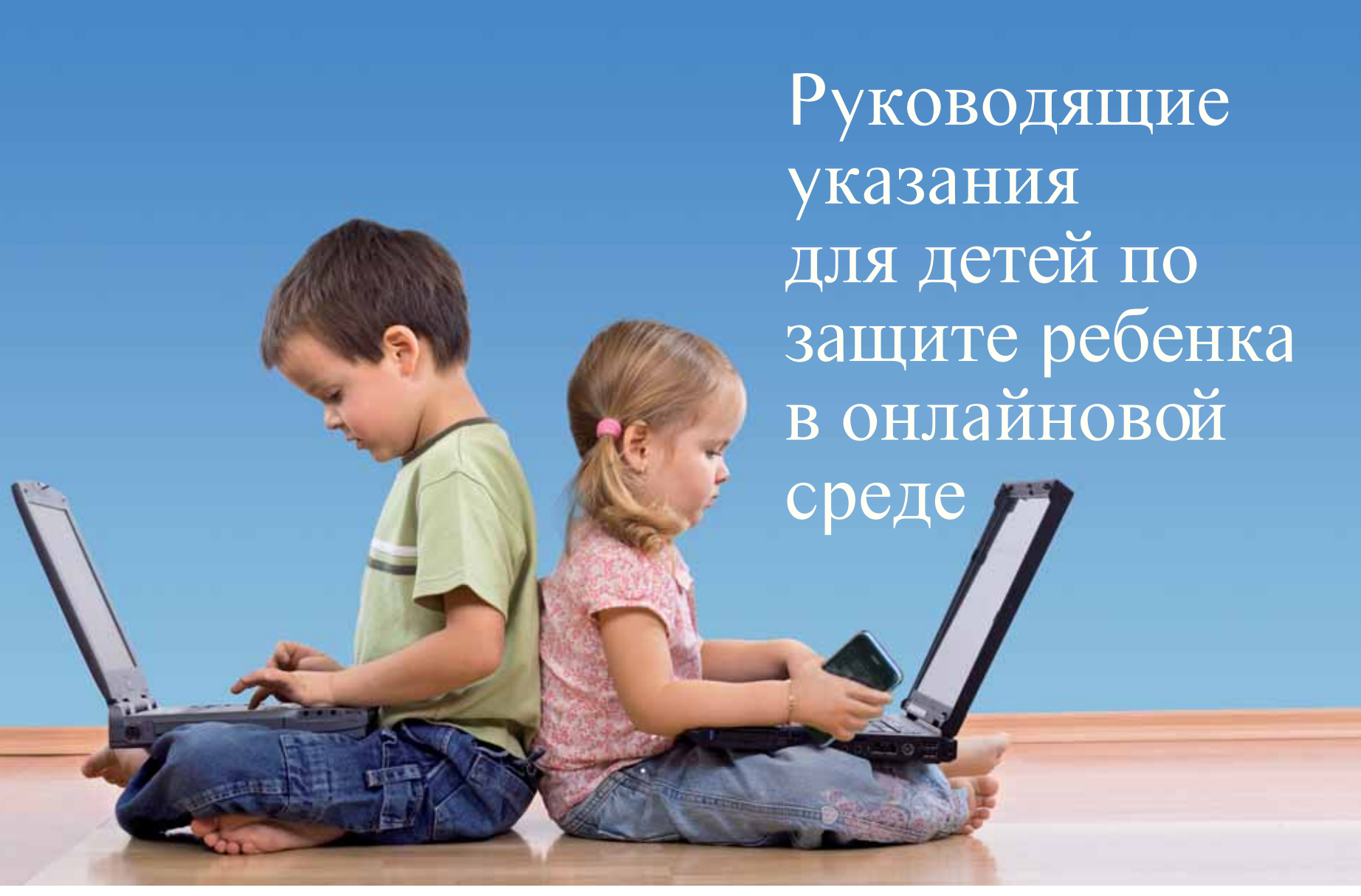


Руководящие указания для детей по защите ребенка в онлайновой среде

www.itu.int/cop

Официальное уведомление

Этот документ может периодически обновляться.

При необходимости процитированы источники третьих сторон. Международный союз электросвязи (МСЭ) не несет ответственности за содержание внешних источников, включая внешние веб-сайты, указанные в данной публикации.

Ни МСЭ, ни кто-либо, действующий от его имени, не несет ответственности за использование кем-либо информации, содержащейся в данной публикации.

Отказ от ответственности

Указание или ссылки на конкретные страны, компании, продукты или рекомендации, ни в коем случае не означает, что они поддерживаются или рекомендуются МСЭ, авторами или иными организациями, к которым принадлежат авторы, как предпочтительные по отношению к аналогичным товарам, компаниям и услугам, которые не упоминаются.

Запросы на воспроизведение выдержек из данной публикации можно направлять по адресу: jur@itu.int.

© международный союз электросвязи (МСЭ), 2009 г.

БЛАГОДАРНОСТИ

Данные руководящие указания подготовлены МСЭ и командой авторов из ведущих организаций, работающих в отрасли ИКТ, и они не смогли бы состояться без затраченного ими времени, присущего им энтузиазма и самоотверженности.

МСЭ благодарит всех следующих авторов, потративших свое драгоценное время и знания (перечислены в алфавитном порядке):

- Кристина Буети (Cristina Bueti) – МСЭ
- Мария Жозе Кантарино де Фриас (Maria José Cantarino de Frías) – Telefonica
- Джонн Карр (John Carr) – Детская благотворительная коалиция за безопасность интернета
- Дитер Карстенсен (Dieter Carstensen), Кристиана де Паоли (Cristiana dePaoli) и Мари Лаихо (Mari Laiho) – Спасем детей
- Майкл Моран (Michael Moran) – Интерпол
- Жанис Ричардсон – В безопасной сети

Авторы хотели бы поблагодарить Кристин Квинь (Kristin Kvigne) из Интерпола за ее подробный разбор и комментарии.

МСЭ хотел бы поблагодарить Сальму Аббаси (Salma Abbasi) из eWWG за ее неоценимое участие в инициативе "Защита ребенка в онлайновом режиме" (COP).

Дополнительная информация по этому проекту Руководящих указаний размещена по адресу: http://www.itu.int/cop/, и будет регулярно обновляться.

Если у вас есть какие-либо замечания, или вы хотели бы предоставить дополнительную информацию, пожалуйста, свяжитесь с г-жой Кристиной Буети по адресу: cop@itu.int.

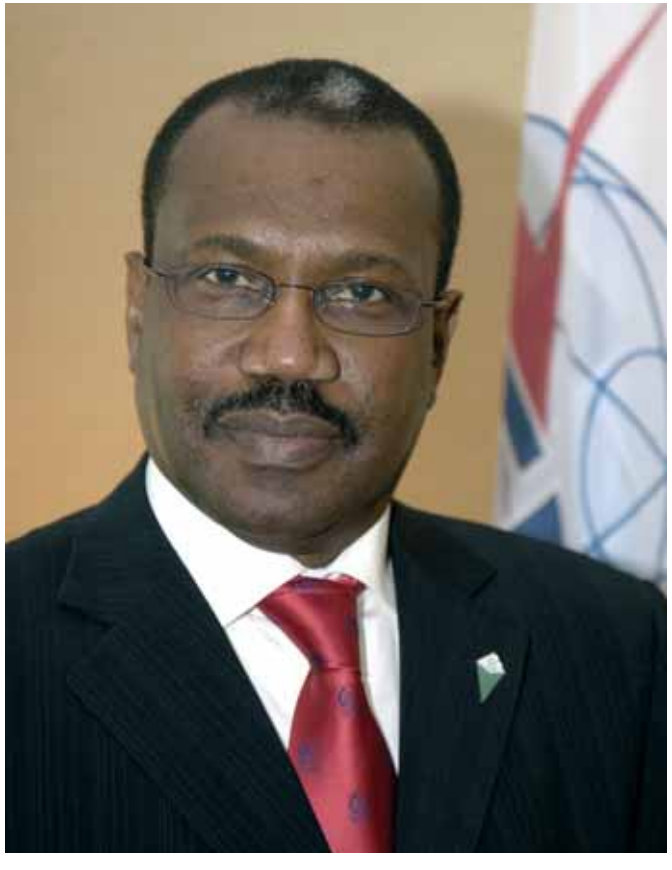
Оглавление

Конвенция ООН по правам ребенка определяет ребенка как лицо в возрасте до 18 лет. Настоящие Руководящие указания касаются проблем, стоящих перед всеми лицами, не достигшими 18 лет, во всех частях мира. Однако маловероятно, что семилетний пользователь интернета будет иметь те же потребности и интересы, что и 12-летний ученик средней школы или 17-летний подросток на пороге взрослости. В разных частях Руководящих указаний мы разработали советы или рекомендации, которые соответствуют этим различным условиям. Хотя использование широких категорий может оказаться полезным руководством, никогда не следует забывать, что каждый ребенок отличен от других. Потребности каждого конкретного ребенка заслуживают индивидуального рассмотрения. Более того, существует множество местных, юридических и культурных факторов, которые могут оказывать значительное влияние на то, каким образом эти Руководящие указания могут использоваться или пониматься в каждой отдельной стране или регионе.

В настоящее время существует множество международных законов и международных инструментов, которые поддерживают и, во многих случаях, действуют для защиты детей, как в общем, так и отдельно, в том что касается интернета. Эти законы и инструменты образуют основу настоящих Руководящих указаний. Они исчерпывающим образом учитывают Рио-де-Жанейрскую декларации и Призыв к действиям по предотвращению сексуальной эксплуатации детей и подростков и борьбе с ней, принятые на 3-м Всемирном конгрессе против сексуальной эксплуатации детей и подростков в ноябре 2008 года.

“Защита детей в онлайновой среде является глобальной задачей, поэтому нужно глобальное решение”

Предисловие



Я с радостью пользуюсь этой возможностью рассмотреть вместе с вами предварительный вариант руководящих указаний, которые разработаны при неоценимой помощи многочисленных участников.

Защита ребенка в онлайновой среде в эру общедоступного широкополосного интернета является важнейшей проблемой, которая срочно требует глобальной скоординированной реакции. Хотя местные и даже национальные инициативы прочно заняли свое место, интернет не знает границ и международное сотрудничество могло бы стать ключом к нашему успеху и победе на поле предстоящей битвы.

Дети сами по себе, используя для доступа в интернет компьютеры и подвижные устройства, могут сделать очень многое, чтобы помочь нам одержать победу в борьбе против киберпреступлений и киберугроз, и я лично очень благодарен вам за вашу поддержку.

Д-р Хамадун И. Туре

Генеральный секретарь Международного союза электросвязи (МСЭ)

Краткое содержание

Информационное общество, в котором сегодня растут дети и подростки, предлагает возможности мгновенно погрузиться в цифровой мир, просто щелкнув мышкой. При помощи компьютера или подвижного устройства с доступом в интернет можно получить доступ к небывалому уровню услуг и информации. Преграды, связанные со стоимостью таких устройств и доступом в интернет, очень быстро исчезают. Все эти технические разработки предоставляют детям и молодым людям небывалые возможности для исследования новых границ и знакомства с людьми из далеких стран. Дети и подростки в полном смысле этого слова становятся гражданами цифрового онлайнового мира, который не имеет преград или границ.

Чаще всего эта возможность дает положительный и образовательный опыт: опыт, который может помочь младшим поколениям лучше понимать и отличия, и общие черты людей во всем мире. Однако детям и молодым людям необходимо знать также о некоторых потенциально негативных аспектах технологий.

Опасные действия могут включать в себя запугивание и притеснение, кражу идентичности и злоупотребления в онлайновой среде, например, дети просматривают опасный и незаконный контент, или являются объектами злонамеренного контакта с целью сексуального насилия, или создания, распространения и сбора материалов с сексуальной эксплуатацией детей.

Все это угрожает благополучию детей и молодых людей и ставит сложные задачи перед всеми заинтересованными сторонами, включая самих детей.

Несмотря на то, что все поставщики онлайновых услуг должны делать все от них зависящее на техническом уровне, чтобы сделать интернет максимально безопасным для детей и подростков, первая и лучшая форма защитить ТЕБЯ – это дать тебе возможность узнать обо всем, что может случиться в онлайновой среде, и понять, что у проблемы, которая может встретиться в онлайновой среде, всегда есть решение. Поэтому чрезвычайно важно вооружить детей и подростков, обучая их и повышая их осведомленность.


ABCDEFGHIJKLM
2345678901234567
LOVE LOVE LOVE LOVE
1 2 3

Данные Руководящие указания были подготовлены в рамках Инициативы по защите детей в онлайновой среде (COP)[1] с целью создания основы для безопасного и надежного кибермира не только для детей, живущих сегодня, но и для будущих поколений. Предполагается, что эти указания станут программой, которая может быть адаптирована и использована в соответствии с национальными или местными традициями и законами. Более того, как указано во вставке на странице 4, желательно чтобы эти Руководящие указания решали вопросы, которые могут затрагивать всех детей и подростков младше 18 лет, но каждая возрастная группа будет иметь разные потребности. И в самом деле, каждый ребенок уникален и заслуживает особого внимания.

Эти глобальные руководящие указания для детей и подростков были разработаны МСЭ и командой авторов из лидирующих учреждений, действующих в секторе МСЭ, например, "Спасем детей", Интерпол и Telefonica, CHIS и "В безопасной сети".

В Конвенции Организации Объединенных Наций по правам ребенка[2] и особенно итоговых документах ВВУИО определены потребности детей и подростков и их защита в киберпространстве. В Тунисском обязательстве признается "роль ИКТ в защите детей и расширении развития детей", а также необходимость "укрепить деятельность по защите детей от эксплуатации и защитить их права в контексте ИКТ".

Публикуя эти Руководящие указания, Инициатива COP призывает все заинтересованные стороны, включая детей и подростков, поддержать принятие правил и стратегий, которые защитят детей в киберпространстве и предоставят им безопасный доступ ко всем замечательным возможностям и ресурсам, доступным в онлайновой среде.

Мы надеемся, что это приведет не только к созданию более полного информационного общества, но также даст возможность странам выполнять свои обязательства по отношению к защите и реализации прав детей, как гласят Конвенция Организации Соединенных Наций по правам ребенка, принятая в соответствии с Резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 года, и Итоговый документ ВВУИО.

[1] www.itu.int/cop
[2] http://www.unicef.org/crc/


e
WWW

1. Базовая информация

Конвенция ООН по правам Ребенка, принятая Организацией Объединенных Наций в 1989 году, является наиболее важным и значительным правовым инструментом по защите и поддержке прав детей и подростков. Она сфокусирована на реальных потребностях не только в том, что касается уязвимости и мер защиты, но также и в том, что касается поддержки и оценки возможностей каждого отдельного ребенка и молодого человека.

Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО), которая проходила в два этапа в Женеве с 10 по 12 декабря 2003 года и в Тунисе с 16 по 18 ноября 2005 года, завершилась принятием Итоговых документов ВВУИО, в которых было принято твердое обязательство "построить ориентированное на интересы людей, открытое для всех и направленное на развитие информационное общество, в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими".

На ВВУИО главы международного сообщества, приняв Направление деятельности С5, поручили МСЭ: "Создавать уверенность и безопасность при работе с ИКТ". В итоговых документах ВВУИО также однозначно определяются потребности детей и подростков и их защита в киберпространстве. Тунисское Обязательство признало "роль ИКТ в деле защиты и содействия развитию детей", а также необходимость "активизировать деятельность по защите детей от растления и защитить их права в контексте ИКТ".

Более того, мировое сообщество детей и подростков заявило в итоговом документе III-ого Всемирного конгресса по борьбе с сексуальным насилием над детьми и молодыми людьми, прошедшем в 2008 году в Бразилии[3], следующее: "Мы хотим иметь четкие правила по кибербезопасности, пропагандируемые как при помощи веб-сайтов, так и внутри сообществ. С этой целью мы призываем к ускоренной разработке руководств для детей, учителей, родителей и семей, рассматривающих угрозы интернета дополнительно к предоставлению информации о сексуальной эксплуатации детей".

Онлайновые технологии предлагают множество возможностей для общения, получения новых навыков, творчества и участия в создании лучшего общества для всех, но зачастую они также могут нести новые риски, например, они могут подвергать детей и подростков таким возможным опасностям, как незаконный контент, вирусы, домогательство, например, в чатах, злоупотребление личной информацией и знакомство с целью сексуального насилия.

Для защиты детей в онлайновой среде не существует единственно верного решения. Это глобальная проблема, которая требует глобального решения всех слоев общества, включая самих детей и подростков.

3 http://www.ecpat.net/WorldCongressIII/PDF/Outcome/WCIII_Outcome_Document_Final.pdf

Ситуационное исследование: Голоса детей и подростков

III-й Международный конгресс по борьбе с сексуальным насилием над детьми и подростками проходил в Рио-де-Жанейро, Бразилия, с 25 по 28 ноября 2008 года. В нем приняло участие 3500 человек, включая 300 подростков, 150 из которых были иностранцами.

Он завершился принятием итогового документа "Декларация Рио-де-Жанейро по предотвращению и прекращению сексуального насилия над детьми и подростками", которая содержит "Декларацию подростков для прекращения сексуального насилия". Ниже приведено несколько основных посланий от детей и подростков всему миру:

Мы, дети мира, благодарим правительство Бразилии и другие правительства и ответственные организации за то, что нам, детям – настоящему и будущему этого мира, дали право голоса на этом III-м Международном конгрессе.

…

7 В настоящее время мы требуем правительственных действий по созданию законов и правил, направленных на то, чтобы приносить пользу, защитить и обеспечивать благополучие детей, как на местном, так и на международном уровне. Однако недостаточно просто позволить правительствам давать пустые обещания по борьбе с посягательством на детей. Поэтому мы, дети, требуем создать действенные комитеты для проверки планов действий в каждой стране.

8 Кроме того, мы призываем к объявлению Международного дня, когда дети возглавят деятельность в рамках кампаний, слетов и маршей по повышению осведомленности. Для расширения сферы действий в этот день мы призываем организовать Международный конкурс рисунка, литературных произведений и художественной речи, которые станут кульминацией этого дня.

9 Теперь мы обращаем свое внимание на средства информации и, особенно, на интернет, который представляют собой одну из самых больших угроз миллионам детей по всему миру.

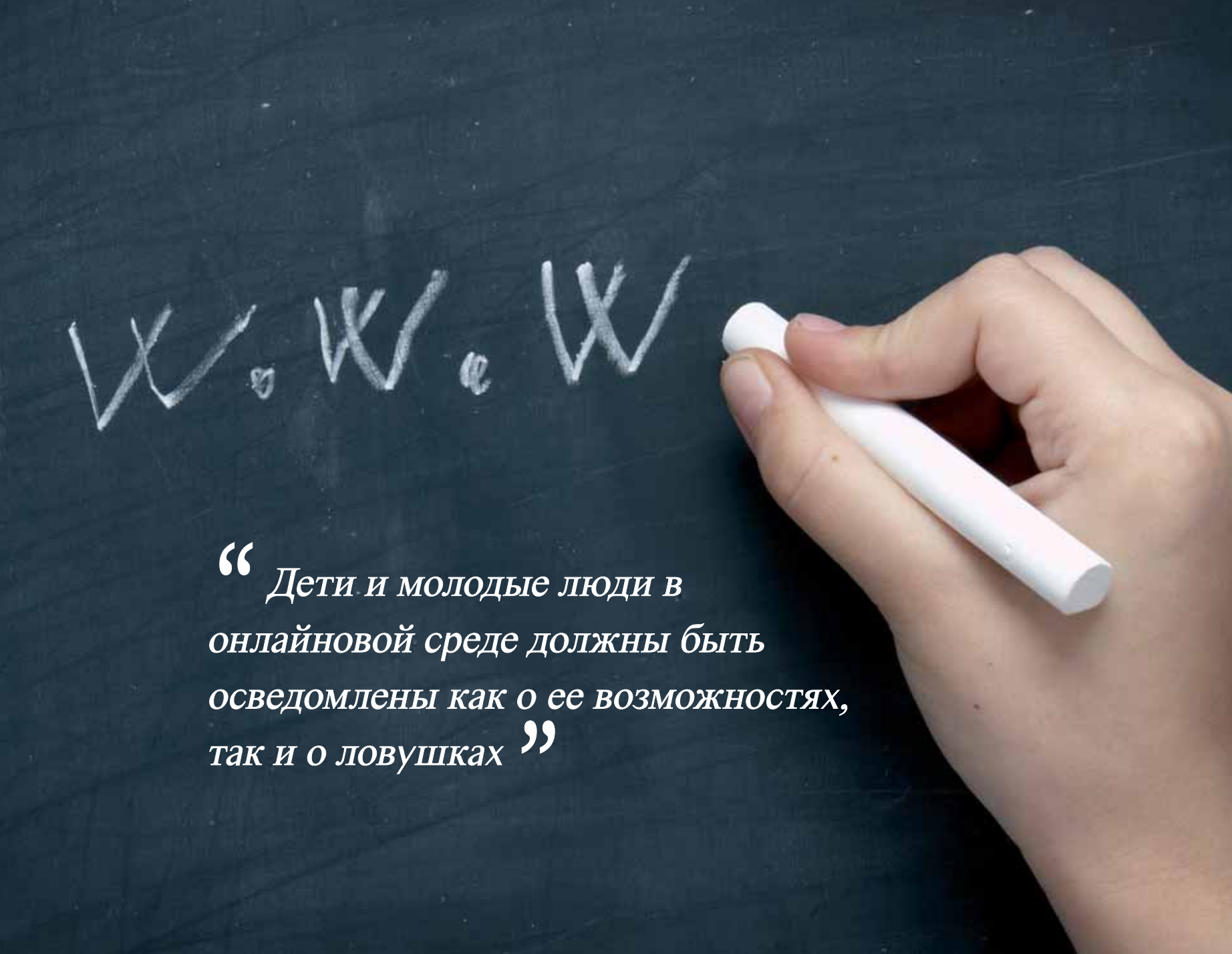
10 Мы, дети, должны информировать правительства о нашем положении с тем, чтобы добиться создания строгого и действенного законодательства в том, что касается интернета, особенно, детской порнографии, которая является всего лишь еще одной формой насилия.

11 Также мы требуем создания твердых правил по кибербезопасности, распространяемых как на веб-сайтах, так и в рамках сообществ. С этой целью мы призываем к ускоренной разработке руководств для детей, учителей, родителей и семей, рассматривающих угрозы интернета дополнительно к предоставлению информации о сексуальной эксплуатации детей.

12. Далее поручаем средствам информации собрать документы, отчеты, папки, CD, видеоролики и другие материалы с целью повышения осведомленности по этому вопросу. Мы, дети мира, даем обещание строго и принципиально следовать этим правилам и будем призывать наши правительства к действию, если мы не увидим, что предпринимаются положительные меры для прекращения этого явления, которое продолжает уродовать мир сегодня.

...

"Декларация для прекращения сексуального насилия" размещена по адресу: http://www.iiicongressomundial.net/congresso/arquivos/Rio%20Declaration%20and%20Call%20for%20Action%20-%20FINAL%20Version.pdf



“ Дети и молодые люди в онлайновой среде должны быть осведомлены как о ее возможностях, так и о ловушках ”

2. Дети и молодые люди в онлайновой среде

Информационно коммуникационные технологии (ИКТ) меняют способ общения детей со сверстниками, способ доступа к информации, способ выражения мнений, способ размещения и совместного использования творческого контента. В высшей степени интерактивный характер многих услуг интернета особенно нравится детям и молодым людям. В целом интернет для детей – это место, где они чувствуют себя в безопасности, то, что им нравится, нечто интересное, развлекательное, приятное, полезное и дружелюбное[4].

Доступ

Исследование, проведенное в Дании, показало , что по мере того как "дети взрослеют, частота использования ими интернета растет. 19% опрошенных в возрасте 9–10 лет пользуются интернетом каждый день. Для сравнения, интернетом ежедневно пользуются 80% опрошенных в возрасте 14–16 лет". Похожая тенденция наблюдается в Сингапуре , где, согласно отчетам, 56% детей в возрасте 5–14 лет, выходят в он-лайн ежедневно. Выясняется, что чаще всего в интернете ищут информацию, связанную с хобби и личными интересами, играют в игры и проводят исследования для выполнения домашних заданий.

[4] http://www.childresearch.

[5] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0409/digital_life.htm

[6] http://www.itu.int/ITU-D/ict/material/Youth_2008.pdf (page 62)


ODPOVĚĎ
POMOC
7
SI
6
LA
5
SOL
4
FA
Gg
AKT 7
Ff
AKT 6
Fe
AKT 5
Oo

В развитых странах широкодоступный фиксированный широкополосный доступ в интернет до сих пор является наиболее предпочтительным способом выйти в онлайновый режим, в сравнении с развивающимися странами, где такая инфраструктура развита более слабо. Здесь основным способом выхода в интернет остается и будет оставаться мобильный доступ. Во многих странах важными поставщиками доступа для детей и молодых людей также являются интернет-кафе и другие коллективные ресурсы. Так, скорее всего, и останется в течение некоторого времени. В Европейском союзе 50% детей в возрасте 10 лет, 87% в возрасте 13 лет и 95% 16-летних детей имеют мобильный телефон[7]. В Азиатско-Тихоокеанском регионе, самом быстроразвивающемся регионе по числу абонентов подвижных услуг, Китай и Индия стали лидерами в области технологии, при этом рост составляется в шесть миллионов мобильных телефонов в месяц только в одной Индии[8]. В настоящее время насчитывается четыре миллиарда абонентов подвижной связи в мире, из них почти 100 миллионов имеют возможность подвижной широкополосной связи[9]. Очевидно, что возможность доступа к онлайновым услугам будет все больше осуществляться через портативные устройства.

Преимущества очевидны: в удаленных деревнях и общинах при помощи портативных устройств детям может быть предоставлено множество образовательных услуг. Мобильные телефоны могут служить важным средством, помогающим детям общаться с другими детьми в рамках образовательной и познавательной деятельности. Это особенно важно для общин, которые либо ведут кочевой образ жизни, либо были вынуждены сняться с места из-за стихийных бедствий, войн, в том числе гражданских, или других крупных разрушитель-

Цифровые устройства

Недавнее исследование, проведенное в латиноамериканских домах, показало, что самое молодое поколение имеет хорошее оборудование[10]. Кроме компьютеров и сотовых телефонов доступ в интернет могут предоставить, или вскоре смогут это предоставить, множество других электронных устройств. Ниже приведен набор устройств, которые участники исследования имеют у себя дома:

Устройства в доме	Группа в возрасте 6–9 лет	Группа в возрасте 10–18 лет
Домашний компьютер	61%	65%
Соединение с интернетом	40%	46%
Личный сотовый телефон	42%	83%

7 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/596

8 http://www.tigweb.org/express/panorama/article.html?ContentID=11441

9 http://gsmworld.com/newsroom/press-releases/2009/2521.htm#nav-6

10 http://www.generacionesinteractivas.org/?page_id=660

Информация

Доступ к информации важен для детей и молодых людей при выполнении домашних заданий. Исследования, посвященные использованию интернета японскими детьми[11], показали, что для выполнения домашних заданий 70% детей используют интернет. Библиотека перешла в онлайновый формат, и возможность поиска и обнаружения соответствующей и надежной информации на любом языке является важным преимуществом, которое приветствуется молодым поколением по всему миру. Одним из наиболее часто используемых онлайновых ресурсов является Википедия[12]. Википедия – это многоязычный, энциклопедический веб-проект с бесплатным контентом, где вы можете читать, редактировать и писать статьи по любой теме или вопросу, который вам кажется значимым. Упражнения по поиску фактов легко могут провести вас с одной страницы на другую и так далее. Поиск новой информации никогда не надоедает, и в условиях растущей локализации контента языковые барьеры понемногу исчезают.

Социальные сети

Создание онлайновых социальных сетей иметь большой успех. Разнообразие социальных сетей удовлетворяет потребности всех возрастов, культур и языков. Иметь профиль в социальной сети стало важной частью жизни в онлайновой среде для многих детей и молодых людей. Возвращаясь домой из школы, дети имеют возможность продолжить общение со своими друзьями в он-лайне, пока они делают домашнюю работу, отправлять SMS и слушать музыку (часто одновременно!) – эта картина, знакомая многим. Социальные сети часто могут представлять собой единый доступ к играм, друзьям, новостям, музыке и средствам самовыражения. Другими словами, вы можете творить, веселиться, размышлять и развлекаться при помощи ИКТ.

В качестве примера можно привести группу молодых исполнителей, которая пишет новую песню, помещает ее на страничке MySpace[13] и сообщает об этом своим друзьям и поклонникам. Теперь поклонники могут прослушать эту песню в виде потокового аудио в он-лайне или скачать ее на свои mp3-плееры или мобильные телефоны и слушать ее в пути. Если им понравится эта песня, они будут распространять информацию о ней, рассказав своим друзьям, которые, в свою очередь, расскажут своим и так далее. При помощи простых методов и небольших финансовых вложений эта группа теперь может приобрести большую аудиторию поклонников, и возможно ее услышит звукозаписывающая компания, которая пожелает заключить с ними контракт. Имеется множество историй о группах, продвигающих свои песни при помощи услуг, наподобие MySpace, и в конце концов заключающих контракт. Эта ситуация мало отличается от реального мира, но возможность приобрести больше слушателей за более короткое время является одним из главных преимуществ ИКТ. В сущности, такая услуга может медленно раскручиваться, но достигает критической мировой массы за очень короткое время, благодаря тому, что дети и молодые люди постоянно делятся впечатлениями с друзьями.

Виртуальные миры для детей и подростков

В этих мирах дети часто создают свой аватар и с его помощью исследуют воображаемую вселенную. Они могут играть в игры, общаться и украшать виртуальные комнаты или другие пространства. К концу 2009 года, со-

11 http://www.childresearch.net/RESOURCE/RESEARCH/2008/KANOH2_1.HTM

12 http://en.wikipedia.org/wiki/Main_Page

13 http://www.myspace.com/

гласно исследованиям консалтинговой фирмы K Zero, в виртуальных мирах, предназначенных для детей младше 16 лет, будет более 70 миллионов уникальных учетных записей.

Компания по исследованиям информационных и коммерческих событий Virtual Worlds Management считает, что в настоящее время "существуют, планируются или активно разрабатываются"[14] более 200 виртуальных миров, ориентированных на молодежь.

Виртуальные миры, например, Habbo hotel[15], которые ориентированы на подростков, позволяют пользователям создавать профиль и представлять себя в виртуальном мире посредством аватара[16]. Все пользователи создают свои собственные аватары при помощи простых в использовании инструментов. Возможность представать в виде аватара позволяет каждому, вне зависимости от того, как он выглядит в реальном мире, войти в сообщество, где все равны и не существует предубеждений.

Применение такой новой идентичности может дать пользователю возможность выразить себя другим способом, попробовать новый профиль или отношение, быть упрямым и честным в важных для них вопросах или даже пожить немного "чужой" жизнью.

Нет необходимости говорить, что существуют правила, которые следует соблюдать, но возможность примерить другую личность может быть забавной.

Каков твой онлайновый профиль?

Интересное исследование[17], проведенное с пользователями Habbo Hotel, показало существование следующих типов онлайновых цифровых профилей подростков:

Стремящиеся к достижениям	Амбициозные, сильные духом и материалистичные. Они ценят материальный успех и, хотя имеют множество друзей, не обращают на чувства других такое внимании, как остальные сегменты
Бунтари	Больше всего ценят получение впечатлений от жизни и наслаждаются быстрым ритмом жизни. Как и Стремящиеся к достижениям хотят стать "богатыми и знаменитыми", но не хотят жертвовать удовольствиями для достижения этой цели
Консерваторы	Более всего ценят обычную жизнь и считают себя честными, воспитанными и послушными. Они стремятся помогать другим, но менее амбициозны и меньше стремятся к удовольствиям, чем другие
Творцы	Имеют многие положительные черты консерваторов, но направлены на творчество. Они ценят хорошее образование и влияние в жизни, но они также активны, общительны и интересуются путешествиями
Одиночки	Более направлены в себя и менее других связаны с определенными личными чертами. Они редко видят себя активными или уверенными в себе, но имеют более восприимчивый ум в своих устремлениях, если сравнивать с Консерваторами или Стремящимися к достижениям

[14] http://www.nytimes.com/2009/04/19/business/19proto.html?_r=1&emc=eta1

[15] http://www.habbo.com/

[16] Avatars in video games are essentially the player's physical representation in the game world http://en.wikipedia.org/wiki/Avatar_(computing)

[17] http://www.sulake.com/press/releases/2008-04-03-Global_Habbo_Youth_Survey.html

Дети и подростки имеют онлайновые профили и общаются друг с другом, размещая комментарии или приветствия на страницах своих друзей. Наличие множества друзей, связанных с чьим-либо профилем, как выясняется обеспечивает высокий статус среди ровесников, хотя возникает вопрос, стоит ли стремиться к тому, чтобы просто иметь большое количество друзей в онлайне. Тем не менее, 74% юных датчан в возрасте 14–16 лет утверждают, что они оставляли свои комментарии в онлайновых профилях других людей[18], похожая тенденция наблюдается на всех международных сайтах социальных сетей, например, Facebook[19], Hi5[20] и Bebo[21], где большая часть взаимодействий относится к размещению комментариев в профилях других людей.

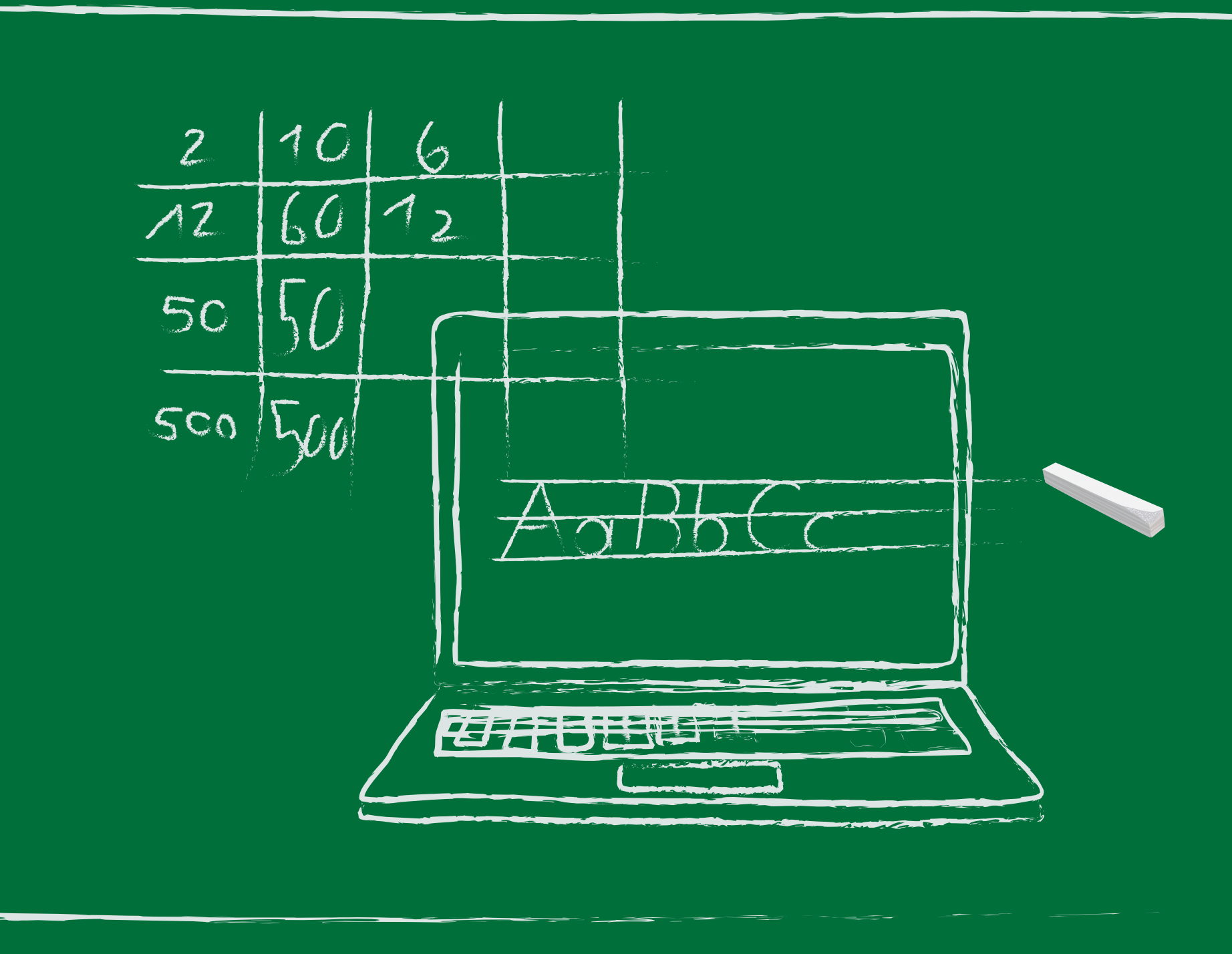
Многие социальные сети допускают создание подгрупп по различным темам, например, демократия, игры, домашние любимцы, школьные занятия, музыка и тому подобное. Таких сообществ может не быть в вашем городе, регионе, стране, но опять же, ИКТ сворачивают мир и доставляют его на ваш экран, и предлагают вам возможность экспериментировать с формами участия и свободы самовыражения, которые редко можно встретить в реальной повседневной жизни во взрослом мире. Положительная культура, царящая в онлайновых сообществах, помогает каждому приобрести хороший опыт и увеличивает готовность общения с людьми в онлайновой среде и обучение новым вещам.

[18] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0409/digital_life.htm

[19] http://www.facebook.com/

[20] http://hi5networks.com/

[21] http://www.bebo.com/


2 10 6
12 60 12
50 50
500 500
AaBbCc

Ситуационное исследование: Положительные стороны социальных сетей для детей с затруднениями в учебе

Положительное влияние социальных сетей для детей с затруднениями в учебе может быть описано следующим образом[22]:

Обучение навыкам общения: вы получаете шанс познакомиться в онлайновой среде с разными людьми. Так как общение при помощи технологий не имеет той спонтанности, как личное общение или разговор по телефону, у вас есть немного больше времени, для того чтобы обдумать ситуацию прежде, чем отвечать. Это возможность для вас, чтобы поэкспериментировать с приветствиями, ответами и пр.

Заданное/управляемое социальное взаимодействие: тогда как технологии онлайнового общения все в большей степени позволяют взаимодействовать в свободной форме, с целью обеспечения безопасности круг социального взаимодействия можно сузить. Примерами направленного взаимодействия в онлайновой среде служат списки приятелей/друзей, модерируемые чаты или тематические форумы, а для маленьких детей еще и возможность, предоставляемая родителям помочь ребенку, печатая или читая в течение некоторого времени. Это поможет детям приобрести навыки и уверенность, которые укрепят их независимость по мере их взросления.

Эксперименты с идентичностью: в онлайновой среде ребенок может создать идентичность, которая будет отличаться от того, что он или она обычно из себя представляет. Например, ребенок, на самом деле любящий комиксы, в онлайновой среде может быть "королем всех знаний супергероев", и его не будут дразнить в школе. Такой ребенок также может найти в онлайновой среде группу сверстников, которые будут ценить именно эту его или ее сторону.

Частое использование существующих и развивающихся/изменяющихся технологий. Сегодня технология развивается быстрее, чем когда-либо раньше. Когда вы научитесь применять новые технологии (или новые приложения существующих технологий), вы будете лучше готовы к применению технологий будущего. Это поможет вам быстро оценивать риски этих новых способов общения и изменить свои действия так, чтобы сохранять контроль над своей собственной безопасностью.

22 http://www.greatschools.net/cgi-bin/showarticle/3120

Игры

Классические настольные игры также перебрались в он-лайн, и теперь они известны, как "Многопользовательские ролевые онлайн-игры" (MMORPG). Как и в случае с социальными сетями, онлайновые игры могут соединить вас с другими игроками по всему миру. Это такой вид социальной деятельности, которая захватывает вас полностью. Термин "онлайновый игрок" может напомнить об одиноком подростке, который играет в "EverQuest" в подвале родительского дома, но этот образ совершенно отличается от того, что мы видим в Южной Корее. Взаимодействие в группе является в этой стране мощной культурной традицией так же, как обучение и поход по магазинам. Молодые люди идут в компьютерные клубы, чтобы выпустить пар и пообщаться. "Игровые сообщества на самом деле популярны, как и возможность создавать группы или гильдии", – говорит Луонг. "Эти социальные аспекты являются важной причиной, по которой люди продолжают играть в игры [в Южной Корее][23]."

Цифровое гражданство

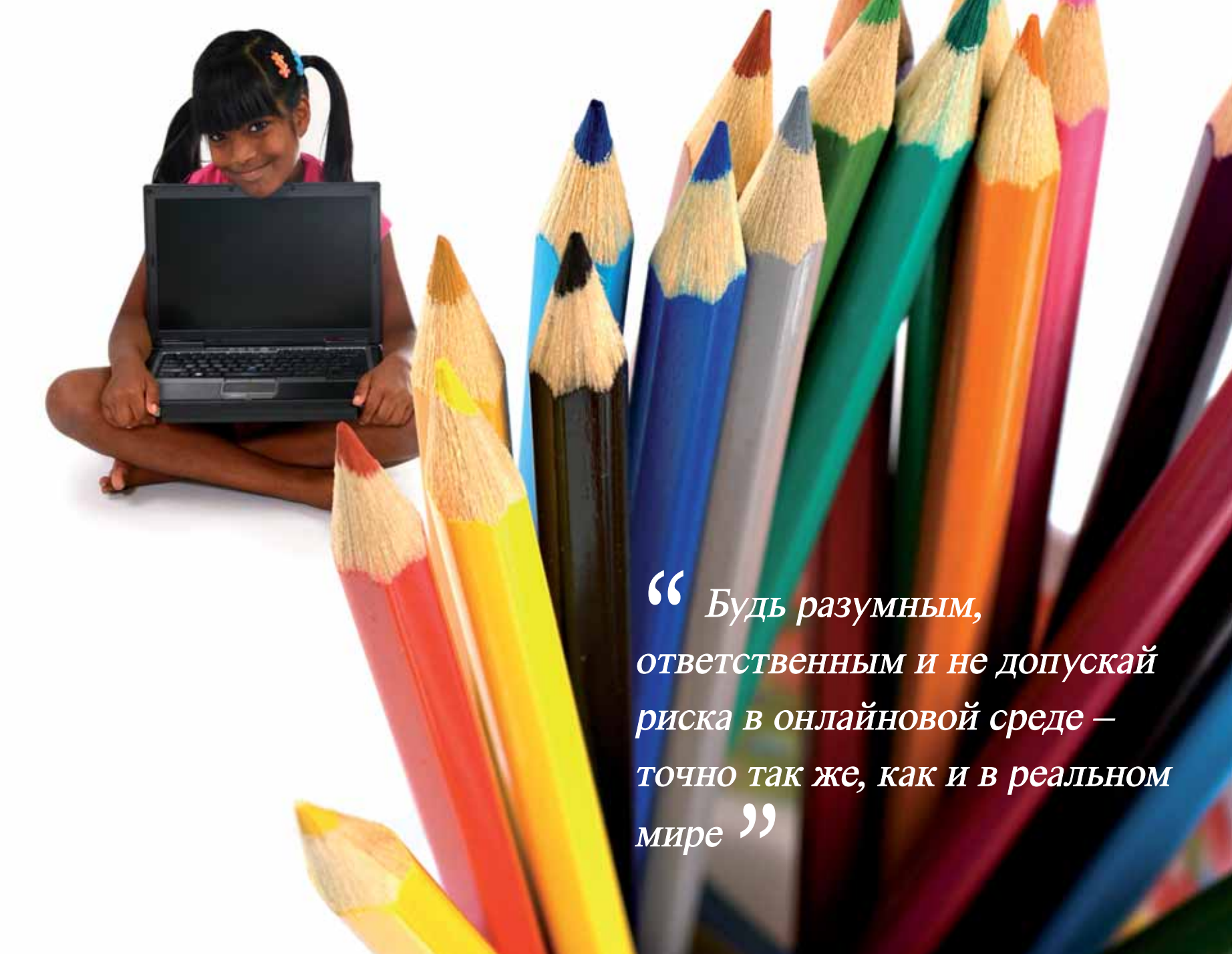
Введение новых технологий часто вызывает необходимость понимания того, как правильно их использовать. Все мы, включая детей и молодых людей, можем потребовать, чтобы производители и поставщики встроили в технологии как можно больше функций безопасности, позволяя нам делать осознанный выбор по вопросам, например, раскрытия частной информации. Однако основная ответственность за правильные и уважительные действия в онлайновой среде ложится на детей и молодых людей. Все чаще начинает использоваться термин "цифровое гражданство". Цифровое гражданство служит не только для распознавания и борьбы с опасностью в онлайновой среде. Оно служит для создания безопасных пространств и сообществ, понимания того, как управлять персональной информацией и как овладеть знаниями об интернете, используя свое присутствие в онлайновой среде для расширения и формирования своего мира безопасными, творческими способами и вдохновлять людей делать то же самое[24].

Празднование безопасного интернета

Приятное и безопасное использование интернета празднуется по всему миру ежегодно. В таком празднике могут участвовать дети, местная школа, промышленность и соответствующие участники рынка, сотрудничающие в деле создания большей осведомленности о возможностях продвижения положительного опыта в онлайновых действиях. Самую свежую информацию о таких событиях можно найти в поисковых машинах, используя поиск с запросами типа "празднование безопасного использования интернета" + "название страны".

[23] http://www.msnbc.msn.com/id/17175353/

[24] http://www.digizen.org/



“ Будь разумным, ответственным и не допускай риска в онлайновой среде – точно так же, как и в реальном мире ”

Вот список вопросов, которые следует иметь в виду при обсуждении "Цифрового гражданства"

Цифровой этикет: электронные стандарты поведения или процедуры.

- Недостаточно создать правила и указания, мы должны научиться быть ответственными цифровыми гражданами в этом новом обществе.

Цифровое общение: электронный обмен информацией.

- Каждый должен иметь возможность доступа к информации всегда и везде.

Цифровая грамотность: процесс обучения и изучения технологий и использования технологий.

- С появлением новых технологий, нам необходимо научиться использовать эти технологии быстро и надлежащим образом. Нам необходимо овладеть цифровой грамотностью.

Цифровой доступ: полностью электронное участие в деятельности общества.

- Исключение из цифрового отражения любого вида не ведет к увеличению числа людей в электронном обществе. Ни один пол не должен иметь преимущества перед другим. Электронный доступ не должен делиться по расовым, физическим или умственным различиям. Следует также уделить внимание проблемам людей в крупных и малых городах с ограниченными потребностями в соединении. Для того чтобы стать эффективными гражданами, мы должны иметь равный цифровой доступ.

Цифровая коммерция: покупка и продажа товаров в электронной форме.

- Дети и молодые люди должны научиться быть эффективными потребителями в условиях безопасной цифровой экономики.

Цифровое законодательство: электронная ответственность за действия и поступки.

- Цифровое законодательство имеет дело с этикой технологии. В обществе существуют определенные правила, которые относятся к противоправным действиям. Эти законы применимы к каждому, кто работает или играет в онлайновой среде.

Цифровые права и обязанности: эти свободы относятся ко всем в цифровом мире.

- В цифровом мире должны быть рассмотрены, обсуждены и поняты основные цифровые права. С этими правами приходят и обязанности. Пользователи, включая детей и молодых людей, должны помочь в определении того, как должна правильно использоваться технология. В цифровом обществе эти два аспекта должны работать вместе и для каждого, чтобы обеспечить эффективность.

Цифровая безопасность (самозащита): электронные меры предосторожности для обеспечения безопасности.

- В любом обществе существуют люди, которые воруют, портят собственность или разрушают жизни других людей. То же самое справедливо и для цифрового общества. Для вашей собственной безопасности недостаточно просто доверять своим согражданам в обществе. В наших собственных домах мы ставим замки в двери и пожарную сигнализацию, чтобы обеспечить определенный уровень защиты. Для обеспечения безопасности и цифровой защиты то же самое необходимо сделать и в цифровом мире. Нам необходима защита от вирусов, резервное копирование данных и усиление контроля за нашим оборудованием. Как ответственные граждане мы должны защищать нашу информацию от внешних сил, которые могут вызвать ее разрушение или причинить ей ущерб.

Источник: http://www.digitalcitizenship.net/Nine_Elements.html

“ Все дети и молодые люди всего мира имеют право на безопасное пребывание в онлайновой среде ”

3. Что ты должен знать, чтобы оставаться в безопасности, находясь в онлайновой среде

Руководящие указания по безопасному использованию интернета

Сообщения по вопросам безопасности в интернете должны быть своевременными, соответствующими возрасту, с учетом культурных особенностей, а также соответствовать ценностям и законам общества, в котором живет ребенок или молодой человек.

Инициатива COP определила три основные возрастные группы молодых пользователей интернета. Эти группы в целом соответствуют ключевым этапам развития ребенка на его пути к совершеннолетию. Таким образом, эти руководящие указания можно рассматривать как лестницу, которая ведет вас через все этапы развития. Однако мы не можем еще раз не подчеркнуть, что каждый ребенок отличен от других, и требует, и заслуживает особого внимания. Один размер не подходит всем. Ничто не должно всегда считаться или восприниматься как должное.

Первая возрастная группа: 5–7 лет

Эта группа получает свой опыт взаимодействия с технологией. Ее использование должно все время внимательно контролироваться одним из родителей или взрослым. Фильтрующее программное обеспечение или другие технические средства могут также быть чрезвычайно полезны в содействии использования интерне-

та ребенком этого возраста. Было бы целесообразно рассмотреть вопрос об ограничении потенциального доступа таких маленьких детей к интернету, например, путем создания списка безопасных веб-сайтов, которые подходят данному возрасту, создавая нечто подобное огороженному стеной саду. Цель состоит в том, чтобы научить данную возрастную группу основам безопасности в интернете, этикету и пониманию. Данная возрастная группа вероятно не сможет понять более сложные сообщения. Родителям и взрослым, которые несут ответственность за детей, следует обратиться к руководящим указаниям COP для родителей, опекунов и учителей, где они смогут увидеть, как наилучшим образом помочь самой младшей возрастной группе сохранить безопасность в онлайновой среде.

Вторая возрастная группа: 8–12 лет

Этот возрастной промежуток является сложным переходным возрастом для ребенка. Обычно он или она становятся молодыми людьми, способными задавать массу вопросов. Их любопытство в поисках ответов на вопросы начинает толкать их к поискам проблем и попыткам сломать существующие границы. У этой возрастной группы уже есть понимание того, с чем можно ознакомиться в интернете. Импульс искать и найти что-то необыкновенное – очень велик. На протяжении всего детства ребенок должен проверять барьеры на прочность и развиваться в ходе такого обучения. Фильтрующее программное обеспечение или другие технические средства могут также быть чрезвычайно полезны в содействии использования интернета ребенком этого возраста. Важным аспектом этой возрастной группы является порой некритичный подход к содержанию и контактам, что может сделать данную возрастную группу особенно уязвимой для преступников и коммерческих организаций, желающих привлечь их.

Последняя возрастная группа: 13 лет и больше

Эта группа охватывает большой промежуток времени, а также состоит из молодых людей, главным образом, подростков. Дети этой группы быстро взрослеют, переходя от возраста молодых людей к возрасту молодых взрослых. Они развиваются и изучают свою собственную личность, свои собственные вкусы. Очень часто они используют технологии с высоким уровнем профессионализма без какого-либо надзора со стороны взрослых и без какого-либо взаимодействия с ними. Фильтрующее программное обеспечение становится менее полезным и менее актуальным, но оно, конечно, могло бы продолжать играть важную вспомогательную роль, особенно для некоторых молодых людей, которые могут быть временно или долговременно уязвимы.

Связанные со своим собственным гормональным развитием и растущим чувством физической зрелости, подростки могут пройти через те этапы, когда они чувствуют очень сильную потребность поиска своего собственного пути, избегая пристального надзора со стороны родителей или взрослых и искать своих сверстников. Природное любопытство в сексуальных вопросах может привести некоторых людей этой возрастной группы к потенциально опасным ситуациям, что делает для них еще более важным понимание того, как обезопасить себя в онлайновой среде.

Руководящие указания COP признают, как трудно создать инструкции, которые будут охватывать все потребности всех возрастов в пределах определенных групп. Местные законы и обычаи также очень важны в вопросах такого рода.

Не существует единого подхода, который подходил бы всем. Инициатива Защита ребенка в онлайновой среде готова оказать помощь в адаптации и локализации содержания этих или любых других Руководящих указаний COP. Если вы желаете присоединиться, предлагаем вам написать по адресу: cop@itu.int.


SMART

"Разумные" правила

Использование интернета – это радость. Получай максимум удовольствия, сохраняя свою безопасность.

1 В интернете ты можешь найти много интересного. Ты можешь играть в игры, ты можешь общаться с друзьями, встретить новых друзей и найти много полезной информации. Ты имеешь право пользоваться им и изучить все, что может предложить тебе цифровой мир!

2 Но ты должен знать также, что можешь встретить в интернете некоторые неприятные вещи, например, картинки и истории, которые могут смутить или даже напугать тебя. В этом цифровом мире существуют не только твои друзья и взрослые, которым можно доверять. К сожалению, интернет также используется людьми, которые совсем не такие хорошие или которые могут даже стремиться к тому, чтобы навредить тебе, преследовать или запугивать тебя или других людей. Используя интернет, ты должен знать некоторые основные правила, которые позволят тебе защитить себя и других.

3 Ты имеешь право безопасно использовать интернет и установить свои собственные рамки. Будь разумным, ответственным и не иди на риск в онлайновой среде, а также в реальной жизни!

Руководящие указания для детей и молодых людей

Установи свои рамки

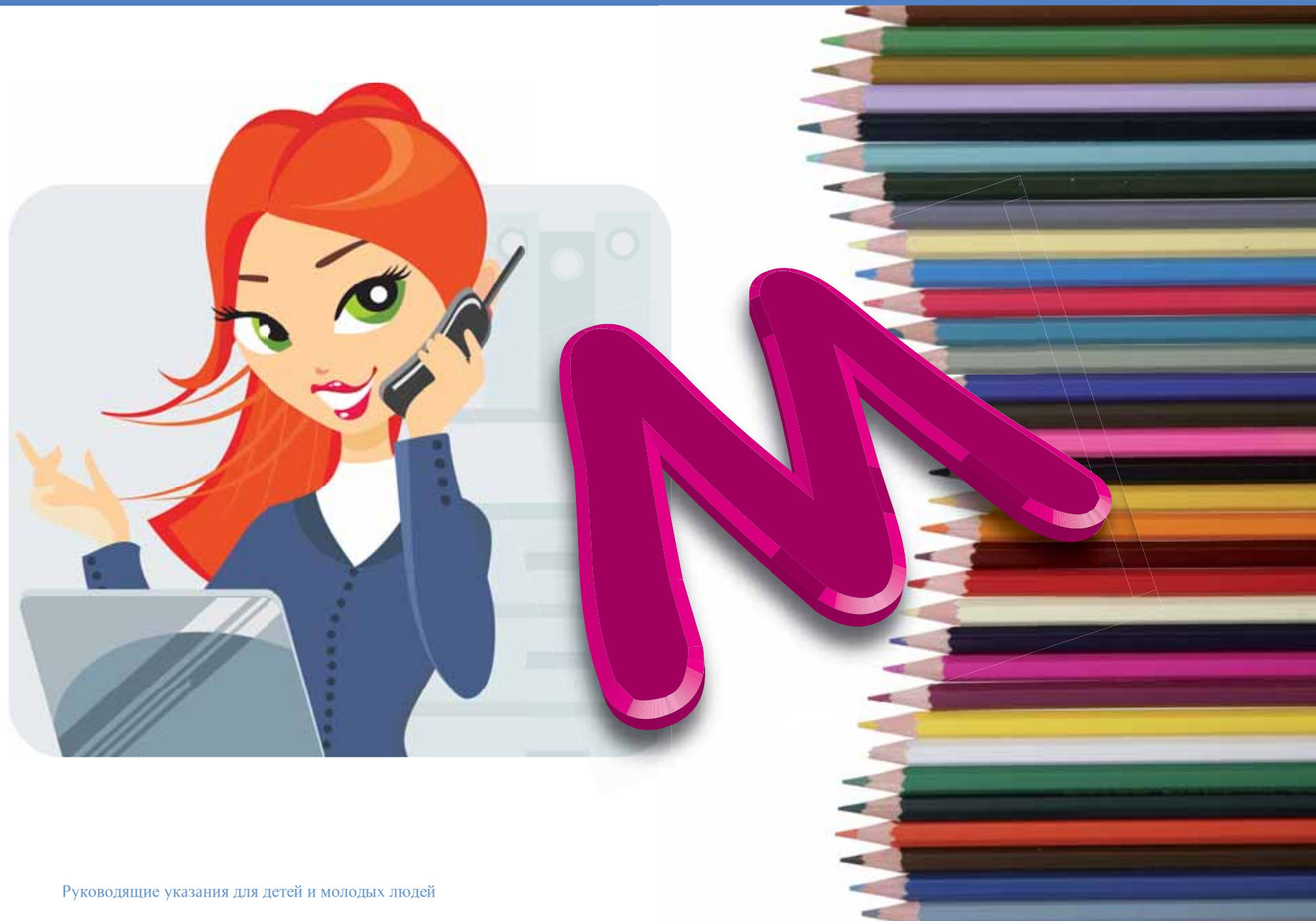
1 Позаботься о своей конфиденциальности. Используя либо социальные сети, либо любую другую онлайновую услугу, позаботься о своей конфиденциальности и конфиденциальности своей семьи и друзей. У тебя может возникнуть чувство того, что ты действуешь анонимно в онлайновой среде, но, сбор информации из различных источников в онлайновой среде, может раскрыть слишком много личной информации о тебе самом или других, с кем ты близок, включая твою семью.

2 Если ты присоединился к сайту социальной сети, используй настройки конфиденциальности, для того чтобы защитить твой онлайновый профиль так, чтобы только твои друзья могли видеть его. Везде, где возможно, вместо своего реального имени ты должен использовать ник, чтобы только твои настоящие друзья могли узнать тебя. Другие интерактивные услуги, например, обмен мгновенными сообщениями, также предоставят инструменты защиты конфиденциальности. Используй их.

3 Дважды подумай прежде, чем разместить или рассказать о чем-нибудь в онлайновой среде. Готов ли ты рассказать об этом всем, кто находится в он-лайне: твоим близким друзьям, а также посторонним? После размещения информации, фотографий или любого другого материала в интернете ты никогда не сможешь удалить его или помешать другим людям использовать его. Ты никогда не сможешь узнать наверняка, где он будет использоваться, в конце концов.

4 Отнесись критично: не все является тем, чем кажется. К сожалению, если это кажется слишком хорошим, чтобы быть правдой, то так на самом деле и есть. Всегда дважды проверяй информацию из других надежных источников.

5 Ты имеешь права – и ты, и другие люди, должны уважать их. Ты никогда не должен терпеть преследования или запугивания со стороны других людей. Законы и уважение достойного и приемлемого поведения действуют и в онлайновой среде, и в реальной жизни.



Встреча онлайновых друзей в реальной жизни

1 Иногда онлайновые контакты перерастают в дружбу.

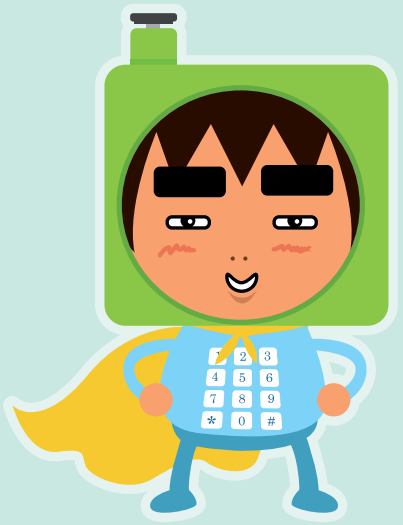
2 Подумай дважды, прежде чем встречаться с онлайновым другом в реальной жизни. Если ты все еще хочешь встретиться с онлайновый другом в реальной жизни, ты всегда должен позвать с собой кого-то надежного. Ты должен попросить родителей или другого взрослого, которому доверяешь, пойти с тобой, для того чтобы избежать любой проблемы в случае, если встреча обернется разочарованием.

3 Имей в виду, что твой онлайновый друг может оказаться совсем другим человеком, не таким, каким ты его или ее представлял.

Принятие приглашений/дружбы

1 Большинство людей, с которыми ты общаешься в онлайновой среде, вероятно уже являются твоими друзьями в реальной жизни. Ты также можешь быть связан с друзьями твоих друзей. Очень часто это может быть забавным, но в то же время, если ты сам не знаешь фактически кого-то, готов ли ты действительно считать его "другом" и поделиться с ним точно такой же информацией, какой ты делишься со своими старыми и лучшими друзьями?

2 Посредством онлайнового общения ты можешь общаться с людьми, ранее тебе неизвестными. Ты можешь получать просьбы от незнакомцев, которые хотели бы, чтобы ты включил их в твой список контактов и иметь возможность видеть твой профиль, но тебе не стоит принимать их. Нет ничего плохого в том, чтобы отклонить приглашения, если ты в них не уверен. Получение большего количества контактов не является целью общения в социальной сети.



Реагируй

1 Защити себя от неприятного или тревожного контента. Не заходи на эти сайты и не делись ссылками на такие сайты. Если ты видишь, что что-то тебя беспокоит, обсуди это с родителями или с кем-то, кому ты доверяешь.

2 Игнорируй плохое поведение и уйди от неприятных разговоров или сайтов с некорректным содержанием. Как и в реальной жизни, существуют люди, которые по каким-то причинам ведут себя агрессивно, оскорбительно или провокационно по отношению к другим, или которые хотят поделиться вредоносным содержанием. Обычно лучше всего игнорировать их и затем блокировать.

3 Заблокируй любого, кто обращается к тебе, используя грубые, навязчивые или угрожающие электронные письма или контент. Даже если сообщение может беспокоить тебя или ставить в неудобное положение, ты должен сохранить его, для того чтобы показать, если нужно, взрослому для получения совета. Ты – не единственный, кто стыдится такого содержания сообщения.

4 Всегда будь начеку, если кто-то, особенно незнакомец, хочет поговорить с тобой о сексе. Помни, что ты никогда не можешь быть уверенным в истинной сущности человека или намерений этого лица. Обращение к ребенку или молодому человеку с сексуальными намерениями всегда является серьезным поводом для беспокойства, поэтому ты должен рассказать об этом взрослому, которому доверяешь, для того чтобы ты и взрослый, которому ты доверяешь, могли сообщить об этом.

5 Если тебя заманили или привлекали обманом к совершению действий сексуального характера или к передаче сексуальных изображений с тобой, ты всегда должен рассказать взрослому, которому доверяешь, для того чтобы получить совет или помощь. Ни один взрослый не имеет права требовать от ребенка или молодого человека каких-то вещей с таким специфическим характером – ответственность всегда лежит на взрослом!


Т

Расскажи кому-нибудь о твоих проблемах

1 Если у тебя возникли любые вопросы или проблемы в то время, когда ты находишься в онлайновой среде, тебе необходимо рассказать об этой кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Нет таких проблем, которые были бы настолько большими, что их нельзя было бы решить! Ты можешь также обратиться к детскому телефону доверия[25], имеющемуся в твоей стране.

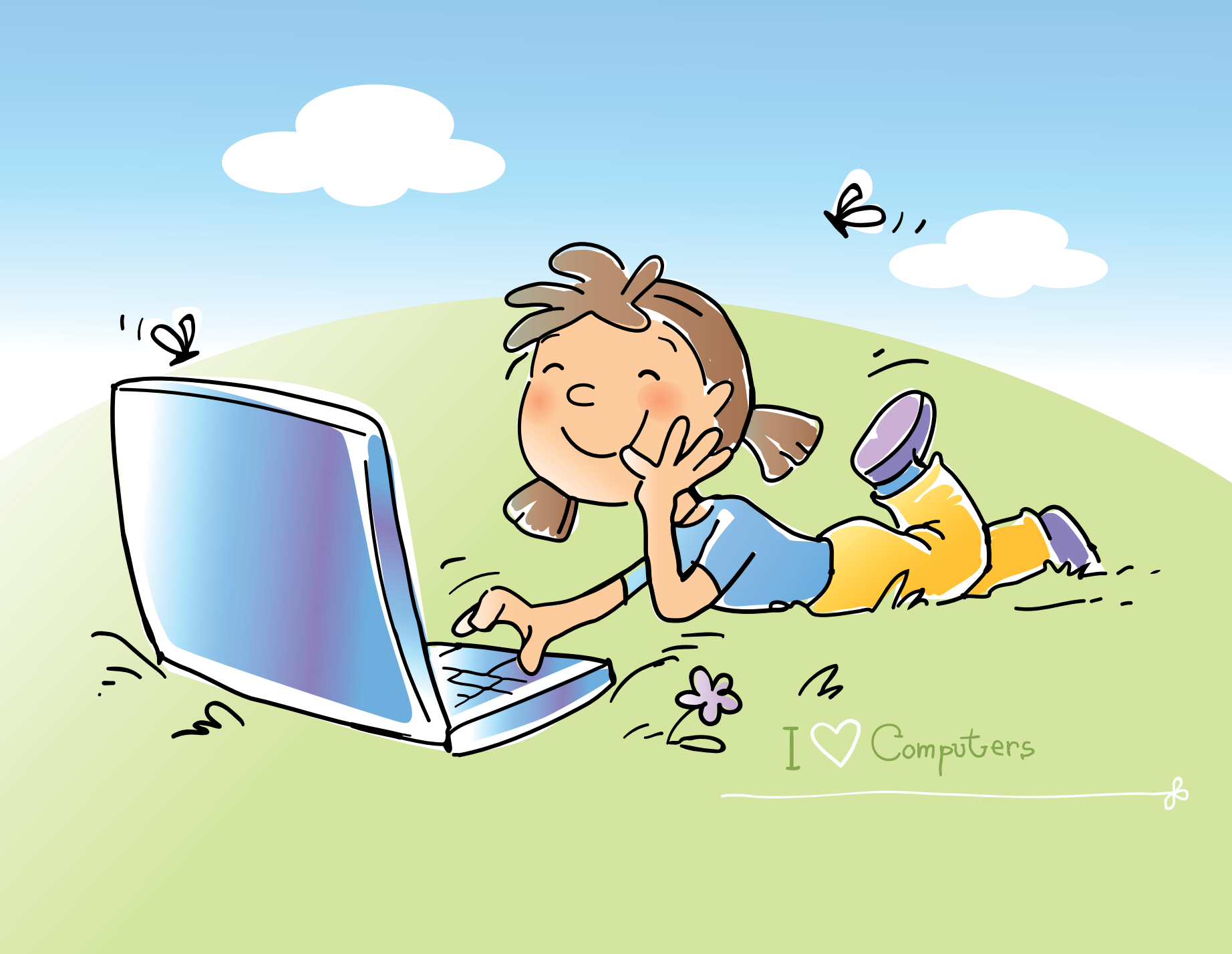
2 Ты можешь сообщить о вредоносном или несоответствующем контенте или действиях на веб-сайтах на адрес электронной почты владельца сайта, который создан специально для сообщений о нарушениях.

3 Ты можешь сообщить о незаконном контенте на горячую линию интернета или в полицию.

4 Ты можешь сообщить местной полиции о незаконных или возможных незаконных действиях.

5 В дополнение к заботе о собственной безопасности ты должен позаботиться о твоем компьютере или мобильном телефоне. Так же как и в Правилах SMART, существуют несколько простых советов, для того чтобы помнить, что необходимо сохранить свой компьютер и мобильный телефон в безопасности.

[25] Например, CHI доступна по адресу: www.childhelplineinternational.org


I ♡ Computers

Научись безопасно использовать свой компьютер

1 Убедись, что ты установил брандмауэр и антивирусное программное обеспечение и научился их правильно использовать. Помни о своевременном обновлении!

2 Узнай об операционной системе своего компьютера (как Windows, Linux и т. д.), особенно о том, как исправлять ошибки и обновлять.

3 Если установлен родительский контроль, поговори со своими родителями и договорись о том уровне, который соответствует твоему возрасту и потребностям. Не пытайся взломать его!

4 Если ты получил файл, в котором ты не уверен или не знаешь, кто его отправил, НЕ открывай его. Именно так Трояны и вирусы заражают твой компьютер.

5 Почувствуй свой компьютер и то, как с ним работать, чтобы ты мог правильно действовать в случае, если заметишь что-то необычное.

6 Научись проверять, кто соединяется с тобой – научись использовать инструменты типа "Netstat". Наконец, хороший способ, для того чтобы быть уверенным, что твои родители согласятся с твоей онлайновой жизнью, – это заключить с ними письменное соглашение. Его цель состоит в том, чтобы заверить их в том, что ты знаешь о рисках, связанных с онлайновой средой, знаешь как вести себя и что делать, а также в том, чтобы привлечь твоих родителей и дать им понять, чем ты занимаешься, когда находишься в онлайновой среде. Соглашение должно основываться на взаимном согласии между тобой и твоими родителями. В конце этих Руководящих указаний приведен пример такого соглашения (Приложение 1). Ты можешь найти различные варианты Семейного соглашения по безопасному использованию интернета в онлайновой среде.

Твои права в онлайновой среде

- Ты имеешь право использовать технологию для развития своей индивидуальности и помощи в расширении твоих возможностей;
- Ты имеешь право защитить свою идентичность;
- Ты имеешь право становиться участником, весело проводить время и иметь доступ к информации, соответствующей твоему возрасту и личным желаниям;
- Ты имеешь право свободно выражать себя, и право на уважение к себе, и в то же время должен всегда уважать других;
- Ты имеешь право быть критичным и обсуждать что-либо, что написано или доступно, когда ты находишься в онлайновой среде;
- Ты имеешь право сказать НЕТ, тому, кто просит тебя о чем-то, что заставляет тебя чувствовать себя некомфортно, когда ты находишься в онлайновой среде.

Руководящие указания для возрастной группы 5–7 лет

Многие молодые люди в данной возрастной группе не умеют читать или не понимают Руководящих указаний такого вида. Их использование интернета должно все время контролироваться родителем или взрослым. Фильтрующее программное обеспечение или другие технические средства могут также быть чрезвычайно полезны в содействии использования интернета ребенком этого возраста. Было бы целесообразно рассмотреть вопрос об ограничении потенциального доступа таких маленьких детей к интернету, например, путем создания списка безопасных вебсайтов, которые подходят данному возрасту, создавая нечто огороженного стеной сада. Цель состоит в том, чтобы научить данную возрастную группу основам безопасности в интернете, этикету и пониманию. Данная возрастная группа вероятно не сможет понять более сложные сообщения. Родителям и взрослым, которые несут ответственность за детей, следует обратиться к руководящим указаниям COP для родителей, опекунов и учителей, где они смогут увидеть, как наилучшим образом помочь самой младшей возрастной группе сохранить безопасность в онлайновой среде. Кроме того, несколько полезных и интересных ссылок на онлайновые ресурсы для данной возрастной группы можно найти в разделе "Материалы для дополнительного чтения и отыскания новых идей".

Руководящие указания для возрастной группы 8–12 лет

Существует много вещей, которые ты можешь делать в онлайновой среде. В то время как большая часть времени посвящена веселым забавам, иногда дела идут не так хорошо, как ты надеялся, и ты не можешь сразу понять, почему это так или что делать с этим. В данном разделе даны, действительно, полезные советы, для того чтобы помочь тебе оставаться защищенным в онлайновой среде.

Общение с друзьями, используя услугу мгновенных сообщений, в чатах и на сайтах социальных сетей могут стать хорошими способами идти в ногу со временем. Знакомство с новыми онлайновыми друзьями – это тоже весело. В онлайновой среде ты можешь встретить людей, которым нравятся те же фильмы или спорт, что и тебе. И хотя есть много хороших причин для сохранения контактов с онлайновыми друзьями, у знакомств в онлайновой среде есть и риски, особенно если ты не знаешь этих людей в реальной жизни.

Для того чтобы помочь тебе сохранить безопасность, в то время когда ты находишься в чате, помни несколько простых советов:

1 Будь осторожен с тем, кому ты доверяешь в онлайновой среде. Человек может притвориться тем, кем на самом деле не является.

2 Выбирай своих друзей. Хотя очень хорошо иметь много друзей, но имея слишком много друзей, тебе будет трудно следить за тем, кто видит материал, который ты отправляешь в сеть. Не принимай предложение дружбы, если ты действительно не знаешь человека и не уверен в нем.

3 Храни свои персональные данные конфиденциально. Используй ник вместо своего настоящего имени, если ты на сайте или в игре, где может быть много людей, которых ты не знаешь. Спроси своих родителей прежде, чем сообщать кому-либо в интернете свое имя, адрес, номер телефона или любую другую личную информацию.

4 Сделай свой профиль конфиденциальным. Попроси своих родителей помочь тебе сделать это, если ты не уверен. Это очень важно.

5 Всегда храни свой пароль в секрете. Не говори его даже своим друзьям.

6 Если ты хочешь встретиться с кем-то, с кем ты познакомился в онлайновой среде, согласуй это сначала с родителями и попроси их пойти с тобой. Всегда встречайся в ярко освещенном общественном месте, где вокруг много других людей, предпочтительно днем.

7 Если кто-то пишет что-то грубое, пугающее или что-то, что не нравится тебе, расскажи об этом своим родителям или другому взрослому, кому доверяешь.

Сетевой этикет

Иногда легко забыть, что другой человек, с которым ты общаешься путем мгновенных сообщений, играешь с ним в игры или отправляешь ему свой профиль, является реальным человеком. В онлайновой среде легче сказать и сделать вещи, которые ты не можешь сделать в "реальной жизни". Это может задеть чувства человека или заставить его чувствовать себя небезопасно или смутить его. Очень важно быть добрым и вежливым к другим в онлайновой среде – остановиться и подумать, как твое поведение будет затрагивать их.

Советы

Относись к другим людям так, как ты хотел бы, чтобы относились к тебе. Избегай сквернословия и не говори вещей, которые заставят кого-то плохо себя чувствовать. Научись "сетевому этикету", когда находишься в он-лайне. Что считается делать и говорить хорошо, а что нет? Например, если ты печатаешь сообщение ЗАГЛАВНЫМИ БУКВАМИ, он может подумать, что ты кричишь на него.

Если кто-то говорит что-то грубое или что-то, что может заставить тебя чувствовать себя неудобно, не отвечай. Уйди из чата или форума незамедлительно.

Расскажи своим родителям или другому взрослому, кому доверяешь, если ты прочел ненормативную лексику, или увидел неприятные изображения, или что-то страшное.

Игра в онлайновые игры

Игра в онлайновые игры и использование консолей или игр на компьютере может быть очень веселым занятием, но будь осторожен с тем, как долго ты играешь и кто играет с тобой. При общении с другим игроком очень важно защитить свою конфиденциальность и не сообщать личную и персональную информацию. Если ты не уверен в том, является ли эта игра подходящей, попроси своих родителей или взрослого, которому доверяешь, проверить для тебя ее классификацию и отзывы о ней.

Советы

1 Если другой игрок ведет себя ужасно или заставляет тебя чувствовать неудобство, заблокируй его в своем списке игроков. Ты также можешь сообщить о нем модератору игры.

2 Ограничь свое игровое время, для того чтобы ты смог сделать другие вещи, такие как домашние задания, работу по дому и встречи со своими друзьями.

3 Храни персональную информацию конфиденциально.

4 Не забудь выделить время в реальной жизни для твоих друзей, твоих любимых спортивных занятий и другой деятельности.

Запугивание

Правила "реального мира", касающиеся того, как относиться к другим людям, касаются и онлайновой среды. К сожалению, в онлайновой среде люди не всегда относятся друг к другу хорошо, и ты или твой друг можете обнаружить, что вы стали целью запугивания. Тебя могут дразнить в онлайновой среде или распространять слухи о тебе, ты можешь получать неприятные сообщения или даже угрозы. Это может случиться в школе или за ее пределами, в любой час дня, со стороны людей, которых ты знаешь, и иногда от тех, кого ты не знаешь. Ты можешь почувствовать себя в опасности и в одиночестве.

Никто не имеет право запугивать другого человека. Запугивание является совершенно незаконным и может расследоваться полицией.

Советы

Если тебя запугивают в онлайновой среде:

1 Игнорируй. Не отвечай обидчику. Если они не получают ответа, им может это наскучить и они уйдут.

2 Заблокируй этого человека. Это остановит тебя от просмотра сообщений или текстов конкретного человека.

3 Расскажи кому-нибудь. Расскажи своей маме или папе, или другому взрослому, которому доверяешь. Сохрани доказательства. Это может быть полезным для выслеживания того, кто запугивал тебя. Сохрани в качестве доказательств тексты, электронные письма, онлайновые разговоры или голосовую почту.

4 Сообщи об этом в:

- твою школу – она должна иметь свою политику поведения относительно запугивания.
- твоему поставщику услуг интернета и/или оператору мобильной связи или администратору веб-сайта – они могут предпринять действия, для того чтобы помочь тебе.
- полиции – если это является угрозой твоей безопасности, полиция поможет тебе.

Если в онлайновой среде запугивают твоего друга

Узнать, если твоих друзей запугивают в онлайновой среде, может быть очень трудно. Они могут держать это в себе. Если они запуганы, ты можешь заметить, что они возможно не общаются с тобой в чате столько же, или они неожиданно получили много СМС сообщений, или они несчастны после того, как они побывали за компьютером, или проверили свои телефонные сообщения. Они могут прекратить гулять с друзьями или потеряли интерес к школе или общественной жизни.

Помоги остановить запугивание

1. Смело выступи против этого! Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом. Ведь ты бы захотел, чтобы он сделал то же самое для тебя.
2. Не посылай сообщения или изображения, которые могут повредить или огорчить кого-нибудь. Даже если не ты это начал, тебя будут считать участником цикла запугивания.
3. Когда общаешься в онлайновой среде, помни, что к другим надо относиться так, как ты хотел бы, чтобы они относились к тебе.

Твой цифровой отпечаток

Это здорово – делиться чем-нибудь с друзьями в онлайновой среде. Частью развлечения, когда делишься видео, изображениями или другим контентом, является то, что много людей могут увидеть это и прокомментировать. Помни, что то, чем ты делишься со своими друзьями, может просматриваться и другими людьми, которых ты не знаешь. Они также могут видеть это в течение последующих лет. Все, что ты размещаешь в сети, добавляется к твоему цифровому отпечатку и, так как это происходит в онлайновой среде, это может остаться там навеки. Так что подумай прежде, чем размещать что-либо.

Советы

1. Храни свои личные данные в тайне. Используй соответствующий ник вместо своего настоящего имени. Спроси родителей прежде, чем сообщать кому-либо в интернете свое имя, номер телефона или другие персональные данные.
2. Никому не говори свои имя пользователя или пароль.
3. Подумай прежде, чем нажать кнопку "отправить" или "разместить". Контент, который однажды размещен, иногда бывает очень сложно удалить.
4. Не размещай ничего такого, о чем ты бы не хотел, чтобы знали или узнали другие, или чего ты бы никогда не сказал им лично.
5. Помни, что личные изображения и видео, которые ты отправляешь друзьям или размещаешь на сайтах социальных сетей, могут быть переданы другим или загружены на общедоступные сайты.
6. Уважай контент других людей, который ты размещаешь или которым делишься. Например, фотография, которую тебе дал друг, – его собственность, а не твоя. Ты можешь размещать ее в онлайновой среде только, если у тебя есть на это его разрешение, и ты укажешь, откуда ты ее взял.

Оскорбительный или нелегальный контент

Когда ты "путешествуешь" по интернету, ты можешь наткнуться на веб-сайты, фотографии, текст или другие материалы, которые могут заставить тебя почувствовать себя неудобно или огорчить. Существует несколько простых способов справиться с такими ситуациями.

Советы

1. Храни свои личные данные в тайне. Используй соответствующий ник вместо своего настоящего имени. Спроси родителей прежде, чем сообщать кому-либо в интернете свое имя, номер телефона или другие персональные данные.
2. Знай, как "сбежать" с веб-сайта, если поиск по интернету приведет тебя на неприятный или неприличный веб-сайт. Нажми control-alt-delete, если сайт не позволяет тебе выйти.
3. Если веб-сайт выглядит подозрительно, или имеет страницу с предупреждением для лиц моложе 18 лет, покинь его немедленно. Некоторые сайты не предназначены для детей.
4. Проверь с родителями, настроен ли твой поисковый механизм так, чтобы он блокировал материалы, предназначенные для взрослых.
5. Попроси родителей установить программное обеспечение для фильтрации информации из интернета, которое блокировало бы "неправильные" сайты.
6. Попроси родителей помочь тебе найти безопасные и забавные сайты и сделай на них "закладки" для последующего использования.

Возрастная группа 13 лет и старше

Огромное количество молодых людей в этом возрасте пользуются сайтами социальных сетей, онлайновыми играми и приложениями мгновенных сообщений. Выход в он-лайн – это не просто что-то, что они делают изредка или для веселья. Для многих он является частью повседневной жизни. Так они поддерживают контакты и общаются с друзьями, организуют большую часть своей общественной и школьной жизни. Здесь ты найдешь и информацию о том, как оставаться в безопасности, используя эти платформы, и информацию о том, как помочь в создании безопасного и положительного пространства в онлайновом мире для тебя и твоих друзей.

Опасный и нелегальный контент

Любопытство, интересы и желание научиться новым вещам и исследовать новые грани знаний: интернет является превосходным инструментом для удовлетворения таких потребностей. Но интернет – это открытый мир, в котором каждый может распространять новости или почти что угодно. Он содержит бесконечный объем информации, в котором легко потеряться или наткнуться на неправду и материалы, которые не подходят для твоих потребностей или возраста. Мы имеем в виду сайты, которые, например, пропагандируют расовую ненависть или подстрекают к насилию, сайты, которые могут привести тебя к материалам с порнографическим контентом или с сексуальным насилием над детьми. Это может произойти абсолютно случайно, например, во время поиска совершенно других материалов, по электронной почте, программам равноправного обмена, на форумах, в чатах и, в более широком смысле, посредством множества каналов, используемых в социальных сетях.

Поэтому:

1 прежде, чем начать поиск, ты должен иметь четкое представление о том, что ты ищешь;

2 для того чтобы сузить поиск, ты можешь использовать функции или директории расширенного поиска, то есть тематические категории, представляемые большинством поисковых систем, т. е. спорт, здоровье, кино и т. д.;

3 заставь работать свое чувство опасности и попытайся определить, достоин ли доверия этот сайт: когда ты посещаешь сайт, начинают ли автоматически открываться другие страницы? Можешь ли ты определить, кому принадлежит сайт? Легко ли связаться с его владельцем? Можешь ли ты сказать, кто создал страницу или определенную статью, которую ты просматриваешь? Ты всегда можешь произвести еще

один поиск, чтобы выяснить больше об авторе и/или владельце. Удостоверься, что ты правильно записал адрес веб-сайта; существуют сайты, имя которых похоже на имя другого сайта. Это сделано с целью получения преимущества при возможном неверном вводе. Правильно ли написан текст на сайте, нет ли там грамматических ошибок? Имеются ли даты, из которых видно, что на сайте проводится обновление? Есть ли какие-либо любые надлежащие уведомления, например, в отношении конфиденциальности?

4 Если во время "путешествия" в онлайновой среде ты наткнулся на сайты, содержащие материалы с насилием, расизмом, противоправным контентом или насилием над детьми, не забудьте, что об этих сайтах можно сообщить в полицию или на горячую линию. Попробуй выяснить, кому можно отправить такие сообщения в вашей стране, твои родители или другие взрослые, которым ты доверяешь, могут помочь тебе составить отчет. Ты также должен поговорить с кем-нибудь о том, что случилось, и что ты чувствуешь по поводу инцидента/события;

5 Контент (изображения, видео и т. п.), который находится в сети и относится к сексу, часто может иметь порнографический характер и передавать сексуальные материалы обычным для взрослых способом с ощущениями, которые не соответствуют твоей возрастной группе.

Что такое груминг?

Интернет и мобильные телефоны могут быть использованы взрослыми злоумышленниками для налаживания контактов с мальчиками и девочками. Обычно это осуществляется при помощи сообщений SMS и MMS, чатов, программ мгновенного обмена сообщениями, форумов по интересам, досок объявлений, онлайновых игр и, в более общем смысле, используя все площадки социальных сетей, где можно получить информацию о возрасте, поле и другие сведения о пользователях при помощи профилей, которые они заполнили.

Сексуальные интернет-хищники используют интернет для вступления в контакт с детьми и подростками с сексуальными целями, часто применяя метод, известный как "груминг". Он включает в себя завоевание доверия ребенка или подростка на основе его или ее интересов. Эти интернет-хищники чрезвычайно ловко манипулируют людьми. Они часто вводят темы, фотографии на сексуальные темы, используют определенные выражения, чтобы увеличить сексуальную осведомленность и заставить свои жертвы потерять бдительность. Иногда для преследования и соблазнения ребенка используются подарки, деньги, даже билеты на транспорт, чтобы завлечь его туда, где интернет-хищник сможет совершить сексуальное насилие над ним или ней. Такие события даже могут фотографироваться или сниматься на видео, или, если встреча происходит не в реальном мире, интернет-хищник может принуждать ребенка создавать изображения сексуального характера со своим участием или участием своих друзей, или принять участие в действиях сексуального характера, используя веб-камеру для их трансляции. Многие дети и подростки, которые вовлечены в такие виды преступных отношений, в определенной степени испытывают недостаток эмоциональной зрелости или имеют низкую самооценку. Это может сделать их восприимчивыми к такому роду манипуляциям и запугиваниям. Также они могут не торопиться рассказать взрослым о своих встречах, испытывая замешательство или страх потерять доступ в интернет. В некоторых случаях они запуганы интернет-хищниками, и им приказано держать эту связь или то, что случилось, в тайне.

Поэтому:

1 крайне важно, чтобы ты знал об этом риске и о том факте, что не всякий человек в онлайновой среде является тем, за кого он/она себя выдает. Совратители в онлайновой среде часто могут притворяться твоими ровесниками, чтобы создать атмосферу дружеских


http://Bullying...

отношений и доверия, которая может привести к встречам и возможному насилию в реальном мире;

2 очень важно защищать свои личные данные; в реальном мире ты никогда не раскроешь эти сведения и никогда не расскажешь незнакомым людям о своих личных проблемах. Даже, если зародилась приятная виртуальная дружба, которая, как кажется, может привести к чему-то большему, важно помнить, что ты не всегда знаешь о том, кто на самом деле сидит на другом конце линии;

3 для того чтобы войти в чат, на форум или, в более общем смысле, социальную сеть, ты часто должен заполнить персональный профиль, поместив в него информацию, которая может быть детализирована на нескольких уровнях. В таких случаях важно быть внимательным, помещая определимые или прослеживаемые данные (имя и фамилия, адрес, название школы, номер мобильного телефона, адрес электронной почты и т. п.). К этим деталям любой может получить доступ, и поэтому рекомендуется создавать свою идентичность при помощи ника или вымышленного имени и вымышленных изображений, или аватаров, и не раскрывать никакую подробную информацию;

4 если тебя волнуют вопросы твоей сексуальности или более интимных ощущений, помни, что интернет иногда может быть источником действительно хорошего совета и информации, но зачастую лучше попробовать найти возможность обсудить такие вопросы с людьми, которых ты уже знаешь и которым доверяешь в реальной жизни;

5 если имеются попытки соблазнения или возникают неловкие ситуации, важно найти кого-нибудь, с кем можно поговорить, взрослого или друга; кроме того, поставщики услуг интернета часто позволяют пользователям сообщать о происшествиях, нажав на "отчет" или "сообщение", чтобы сообщить о преступлении. В ином случае, ты можешь обратиться в полицию.

Также рекомендуется сохранять тексты электронных писем и бесед в чатах, сообщения SMS или MMS (например, в "ящике входящих сообщений"), так как их можно представить в качестве доказательств в полиции.

Запугивание

Используя такие услуги, как электронная почта, форумы, чаты, блоги, мгновенный обмен сообщениями, SMS, MMS и видеокамеры, можно поддерживать в режиме реального времени отношения со старыми друзьями или заводить новых во всех частях мира и обмениваться идеями, играть в игры, проводить исследования и пр. Хотя большинство этих служб и способов, которые они используют, вполне безобидны, в некоторых случаях те же самые инструменты могут использоваться для оскорблений, насмешек, клеветы и домогательства пользователей интернета; и более того, жестокое или оскорбительное поведение в реальном мире усиливается, если снимать его на мобильные телефоны и обмениваться записями или размещать их в Сети.

Что такое запугивание? Запугиванием является действие намеренного причинения вреда другому человеку, используя устные оскорбления, физическое нападение или другие более хитрые методы насилия, например, манипуляцию. В повседневной речи под запугиванием часто понимается вид домогательства, совершаемого злоумышленником, который имеет больше физической и/или социальной силы и влияния, чем жертва. Жертва запугивания иногда называется целью. Домогательство может быть устным, физическим и/или эмоциональным. (www.wikipedia.org)

Зачастую запугивание происходит в школах или в местах жительства. К сожалению, наблюдается увеличение количества задир и реальных форм запугивания в онлайно-

вой среде, начиная с оскорбительных веб-сайтов и заканчивая текстовыми сообщениями в духе домогательства и отправкой нежелательных фотографий при помощи мобильных телефонов и так далее. Этот определенный вид запугивания, который может оскорбить и ранить кого-нибудь без необходимости вступать в любой физический контакт, может иметь такие же неприятные последствия, как и обычные виды запугивания.

Поэтому важно, чтобы ты знал, что такое явление существует, и чтобы знал о разных формах, которое оно может принимать, и что можно сделать, чтобы не стать жертвой:

1 не размещай бездумно свои личные данные, так как это может помочь легко тебя найти и сделать более уязвимым для действий по запугиванию и устрашению со стороны твоих сверстников;

2 после того, как информация размещена в онлайновой среде, ты не сможешь ею управлять, и она может быть доступна любому и открыта для любого вида использования. Ты должен абсолютно ясно это понимать; то что может показаться невинной шуткой, может привести к весьма раздражающим и неприятным последствиям для других;

3 важно воздерживаться от ответа на провокации, получаемые при помощи сообщений SMS, MMS, программ мгновенного обмена сообщениями в оскорбительных или клеветнических электронных письмах, в чатах или во время общения в онлайновой среде с другими пользователями. Вместо этого тебе нужно разработать определенные стратегии, которые могут исключить или ограничить действия с такими попытками провоцировать тебя, как:

- многие игры позволяют исключать неприятных или нежелательных игроков;
- если чаты контролируются, то можно сохранить оскорбительный текст из чата и отправить его наблюдателю;
- поставщикам услуг можно сообщить о злоупотреблениях, или в случае злоупотребления при помощи мобильного телефона отчет можно отправить компании, предоставляющей услуги подвижной связи;
- в более серьезных случаях, например, в случае возникновения физической опасности, рекомендуется также сообщить в полицию;
- можно проследить учетную запись электронной почты, с которой пришло оскорбительное сообщение, но практически невозможно доказать, кто на самом деле использовал ее для отправки сообщения. Онлайновый задира также может взломать чью-нибудь учетную запись и использовать ее для его/ее оскорбительных действий и потому позволить обвинять невиновного человека, чья учетная запись электронной почты была использована в противоправных целях;
- большинство программ электронной почты позволяют включать фильтры для блокировки нежелательных входящих электронных писем.

4 Многие программы мгновенного обмена сообщениями предлагают возможность создания списка имен, которые пользователи предпочитают блокировать. Таким образом, ты можешь предотвратить контакты с тобой нежелательных людей. Система мгновенного обмена сообщениями (IM) позволяет тебе узнать, когда один из твоих известных и принятых контактов находится он-лайн, и поэтому вы можете начать сеанс разговора с человеком, с которым вам хотелось бы поговорить.

Существует достаточно много различных систем IM, например, ICQ, AOL Messenger, Yahoo Messenger! Задиры знают, какие из них наиболее популярны среди подростков и используют их для своих целей, например, перепалок или провоцирования схваток в онлайновой среде. Разговоры или схватки, которые

происходят в онлайновой среде, могут иногда иметь последствия, которые проявляются в школах или других местах реального мира.

Всегда помни, что важно рассказать кому-нибудь, что случилось, если ты хоть когда-нибудь почувствуешь себя неуютно или под угрозой.

Расскажи родителям, учителю или кому-нибудь из школьного персонала, кому ты можешь доверять. Даже просто рассказ друзьям уже может помочь.

Ты также можешь сообщить поставщику услуг или оператору подвижной связи, даже в полицию, если это серьезно. Помни, что когда рассказываешь другим, надо сохранить доказательства запугивания, так как это может быть действительно важно.

Во многих странах существуют национальные или местные организации, к которым ты можешь обратиться за помощью.

В некоторых странах, например, в Канаде "киберзапугивание" считается фактическим преступным деянием. В большинстве стран существует уголовное наказание за угрозы любому человеку или беспокойство или преследование, вне зависимости от того, происходит это, в реальном или в онлайновом мире.

Интересный факт: термин задира раньше имел совершенно другое значение, чем сегодня, на самом деле 500 лет назад он означал "друга" или "члена семьи", как же все изменилось!

Защити свою личную информацию

В настоящее время создать блог или личный веб-сайт относительно просто. Для того чтобы присоединиться к чату, форуму или, в более общем смысле, к социальной сети тебе сначала надо создать личный профиль, который содержит более или менее подробную информацию. На разных сайтах разные правила. Прежде чем ввести любую информацию о себе в базу данных сайта или в записи об участниках, узнай, как может быть использована эта информация, может ли быть опубликована вся информация или ее часть и, если да, то где. Если тебе не по себе от объема запрашиваемой информации, если ты не знаешь или не доверяешь сайту, не давай информацию. Поищи другую или похожую службу, которая требует меньше информации или обещает более бережно обращаться с информацией. Везде, где это возможно, рекомендуется создавать идентичность или псевдоним, используя выдуманный ник и не добавлять больше ничего. Чрезвычайно важно, чтобы ты четко понимал, что можно сообщать другим, а что – лучше не стоит. Все то, что попадает в онлайновую среду, очень быстро может выйти из-под твоего контроля и оказаться в распоряжении кого угодно, и может быть использовано как угодно:

1 каждый раз, когда требуется сообщить свои личные данные, удостоверься, что кто бы ни затребовал информацию о тебе, он является надежным и серьезным человеком, а также помни, что прежде, чем сообщать данные, касающиеся твоих друзей, сначала надо поставить их об этом в известность и получить разрешение, так как они могут не обрадоваться, узнав, что их адреса электронной почты или другая личная информация были переданы другим;

2 от тебя может не требоваться сообщать всю запрошенную информацию о тебе, и тебе нужно будет вставить только те данные, которые строго необходимы. В любом случае всегда лучше выяснить как можно больше о человеке, службе или компании, с которыми ты решил иметь дело, прежде чем предоставлять данные о себе. В частности, проверь, не спрашивают ли у тебя на сайте данные с целью рассылки рекламных материалов или не предполагают ли они передать твои данные любой другой компании. Если ты не хочешь, чтобы они делали какое-либо из этих действий или оба, отметь соответствующие поля. Если тебе не предложена такая возможность, ты должен серьезно задуматься, чтобы совсем не пользоваться этой службой;

3 отправляй личные фотографии и видео только тем, кого ты действительно знаешь, твое изображение представляет собой личные данные, и тебе надо быть уверенным в том, что оно не будет бездумно распространяться. То же относится к изображениям других людей. Имей в виду, что практически невозможно определить, где в онлайновой среде в конце концов окажется изображение; прежде чем снимать на видео или фотографировать кого-нибудь, всегда спроси их разрешения;

4 когда тебе надо зарегистрироваться в определенной службе, попробуй применить простые советы: например, используй пароль, который будет трудно подобрать, так чтобы никто не смог его угадать и получить доступ к твоей учетной записи; используй сложный адрес электронной почты, по возможности и с цифрами и с буквами (например, mrx-3wec97@... . com), так чтобы спамерам или неизвестным лицам, желающим отправить тебе нежелательное письмо, было бы труднее его определить; удостоверься, что твоя антиспамовая служба для входящих электронных писем и антивирусные программы для почтовых вложений активированы и постоянно обновляются; используй два адреса электронной почты, один из которых исключительно для личных сообщений и для переписки с твоими знакомыми из реальной жизни (друзья, родственники и т. п.), а второй – для всех форм регистрации в онлайновой среде, где спрашиваются личные данные (профили пользователя, сообщения о конкурсах, онлайновые игры и пр.), к которым, как ты уже знаешь, могут иметь доступ незнакомцы;

5 не открывай вложения электронной почты, полученные от адресатов, которых ты не знаешь, или программы, о возможном действии которых ты не знаешь, это могут быть программы Key Logger, которые могут записывать, какие клавиши были нажаты на клавиатуре, позволяя определить пароли, цифровые коды, номера кредитных карт и пр., E-Grabber, которая может получить доступ ко всем адресам электронной почты, имеющимся в компьютере жертвы, или Info Grabber, которая может извлечь информацию, например, разные ключи регистрации наиболее важных программ на компьютере. Без твоего ведома эти программы могут отправить через интернет неизвестным лицам любую информацию, которую они собрали;

6 участвуй только в тех действиях, в которых ты абсолютно уверен. Если ты чувствуешь "неприятный душок", что-то не совсем правильное, что не может убедить тебя полностью, или ты думаешь, что с тобой несправедливо обращаются, тогда лучше прекратить это делать. Ты имеешь право критиковать и задавать вопросы, которые у тебя возникли, пока ты был в он-лайне. Помни, что вещи не всегда являются такими, какими они кажутся.

Уважай авторское право

Что хорошо в сети – это бесконечные возможности по поиску и доступу ко всем видам материалов при помощи поисковых систем, и при помощи твоего ПК или мобильного телефона эти материалы можно либо загрузить бесплатно, либо за некоторую плату, а затем использовать вне сети. Не все, что можно найти в онлайновой среде, можно использовать по твоему желанию; большая часть контента защищена законом об авторских правах или правах о названиях.

Программы децентрализованного обмена (P2P) позволяют передавать файлы и обмениваться файлами напрямую с другими пользователями интернета без дополнительной платы за соединение. Среди подростков очень популярны, и они часто скачивают такие виды контента как музыка, фильмы, видео и игры, но они часто подпадают под положения об авторских правах и защищаются законом. Несанкционированная загрузка и распространение контента, защищенного авторскими правами, во многих странах является преступлением и преследуется по закону. Также возможно, что твое участие в незаконной загрузке материалов, защищаемых авторскими правами, может быть отслежено. Это, например, может привести к тому, что родителям ребенка будет прислан счет на большую сумму для покрытия стоимости загруженных материалов, а если семья откажется оплатить счет, могут быть применены другие виды правовых действий. Некоторые страны предполагают запрещать доступ в интернет людям, которые были уличены в постоянном использовании его для получения несанкционированного доступа к материалам, защищаемым авторскими правами. Кроме того, когда ты используешь работы других людей, например, статьи или доклады, не забывай правильно цитировать источники. Если ты не сможешь это сделать, тебя могут осудить за плагиат, что может привести к большим неприятностям.

Помни:

1 ты можешь свободно использовать, изменять и распространять бесплатные программы, которые не защищаются авторскими правами;

2 с другой стороны, некоторые программы являются условно бесплатными, и потому бесплатны они только в течение определенного пробного периода времени;

3 твоя конфиденциальность и твой компьютер могут пострадать от вирусов или других "вредоносных программ". Поэтому лучше всего установить и постоянно обновлять системы защиты, например, антивирусное программное обеспечение, программы, защищающие твой компьютер от программ, которые могут без твоего ведома устанавливать соединение с интернетом, и брандмауэр. Всегда обязательно прочти руководство к программе, которую ты используешь, чтобы избежать нижеперечисленных ошибок;

4 твоя конфиденциальность и твой компьютер могут пострадать от вирусов или других "вредоносных программ". Поэтому лучше всего установить и постоянно обновлять системы защиты, например, антивирусное программное обеспечение, программы, защищающие твой компьютер от программ, которые могут без твоего ведома устанавливать соединение с интернетом, и брандмауэр. Всегда обязательно прочти руководство к программе, которую ты используешь, чтобы избежать нижеперечисленных ошибок;

5 программы децентрализованного обмена (P2P), которые ты используешь для передачи и загрузки файлов, также несут с собой определенные риски. Нужно иметь очень полные знания о них, чтобы использовать без каких-нибудь рисков для безопасности:

a ты не всегда можешь прекратить загрузку того, что хотел загрузить: за названием песни или видео могут скрываться разные виды контента. Например, в худшем случае, он может содержать изображения сексуального насилия над детьми. Изучи свою личную программу, чтобы выяснить, как ты можешь определять ложные файлы, и используй только те источники, о которых ты знаешь, что они заслуживают доверия: спроси друзей, какие источники использовать, а каких избегать;

b прежде чем открыть загруженный файл, просканируй его на вирусы; еще один весьма частый риск связан с тем фактом, что загруженный файл может содержать вирусы и шпионские программы, которые могут подвергнуть риску компьютеры, личные данные и конфиденциальность;

- сделай общий доступ ко всему жесткому диску невозможным: проверь свои настройки, чтобы гарантировать, что общий доступ открыт только к тем папкам, которые ты хотел использовать для общего доступа, и помни, что разрешая общий доступ к файлам, защищенным авторским правом, ты совершаешь преступление.

Торговая деятельность в онлайновой среде

Ты можешь приобретать продукты он-лайн или при помощи мобильного телефона. Покупки можно оплатить кредитной картой или, в случае с мобильным телефоном, при помощи списания денег со счета абонента мобильного телефона. Также в онлайновой среде существуют площадки, где можно обменивать и приобретать любые виды продуктов по очень конкурентным ценам.

Одним из основных различий между онлайновой и традиционной торговлей является сложность идентификации того, кто находится на другом конце обменной цепочки, и риск мошенничества, который может всегда присутствовать. Одним из наиболее широко распространенных рисков является риск "фишинга". Фишинг происходит, когда люди отвечают на ложные электронные письма, спам, которые обычно кажутся пришедшими из надежного источника, например, банка или кредитной компании. Они попросят тебя ввести большой объем личной информации, например, детали банковского счета, пароли, дату рождения и так далее, которую они впоследствии могут использовать в своих целях.

Дополнительная сложность с онлайновой торговой деятельностью касается продажи продуктов или услуг, которые имеют определенные возрастные ограничения. Например, во многих странах продавцам запрещено по закону продавать или поставлять алкогольные или табачные изделия несовершеннолетним. Как правило, определенным возрастом ограничивается также участие в азартных играх. Тем не менее, в онлайновой среде продавцу очень трудно определить возраст человека, который хочет осуществить покупку или заказать услугу. Единственное, что делают многие компании, это просят человека поставить отметку в ячейке, подтверждая, что он отвечает требованиям возрастных ограничений.

Некоторые компании в определенных странах начинают внедрять системы подтверждения возраста, связанные с процедурами покупки, но эта технология пока еще остается совершенно новой и ее применение ограничено, несмотря на то, что она развивается. Покупка в онлайновой среде продуктов, имеющих возрастные запреты, и указание ложных данных о твоем возрасте для этих целей означает, что тебя могут подвергнуть уголовному преследованию как и продавца. У тебя могут конфисковать товары, и даже завести уголовное дело, так что не делай этого.

В любом случае существуют определенные тактики, которые могут помочь тебе уменьшить риски и дать возможность использовать удобные преимущества онлайновой торговли:

1. очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах;
2. предоплаченные кредитные карты, или пополняемые карты выпускаются с ограничениями расходов и могут помочь избежать неприятных сюрпризов;
3. прежде чем купить что-нибудь в онлайновой среде, удостоверься, что сайт использует систему безопасных транзакций, чтобы предотвратить, например, "вынюхивание", которое предполагает перехват данных во время их передачи. Даже учитывая то, что многие сайты внедрили системы, противостоящие перехвату передаваемых данных, ваша информация может быть украдена, если кто-нибудь взломает сервер компании, где хранились данные о твоей кредитной карте. Оче-

видно, выбрав другие способы оплаты, ты можешь избежать вероятности того, что кто-нибудь украдет номер твоей кредитной карты;

4 если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика;

5 если что-то выглядит слишком хорошо, для того чтобы быть правдой, скорее всего, это так и есть, и лучше забыть об этом;

6 если покупка производится при помощи мобильного телефона, для чего не нужна кредитная карта, проверь реальную стоимость услуг, условия предоставления услуги и как от нее можно отказаться.

4. Выводы

Соблюдая данные основные правила, ты сможешь избежать большинства ловушек, с которыми ты можешь столкнуться в онлайновой среде. Если ты столкнешься с неприятными или смущающими тебя случаями, убедись, что ты общаешься с источником, которому доверяешь. Помни, ты имеешь право быть защищенным, а также то, что ты обязан вести себя соответственно как в реальной жизни, так и в онлайновой среде.

Источники для дополнительного чтения и вдохновения

Конвенция Организации Объединенных Наций по правам ребенка
http://www.unicef.org/crc/

Результаты ВВУИО
http://www.itu.int/wsis

Деятельность МСЭ по кибербезопасности
http://www.itu.int/cybersecurity

Инициатива Защита ребенка в онлайновой среде (COP)
http://www.itu.int/cop

Представь твое будущее – прогнозирование, каким будет будущее
http://www.elon.edu/e-web/predictions/kidzone/yourfuture.xhtml#kids%27%20predictions

Большая картина интернета – пользователи всемирного интернета и статистика населения
http://www.internetworldstats.com/stats.htm

Версия для детей "Мир, пригодный для детей"
http://www.unicef.org/specialsession/wffc/child_friendly.html

Опросы общественного мнения: что думают молодые люди
http://www.unicef.org/polls/

Безопасное общение для родителей, подростков, учителей, адвокатов – все привлечены и заинтересованы влиянием социальных веб-сайтов
http://www.connectsafely.org/

Заключительное выступление на III-м Мировом Конгрессе против сексуальной эксплуатации детей и молодых людей
http://www.ecpat.net/WorldCongressIII/PDF/Outcome/WCIII_Outcome_Document_Final.pdf

Всемирный Устав интернета для детей и молодых людей
http://www.iyac.net/children/index.htm

Ряд ресурсов детских сетей для молодых людей
http://www.childnet-int.org/young-people/

Информация по безопасному интернету (доступ к сайтам на разных языках)
http://www.saferinternet.org/ww/en/pub/insafe/index.htm
http://www.getnetwise.org/

Приложение 1

Обязательства родителей

Я знаю, что интернет может быть прекрасным местом, которое могут посещать мои дети. Я также знаю, что я должен сделать со своей стороны, для того чтобы помочь им оставаться в безопасности во время посещения интернета. Понимая, что мои дети могут помочь мне, я согласен следовать этим правилам:

1 Я ознакомлюсь с услугами и веб-сайтами, которые использует мой ребенок.

2 Я установлю разумные правила и руководящие указания для использования компьютера моими детьми и буду обсуждать эти правила и размещать их около компьютера как напоминание.

3 Я не буду реагировать слишком остро, если мой ребенок расскажет мне о чем-то "плохом", что он или она нашел или делал в интернете.

4 Я буду пытаться узнать "онлайновых друзей" моего ребенка и список контактов, также как я стараюсь узнать других его или ее друзей.

5 Я буду пытаться обеспечить поддержку и надзор за использованием интернета моими младшими детьми, например, пытаясь установить их компьютер в общей комнате.

6 Я буду сообщать соответствующим органам о подозрительных и незаконных действиях и сайтах.

7 Я буду создавать или находить перечень рекомендуемых сайтов для детей.

8 Я буду часто проверять, какие сайты в интернете посещали мои дети.

9 Я буду искать способы фильтрации и блокирования материала, непригодного для моих детей.

10 Я буду разговаривать с моими детьми о том, что они нашли в онлайновой среде, и совершать с ними онлайновые приключения так часто, как я смогу.

Я согласен с тем, что изложено выше.

Подпись родителя(ей)

_____

Дата

_____

Я понимаю, что мои родители согласились жить по этим правилам, и согласен помочь своим родителям исследовать интернет вместе со мной.

Подпись ребенка

_____

Дата

_____

Обязательства ребенка

Я знаю, что интернет может быть прекрасным местом для посещения.
Я также знаю, что очень важно следовать правилам, которые сохранят мою безопасность во время этих посещений.
Я согласен выполнять следующие правила:

1 По мере возможности, я буду выбирать для себя безопасное и разумное имя, которое не будет разглашать никакую личную информацию о моей семье или обо мне.

2 Я буду хранить все мои пароли в тайне.

3 Я буду обсуждать с моими родителями все программы и приложения, которые я использую на моем компьютере и в интернете, и рассказывать им о сайтах, которые я посещал. Перед тем, как скачать или загрузить новую программу или соединиться с новым сайтом, я согласую это с моими родителями, для того чтобы удостовериться в том, что они их одобряют.

4 Принимая решение зарегистрироваться для подключения к новой онлайновой услуге, я буду избегать тех сайтов, которые требуют слишком много личной информации, и попытаюсь выбрать те, которые требуют меньше.

5 Я буду всегда стараться выяснить, какая персональная информация обо мне по умолчанию будет размещаться в моем профиле, и всегда буду выбирать максимальный уровень безопасности.

6 Я не буду передавать личную информацию обо мне, или моих родителях, или других членах семьи любым способом, в любой форме или виде, ни в онлайновой среде, ни кому-либо, с кем я встречаюсь в онлайновой среде. Эта информация включает в себя имя, адрес, номер телефона, возраст или номер школы, но не ограничивается этим.

7 Я буду обращаться с другими так, как я бы хотел, чтобы обращались со мной.

8 Находясь в онлайновой среде, я буду проявлять хорошие манеры, включая хороший язык общения и уважение. Я не буду вступать в ссоры или использовать угрожающие или нецензурные слова.

9 Я сделаю мою собственную персональную безопасность моим приоритетом, так как я знаю, что есть люди, которые в онлайновой среде притворяются теми, кем на самом деле не являются.

10 Я буду честен с моими родителями относительно людей, с которыми я встречаюсь в онлайновой среде, и расскажу об этих людях, даже если меня не спросят. Я не буду отвечать на любые электронные письма или мгновенные сообщения от тех, кого не одобряют мои родители.

11 Если я увижу или прочитаю что-либо плохое, непристойное или низкое, я выйду из системы и расскажу об этом моим родителям, для того чтобы они попытались сделать так, чтобы это не повторилось снова.

12 Я расскажу родителям, если я получил картинки, ссылки на плохие сайты, сообщения электронной почты или мгновенные сообщения с ненормативной лексикой или о том, что я общаюсь в чате, где люди используют нецензурные слова или унижающий и жестокий язык общения.

13 Я не буду ничего посылать кому-то, кого я встретил в онлайновой среде, без согласия моих родителей. Если я получил что-то по почте от кого-то, с кем я познакомился в онлайновой среде, я сразу же расскажу об этом родителям, потому что это означает, что они имеют доступ к моей личной информации.

14 Я не буду делать в онлайновой среде ничего, о чем меня кто-либо попросит, если это заставит меня чувствовать себя

некомфортно, особенно, если я знаю, что это расстроит моих родителей или что они могут не одобрить этого.

15 Я не буду звонить, писать обычные письма или встречаться с любым человеком, с которым я познакомился в онлайновой среде, без согласия моих родителей или без доверенного взрослого, который пойдет со мной.

16 Я понимаю, что мои родители будут контролировать мое время, проводимое в онлайновой среде, и могут использовать программное обеспечение для наблюдения или ограничения того, где я бываю в онлайновом режиме. Они делают это, потому что они любят меня и хотят защитить меня.

Я буду учить моих родителей пользоваться интернетом так, чтобы мы могли вместе весело проводить время и учиться новым замечательным вещам.

Я согласен с тем, что изложено выше.

Подпись ребенка

_____

Дата

_____

Я обещаю защищать моего ребенка, убеждая его соблюдать эти правила по безопасному использованию интернета. Если мой ребенок столкнется с небезопасными ситуациями и расскажет мне об этом, я обдуманно и разумно рассмотрю каждую ситуацию, никого не обвиняя, а спокойно помогу своему ребенку так, чтобы обеспечить ему безопасный опыт работы в интернете в будущем.

Подпись родителя(ей)

_____

Дата

_____

Фотографии предоставлены www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

Международный союз электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

Отпечатано в Швейцарии
Женева, 2009 г.

При поддержке:

Save the Children

Telefonica

CHIS

ins@fe