РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ «БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ»

Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Одной из важнейших координат их развития становятся информационно-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для их родителей и педагогов.

Предлагаем Вашему вниманию рекомендации «Безопасность детей в Интернете», разработанные **Н.И. Баскаковой, под общей редакцией Н.К. Солоповой, к.п.н., доцента, проректора по учебно-методической работе и информатизации ТОИПКРО. – Тамбов: ТОИПКРО, 2011. – 191 с.**

В основе предлагаемых рекомендаций лежит разработанная Фондом Развития Интернет классификация Интернет-рисков (опасностей), приведены некоторые результаты исследования «Дети России онлайн», которое было проведено Фондом Развития Интернет по методологии международного исследовательского проекта Еврокомиссии «EU Kids Online II» (2010-11 гг.).

Риски (опасности) по данной классификации разделяются на четыре типа: контентные, коммуникационные, электронные и потребительские. Учитывая их разную природу и механизм действия, в отношении каждого типа рисков даются отдельные рекомендации.

Информация нежелательного характера. Контентные риски

Как их избежать.

Для полного понимания этого термина приведем определение понятия контент. Контент – это наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т.д.. Например: контент интернет-сайта; мобильный контент – мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.).

Информация нежелательного характера, которая несет в себе контентные ***риски***, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относится:

- информация о насилии, жестокости и агрессии,
- информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам,
- пропаганда суицида,
- пропаганда азартных игр,
- пропаганда и распространение наркотических веществ, отравляющих веществ,
- пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи),
- пропаганда деятельности различных сект, неформальных молодежных движений,
- эротика и порнография,
- нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, торрентах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Распространение **противозаконной информации** преследуется по закону, например, распространение наркотических веществ через Интернет, порнографических материалов с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям. Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение противозаконной информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального

характера, порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др.

Неэтичная и **вредоносная** информация может быть направлена на манипулирование сознанием и действиями различных групп людей.

Это могут быть сайты, на которых люди обсуждают способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, и даже сайты, на которых описываются способы самоубийства. Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных, например, просмотр тех или иных видеоматериалов через сеть интернет приводит к заражению компьютера вирусами. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия могут преследоваться по закону в соответствии со статьями Уголовного кодекса РФ (ст. 272,273,274).

Что надо знать о проблемах недостоверной информации в Интернете?

В Интернете есть большая доля информации, которую никак нельзя назвать ни полезной, ни надежной, ни достоверной. Пользователи Сети должны мыслить критически, чтобы оценить достоверность, актуальность и полноту информационных материалов; поскольку абсолютно любой может опубликовать информацию в Интернете. В Интернете не существует служб редакторов и корректоров (такие службы функционируют только в электронных средствах массовой информации), никто не проверяет информационные ресурсы на достоверность, корректность и полноту. Поэтому нельзя использовать Интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативно-правовых актов и т.п..

Рекомендации для родителей по предупреждению контентных рисков «Как избежать материалов с нежелательной информацией»:

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Перечень специальных программных фильтров (интернет-фильтров) приведен в приложении 1. Почти каждый Интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика Интернет-браузеров можно найти подобную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержимое в Интернете могут просматривать их дети, отсекать «плохие» сайты, содержащие нежелательную информацию, в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался Интернетом, устанавливать ограничения пользования компьютером и Интернетом по времени. Родительский контроль можно устанавливать непосредственно с помощью операционной системы (например,Windows), антивирусных программ (например, антивирус Касперского), специальных программ.
2. Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.
3. Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в компьютер (систему) независимо и иметь собственный уникальный профиль Ребенок сможет входить в систему только под своим логином и паролем, не имея административных прав на контроль системных настроек, установку программ. Учетная запись администратора должна быть у родителя, тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Для работы в Интернете необходимо создавать надежные и защищенные пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

4. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра.

Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред такой информации.

Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с Вами.

1. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают**:** авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных.
2. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Безопасное общение детей в интернете или коммуникационные риски общения в Интернете

Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Интернет - это не только средство массовой информации и всемирный справочник, но и среда для общения. В интернете существует много инструментов, позволяющих организовать места для общения – социальные сети, блоги, чаты, форумы, гостевые книги, списки рассылки и пр.

Примерами коммуникационных рисков могут быть: знакомства в сети и встречи с Интернет -знакомыми, интернет-хулиганство: преследование, запугивание и оскорбления (кибербуллинг), незаконные контакты, и др. С коммуникационными рисками можно столкнуться при общении в мобильных

сервисах, чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д.

Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг) – это явления не только виртуальной, но и реальной жизни. 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. Буллинг, осуществляемый в виртуальной среде с помощью Интернета и мобильного телефона, называют кибербуллингом. Кибербуллинг, преследование с использованием цифровых технологий, сильнее всего действует на детей и подростков.

Кибербуллинг не менее опасен, чем реальные издевательства. Если террор может закончиться, когда жертва вернется домой или пожалуется старшим, то кибербуллинг продолжается все время и от него невозможно спрятаться. В отличие от реальной травли, для кибер-буллинга не нужно быть здоровяком, достаточно компьютера, времени и желания кого-то терроризировать. Распространение кибербуллинга, во многом, отражает проблемы морали в обществе, где к человеку не относятся, как к ценности, личности и игнорируют его проблемы и переживания, отвечают цинизмом.

По данным, полученным в исследовании «Дети России онлайн», в среднем по РФ 23% детей, которые пользуются Интернетом, являются жертвой буллинга онлайн или офлайн. Если сравнить виртуальность и реальность, то российские дети подвергаются буллингу в Интернете так же часто, как и в реальной жизни. Оскорбления в чатах, на форумах, в блогах и в комментариях к ним, поддельные страницы или видеоролики, на которых над кем-то издеваются или даже избивают уже давно стали привычной частью Рунета – каждый десятый ребенок 9-16 лет становился жертвой кибербуллинга.

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. Особенно остро переживают кибербуллинг дети 9-10 лет: 52% детей этого возраста, ставшие жертвой подобной ситуации, в первую очередь девочки, указали, что были этим сильно или очень сильно расстроены.

Кроме того, нередко и сами школьники выступают агрессорами. В России 25% детей признались, что за последний год обижали или оскорбляли других людей в реальной жизни или в Интернете. Обращает на себя внимание тот факт, что в России субъектов буллинга в два раза больше, чем в среднем по европейским странам.

Рекомендации для родителей по предотвращению интернет-хулиганства, 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. Признаки того, что ребёнок подвергается кибербуллингу, различны, но есть несколько общих моментов:

- признаки эмоционального дистресса на протяжении и после использования Интернета,
- прекращение общения с друзьями,
- избегание школы или школьных компаний,
- нестабильные оценки и отыгрывание злости в домашней обстановке,
- перемены в настроении, поведении, сне и аппетите
- не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками,
- склонны к депрессии и чаще своих ровесников думают о самоубийстве.

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. Большинство социальных сетей и сервисов электронной почты имеют в настройках опцию "заблокировать пользователя" или "занести в чёрный список".

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 помочь ребенку, если он уже столкнулся с какой -либо Интернет-угрозой

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.
2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате Интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.
3. Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Знакомства в Интернете и встречи с незнакомцами

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 – установление дружеских отношений с ребенком с целью личной встречи **(груминг)**, 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.

Рекомендации по предупреждению встречи с незнакомцами:

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.

Электронные риски

Электронные риски – это вероятность столкнуться с хищением персональной информации и/или подвергнуться атаке вредоносных программ.

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.

Как узнать, что ваш компьютер заражен?

Учитывая, что вирусы обычно хорошо замаскированы внутри обычных файлов, непрофессионалу трудно их обнаружить. Несмотря на это, даже неопытный пользователь, как правило, замечает, что с компьютером происходит что-то неладное: он тормозит, появляются непонятные сообщения, а иногда он просто зависает и только перезагрузка может вывести его из этого состояния.

Существуют определенные признаки, по которым, с высокой степенью вероятности, можно утверждать, что компьютер заражен вирусами:

- медленная реакция на действия пользователя, особенно при запуске программ,
- искажение содержимого файлов и каталогов или их полное исчезновение,
- частые сбои и зависания компьютера,
- самопроизвольное появление на экране сообщений или изображений,
- несанкционированный запуск программ,
- зависание или странное поведение интернет-браузера,

- невозможность перегрузки компьютера (операционная система не загружается).

Однако нужно помнить, что ничто не может дать стопроцентной гарант ии защиты вашего компьютера. Поэтому в любом случае Вы и Ваши д ети должны быть крайне внимательны, когда получаете сообщения по электронной почте от неизвестного адресата с вложением, когда скачиваете файлы из Интернета, пользуетесь чужими носителями информации или открываете файлы, скопированные с чужого компьютера.

Рекомендации по снижению рисков заражения компьютера вирусами и хищению персональной информации:

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.

Потребительские риски

Потребительские риски - злоупотребление в Интернете правами потребителя, включают в себя:

- хищение персональной информации с целью кибермошенничества,

- потеря денежных средств без приобретения товара или услуги,

- риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию,

- азартные игры на деньги.

Хищение личной информации

Кража личных данных или кибермошенничество – любой вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в Интернете. Хищение личных данных через Интернет иногда называется *фишингом*.

Многие интернет-аферы – это варианты мошеннических схем, существовавших еще до появления Сети, число которых увеличилось вместе с популярностью онлайн-шоппинга и других типов электронной коммерции. Для обмана пользователей интернет-мошенники используют электронную почту, чаты, форумы и фальшивые веб-сайты.

Виды кибермошенничества: вишинг, фишинг, фарминг, нигерийские письма и т.п (см. словарь терминов).

Вы можете самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками.

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытия ваших банковских счетов;

- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

- сведения о сделках, которые слишком хороши, для того, чтобы быть правдой;

- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;

- грамматические и орфографические ошибки.

Рекомендации по предупреждению 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.
- Обратите внимание на правила Интернет-магазина.
- Выясните, сколько точно вам придется заплатить.

1. Посещая веб-сайты, нужно самостоятельно набирать в браузере адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.
2. Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.
3. Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что

конфиденциальная информация была предоставлена вами или ваши ми детьми неизвестным лицам, выдающим себя за сотрудников то й или иной компании либо организации. При немедленном обращ ении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Интернет-зависимость

То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветство вали появление Сети, полагая, что она – безграничный источник новых знаний. Вскоре выяснилось, что подростки не столько пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в он-лайновые игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей; Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени, появляется интернет-зависимость.

Обратите внимание на психологические особенности вашего ребенка. Социально дезадаптированные дети имеют повышенную вероятность к приобретению Интернет-зависимости. Причина в том, что Интернет позволяет оставаться анонимным, не бояться осужд ения (если что-то сделал неправильно, всегда можно поменять имя и начать все заново), предоставляет гораздо более широкий выбор возможностей к общению, чем реальный мир.

В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет комфортным. Поэтому, если у ребенка что-то не получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

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.

В случае Интернет-зависимости выделяют следующие типы онлайн-активности:

- навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации,
- пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети),
- игровая зависимость – навязчивое увлечение компьютерными играми по сети,
- навязчивое желание потратить деньги – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянное участие в интернет-аукционах,
- пристрастие к просмотру фильмов через Интернет.

Рекомендации по предупреждению Интернет-зависимости

В первую очередь необходимо обратить внимание на возможные признаки Интернет-зависимости у вашего ребенка.

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.

Если вы обнаружили возможные симптомы Интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

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.