Слайд 1. Сегодня мы поговорим о безопасности в Интернете.

Слайд 2. Что же такое интернет? Это, можете сказать вы: общение, игры, новости, знания, электронная почта.

Слайд 3. Можно ли разрешать детям пользоваться всемирной паутиной? Большинство исследователей, специалистов да и просто рядовых пользователей с уверенностью отвечают на этот вопрос утвердительно. Говорят, что интернет позволяет детям обучаться, развиваться, учиться виртуальному общению, которое наряду с общением реальным стало неотъемлемой частью нашей жизни. Так возникла идея детского, «безопасного», интернета — зоны, схожей по своему назначению с детскими площадками в реальном мире. Здесь дети могут общаться со своими сверстниками, играть с ними в разные игры, «читать» сайты, похожие на детские книжки. Сказки, стихи, обучающая литература для малышей и даже книжки-раскраски — все это можно найти на виртуальных полках детского интернета. Специально для самых маленьких пользователей создаются даже целые поисковые системы, индексирующие только детские странички.

Слайд 4. *Интернет дает ребенку прекрасные возможности для общения и развития, но жизнь в Сети может быть полна неприятных неожиданностей — если родители вовремя не озаботятся этой проблемой.*

Слайд 5. Какие опасности таит в себе интернет для детей? (прочитать со слайда). Остановимся на каждом аспекте подробнее.

Слайд 6. Но для начала обратимся к статистике: количество пользователей социальных сетей (прочитать данные со слайда).

Слайд 7. И сравним ее с количеством детей, пользующих интернетом (прочитать данные со слайда).

Слайд 8. (прочитать данные со слайда).

Слайд 9. Так какие же опасности таят в себе социальные сети?

Слайд 10.

Встречи с незнакомцами и груминг
Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Предупреждение встреч с незнакомцами и груминга

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети — с ровесниками или людьми старше себя.
2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.
3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.
4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.
5. Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.
6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Как противостоять грумингу

1. Если ребенок желает познакомиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу
2. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию
3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать емуребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
4. Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).
5. При обнаружении признаков совращения следует немеделенно сообщить об этом в правоохранительные органы.
6. Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению груминга.

Слайд 11. Пример

Слайд 12. *Кибербуллинг* — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Исследования буллинга начались еще в 70-х годов. прошлого века. Это поведение всегда

присутствует в подростковой среде. В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Многие исследования показывают, что кибербуллинг часто сопровождает традиционный буллинг.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Предотвращение кибербуллинга

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.
2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.
3. Обратите внимание на психологические особенности вашего ребенка. Специалисты выделяют характерные черты, типичные для жертв буллинга, они часто бывают: пугливы, чувствительны, замкнуты и застенчивы;тревожны, неуверены в себе, несчастны;склонны к депрессии и чаще своих ровесников думают о самоубийстве;не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками; мальчики могут быть физически слабее своих ровесников.
4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.
5. Объясните детям, что личная информация, которую они выкладывают в интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.
6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.
7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете.
8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи действия уголовного и административного кодексов о правонарушениях.

Как справляться с кибербуллингом

1. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.
2. Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).
3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная

поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.

4. Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению кибер-буллинга.

Слайд 13. *Кибермошенничество* — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Предупреждение кибермошенничества

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.
2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.
3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:
    - Ознакомьтесь с отзывами покупателей.
    - Избегайте предоплаты.
    - Проверьте реквизиты и название юридического лица – владельца магазина.
    - Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
    - Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
    - Сравните цены в различных интернет-магазинах.
    - Позвоните в справочную магазина.
    - Обратите внимание на правила интернет-магазина.
    - Выясните, сколько точно вам придется заплатить.

Как справляться с кибермошенничеством

1. Проговорите с ребенком всю ситуацию. Он должен рассказать, какой сайт он посещал, на какие баннеры нажимал, какими услугами сети пользовался, что видел и т.д. Сохраните все электронные свидетельства совершенных действий и операций, скриншоты экранов – они могут служить доказательствами в дальнейшем.
2. Фишинг и вишинг: В случае хищения данных, поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета. Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

Слайд 14.профилактика основных интернет-рисков и борьба с ними

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Предупреждение столкновения с вредоносными программами

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).
7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
8. Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки — по этой информации злоумышленники могут многое узнать о вашем ребенке.

Как избавиться от вредоносных программ

1. Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
2. Проведите полную антивирусную проверку компьютера.
3. Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.
4. При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.

Слайд 15. *Интернет-зависимость* — навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996).
По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Предупреждение интернет-зависимости

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
2. Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить — ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.
4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в интернет с помощью телефона или иных мобильных устройств во время урока.

Как справляться с интернет-зависимостью

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
2. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.
3. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате — это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.
4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете. Это поможет наглядно увидеть и осознать проблему, а также

избавиться от некоторых навязчивых действий — например, от бездумного обновления странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями — при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с интернетом увлечения, которым он мог бы посвящать свое свободное время.
6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял — ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет-сообщества.
7. В случае серьезных проблем обратитесь за помощью к специалисту. Информацию, куда обращаться вы можете найти в разделе Полезная информация.

Слайд 16. Безопасный поиск в Интернете

На данный момент в большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», и это первый ключевой момент, на который родителям стоит обратить внимание. Включенная опция «Безопасный поиск» или «Семейный фильтр» (у разных поисковых систем эта функция называется по-разному) предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. Чтобы включить такую опцию, например, в Яндексе, следует сделать следующее:

- заходим в «Настройку»:
- открывается страница настроек поисковой выдачи:
- Выбираем уровень фильтрации в пункте «Фильтрация страниц». Для достижения высокого качества фильтрации мы рекомендуем использовать уровень «Семейный поиск».

Многие другие известные поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. Более подробно о данной опции можно прочитать на порталах самих поисковых систем mail.ru, Bing и Yahoo.

Слайд 17. Одним из способов защиты от несанкционированного доступа к странице вашего ребенка в Контакте является функция Закрыть профиль, которую вы можете выполнить сами.

Слайд 18. Что думают родители? (прочитать со слайда).

Слайд 19. Что есть на самом деле? (прочитать со слайда).

Слайд 20. **Заключение.** Нужно ли позволять детям пользоваться интернетом?

Вне всякого сомнения, ответ на этот вопрос, должен быть положительным, ведь интернет — такая же среда общения, как и школьный двор. Ребенок должен уметь общаться в виртуальном мире. К тому же возможности, которые интернет предоставляет для обучения и познания мира, практически безграничны. Запретить ребенку доступ в интернет — значит лишить его самого емкого источника информации в мире.

Правильнее поставить вопрос так: «Можно ли разрешать детям пользоваться интернетом без присмотра?»

В наше время средний возраст для первого погружения в неизведанные пучины интернета — это 5-6 лет. В мегаполисах довольно много малышей получает доступ в интернет с 3-4 лет, и лишь немногие дети знакомятся с интернетом в школьном возрасте. Однако интернет все равно остается миром взрослых. Как и в реальном взрослом мире, здесь есть вещи непонятные малышу и, зачастую, опасные для него.

В этом мире первая помощь и поддержка маленькому мальчику или девочке должна оказываться, конечно же, со стороны родителей. Мы же не отпускам своих маленьких детей гулять одних в большом городе. Мы знаем, что без нас их подстерегает там много опасностей. Интернет же, как правило, не вызывает у большинства родителей должного беспокойства. В настоящее время более 70% детей от 7 до 12 лет пользуются интернетом самостоятельно. Для детей от 4 до 7 лет эта статистика несколько скромнее, однако она тоже неутешительна.

Совместные выходы в интернет родителей и детей происходят только для обучения ребенка веб-серфингу, помогают ему освоиться в новой среде. Когда ребенок начинает самостоятельно и уверенно пользоваться мышкой или, тем более, клавиатурой, мама и папа перестают страховать его, решив, что их миссия выполнена. Но это не так — в этот момент работа родителей должна только начинаться. Дети наивны и доверчивы, они не умеют критически оценивать ситуацию, и к тому же их очень легко травмировать. Совместный серфинг в интернете родителей с детьми поможет решить массу проблем психологического характера, а заодно и проблему защиты компьютера от интернет-угроз. Понятно, что 10-12-летний ребенок уже хочет некоторой приватности в своем виртуальном общении с друзьями и не будет рад постоянному присутствию родителей . Однако к такому сознательному возрасту практика постоянного совместного серфинга уже должна научить ребенка, «что такое хорошо и что такое плохо» в интернете. И теперь можно позволять — уже не ребенку даже, а подростку полусамостоятельное плавание в Сети, когда папа или мама не сидят рядом, внимательно вчитываясь в личную переписку, контролируя каждый шаг, а являются помощью и поддержкой в сложных ситуациях. Что же касается ребят помладше — они будут только рады научиться безопасному и интересному для них серфингу в интернете в компании своих родителей.