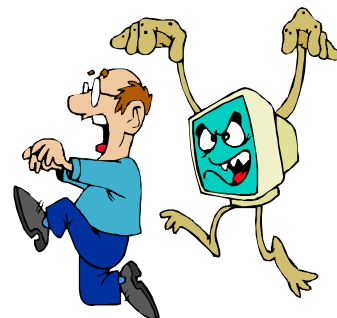


Тема 4.2. Безопасное общение детей в Интернете.

Если ребенок только начал общение с Интернетом, необходимо познакомить его с практическими способами безопасной работы в Интернете. Противостояние угрозам из Интернета включает два основных момента: во-первых, находясь в Интернете не нужно терять бдительности и поддаваться ухищрениям злоумышленников, реализующим атаку на локальный компьютер. Во-вторых, необходимо построить защиту компьютера, которая будет включать в себя надежное приложение-антивирус, а также новейшую версию браузера для работы в Интернете с предварительно настроенными параметрами безопасности. Приведем некоторые рекомендации, которым необходимо следовать:



- Работу с электронной почтой лучше всего осуществлять с помощью почтовых сервисов Web-сайтов, которые выполняют антивирусную проверку почтовых сообщений.
- Можно использовать «временный» адрес электронной почты: спаммеры эффективно собирают адреса электронной почты из всех видов источников, поэтому будет лучше использовать такие адреса, от которых вы готовы избавиться через 6 месяцев или через год, если объем спама станет большим.
- Запомните, что если вы используете почтовый клиент, никогда не конфигурируйте его на автоматическое открытие почтовых вложений. Любое послание от любого лица может содержать вложение самого опасного характера, поскольку его может послать кто угодно, в том числе вирус, заразивший компьютер отправителя.
- Обычно предпочтительнее выступать на форумах с модераторами - такими, где определенному человеку (именуемому «модератор») поручено следить за поведением участников и реагировать на плохое поведение и появление плохих личностей.
- Знайте, что специфика общения в Интернете такова, что она имеет тенденцию притягивать негатив. Будьте очень рассудительны в том, как вы описываете вещи, следите за языком, который может непреднамеренно передавать враждебность. Поддержание собственной безопасности в Интернете означает защиту самого себя от непреднамеренного провоцирования ссор и злой воли.
- Используйте в письмах шаблонные приветствия и благодарности, которые вставляются в начало или конец каждого послания. Ведь электронное послание лишь создается в Сети – прочитает его все равно живой человек.



- Непосредственно перед отправкой специалисты советуют всегда производить контрольное прочтение. Таким образом, можно убедиться, что приложены все файлы, а в сообщении все же написано то, что запланировано.
- Следите за поведением своего компьютера, когда посещаете Web-сайты. Если компьютер начинает проявлять подозрительную активность или процессор по непонятным причинам начнет перегружаться, проверьте с помощью диспетчера задач, что у вас запущено. Настораживать должны непонятные сообщения, некорректное и нелогичное поведение браузера и т.п. В крайнем случае, прервите соединение.

В Интернете также широко распространены службы для мгновенного обмена сообщениями и онлайн-общения (Windows Live Messenger, ICQ, IRC, чаты). Эти службы также могут таить в себе опасности при их использовании детьми, поэтому необходимо придерживаться некоторых правил.

Общение с помощью IRC (ретранслируемый Интернет-чат)

С помощью IRC (система диалогового общения по Интернету) в Интернете можно проводить беседы в режиме реального времени. Эта система предоставляет более широкий выбор возможностей, чем простой чат. Для подключения к необходимым каналам (дискуссионным группам или комнатам) необходима отдельная программа — клиент IRC. С помощью IRC можно одновременно общаться на нескольких каналах, а также вести личные беседы между двумя людьми. В IRC применяются те же правила безопасного использования, что и для чатов.

Мгновенный обмен сообщениями (Windows Live Messenger, ICQ и т.п.)

Так же, как и чаты, программы мгновенного обмена сообщениями позволяют общаться в режиме реального времени. Разница заключается в том, что пользователь может выбирать человека, с которым он хочет пообщаться. В программе отображаются те друзья, которые в настоящее время находятся в Интернете. Для участия в личной беседе можно пригласить одного или нескольких друзей. Кроме того, можно обмениваться файлами, например, фотографиями, музыкальными файлами или видеоклипами, играть в игры или совершать голосовые или видеовывозы.

Технология программ мгновенного обмена сообщениями подвержена тем же рискам, что и электронная почта с чатом. Пользователь может открыть вложение или ссылку, содержащую вирус, шпионскую программу или непригодный для детей материал. Общение в Интернете с человеком, которого вы знаете в жизни, гораздо безопаснее. Общение с помощью программ мгновенного обмена сообщениями всегда является личным, и пользователь может контролировать не только то, с кем и как он разговаривает, но и время разговора.

Общение в чатах

Для общения в Интернете также используют чаты. Чатом называется открытая дискуссионная группа в Интернете, в которой можно общаться с другими людьми в режиме реального времени, используя псевдоним. Чатам и группам чатов часто присваиваются названия на основе темы или возрастной группы. В обсуждении может участвовать множество пользователей, но также возможно личное общение между двумя пользователями. Общение в чатах предполагает собственный язык, этикет и даже культуру. Родителям было бы полезно знать о таких протоколах чатов. Рекомендуется выяснить это у своего ребенка.

Что такое безопасный чат?

Человек, с которым происходит общение, в значительной степени определяет, насколько безопасной и приятной для вас является атмосфера в чате. Как правило, степень безопасности чата, в котором общается ребенок, можно определить по трем основным вопросам. Иногда в чатах работают добровольные модераторы, которые предотвращают случаи неуместного общения и могут заблокировать доступ в чат для хулиганов и других нарушителей порядка. Если контроль не осуществляется, в чате по крайней мере должна иметься кнопка для связи с администратором. Для детей предпочтительны контролируемые чаты; уровень безопасности также повышается, если беседы сохраняются.

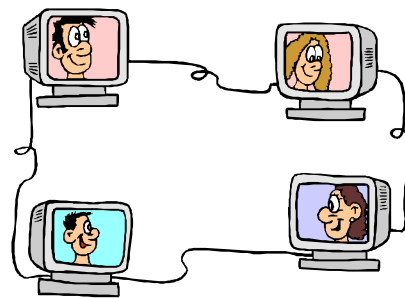
Инструкции по безопасному общению в чатах.

Дети, которые общаются в чатах, должны знать, как делать это безопасным образом. Каждый должен помнить о следующих внутренних правилах чата.

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

Личная беседа.

При знакомстве с новым человеком в интерактивной дискуссионной группе, возможно, захочется перейти от общения в общественном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к общению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте. При использовании этих



средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдоним01@домен.ru). Кроме того, проще предоставить такой тип адреса на случай, если новым контактом окажется человек, с которым необходимо будет прекратить общение. Рекомендуется наставить детей, чтобы они отказывались от участия в личных интерактивных беседах с людьми, которых они не знают в жизни.

Встреча с собеседниками из Интернета.

Если ребенок общается в Интернете с новым человеком, возможно, ему/ей захочется лично встретиться с этим другом. Даже если дружба через Интернет поддерживалась в течение некоторого времени, эту встречу стоит воспринимать с осторожностью. Несмотря на то, что большинство встреч друзей по Интернету являются веселыми и безопасными мероприятиями, к сожалению, иногда они могут оставить неприятные впечатления. К счастью, случаи подобного рода крайне редки. Если встреча запланирована, настоятельно рекомендуется сопровождение ребенка родителем или другим взрослым, которому ребенок доверяет, а также проведение встречи в общественном месте.

Интернет-этика.

Если Вы хотите, чтобы дети стали ответственными пользователями, объясните им фундаментальные правила поведения в Сети:

- Узнайте правила прежде, чем что-нибудь сказать или сделать. Некоторые чаты и форумы имеют специальные правила, поясняющие, что Вы можете и не имеете права говорить или делать. Так как некоторые люди критически относятся к тем, кто нарушает правила, знание правил может избавить Вас и Вашего ребенка от ненужного дискомфорта.
- Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.
- Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.
- Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.



- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайн-чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использовать опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

Как не следует вести себя в Сети:

- Печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или конфликт
- Размещать ложную информацию или грубые высказывания о другом человеке
- Отправлять большие вложенные файлы, не спросив разрешения у получателя
- Обращаться к другим в чате по их настоящему имени
- Рассылать электронную почту рекламного содержания людям, которых Вы не знаете (что является разновидностью спама)
- Отклоняться от темы разговора на форуме
- Не дожидаться своей очереди или не следовать правилам чата или форума

Безопасность работы в форумах.

При работе в различного рода форумах в Интернете необходимо соблюдать все те же самые правила защиты, исходя из того, что вы находитесь на потенциально опасном ресурсе. Как и на любом другом потенциально опасном ресурсе не рекомендуется сообщать о себе любые персональные данные.

Практический совет:

Разделите форумы, которые Вы посещаете минимум на две категории: доверенные и недоверенные. Вы можете для каждой из этих групп одно и то же имя пользователя и пароль для простоты запоминания.

Если Вы создаете свой форум, то необходимо его защитить максимально доступными средствами от злоумышленников. Одно из самых важных правил – это аутентификация на форуме. При аутентификации оставлять сообщения на форуме смогут только зарегистрированные пользователи. Это хороший способ защиты, но недостаточный. Также необходимо включать премодерацию на сайте, в результате которой, сообщения предварительно просматриваются владельцем (администратором) форума и только после подтверждения печатаются на форуме.