**ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ**

**ЧЕМ ОПАСЕН ИНТЕРНЕТ ДЛЯ ДЕТЕЙ?**

В интернете можно найти информацию и иллюстрации практически на любую тему. Необходимо обеспечить защиту детей от контактов в интернете с нежелательными людьми, от знакомства с материалами недетской тематики или просто опасными для детской психики, от вредоносных программ и интернет-атак.

Так как дети по своей наивности, открытости и неопытности, не способны распознать опасность, а любознательность детей делает их крайне уязвимыми в интенет-пространстве, об их безопасности, в первую очередь, должны беспокоиться родители.

**ОПАСНОСТЬ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ МОЖНО РАЗДЕЛИТЬ НА ТРИ ВИДА:**

1. Доступная для детей негативная информация.

2. Противоправные и социально-опасные действия самого ребенка.

3. Целенаправленные действия третьих лиц в отношении ребенка.

Наиболее опасные в сервисах интернет-общения:

1. Педофилы, для которых дети становятся объектами развратных действий и преступлений против половой неприкосновенности.

2. Сектанты, навязывающие нетрадиционные, асоциальные отношения и ценности.

3. Интернет-аферисты (мошенники, онлайн-игроки и пр.), прививающие детям склонность к азартным играм, выманивающие у детей конфиденциальную информацию о родителях и уровне материальной обеспеченности семьи, а также ставящие ребенка в материальную и иную зависимость.

Среди детей приобрели моду суицид и игры со смертью, селфхарм (самоповреждение), анорексия, экстремальные селфи, а также различные радикальные движения: против родителей и семьи, школ и педагогов и прочее.

Более половины детей сталкивается с интернет-угрозами, не ставя в известность родителей, в ряде случаев, боясь их, в ряде случаев, не доверяя.

Как правило, родители не уделяют большого значения интернет-безопасности и интернет-воспитанию детей.

В интерактивном мире дети могут быть так же беззащитны, как и в реальном. Поэтому важно сделать все возможное, чтобы защитить их.



**РЕКОМЕНДАЦИИ:**

1. Расположить ребенка к доверительному диалогу по вопросам интернет-безопасности. Объяснить, что Интернет является не только надежным источником информации, но и опасным собеседником, а доверять следует родителям, педагогам и лучшим друзьям.

2. Установить с ребенком «правила» работы с компьютером и гаджетами, временные ограничения, определить ресурсы, которые можно и нужно посещать. Объяснить, что Интернет, в первую очередь, является средством развития и обучения, и только второстепенно — развлечений и общения. Желательно договориться, что новые игры и программы будут устанавливаться совместно с родителями.

3. Ввести ограничения по использованию гаджетов. Дошкольникам, а также ученикам младших классов мобильный Интернет не нужен в повседневной жизни.

4. Запретить общение с незнакомыми людьми. Эта мера должна восприниматься так же, как и запрет общения с незнакомыми на улице!

5. Привить культуру поведения в IT-пространстве, постоянно осуществляя интернет-воспитание ребенка.

6. Надлежащим образом настроить компьютерную технику ребенка. Использовать контент-фильтры, затрудняющие посещение определенных видов ресурсов на уровне оператора связи и на уровне операционной системы. Контент-фильтрация не всегда эффективна, в частности, из-за того, что не ко всем сайтам закрыт доступ, а социальные сети, онлайн-игры, переписка и иная активность ребенка остаются в стороне!

7. Контролировать деятельность ребенка с компьютером и гаджетами, в частности, при помощи средств родительского контроля. При этом, ребенку нужно объяснить, что Вы это делаете для того, чтобы предотвратить опасность, и что на это имеете полное право. Знайте, что дети способны удалять историю переписки и посещения сайтов, существует множество средств родительского контроля, которые необходимо использовать для того, чтобы обезопасить своего ребенка.



**НЕСКОЛЬКО СОВЕТОВ ПО ОБЕСПЕЧЕНИЮ ИНТЕРНЕТ-БЕЗОПАСНОСТИ:**

• Расскажите своим детям о потенциальных угрозах, с которыми они могут столкнуться в интернете.

• Если возможно, поставьте компьютер в общей комнате.

• Постарайтесь проводить время за компьютером всей семьей.

• Попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении интернета.

• Ограничьте материалы, доступные детям через компьютер.

Вам помогут сделать это антивирусные программы и сами браузеры.

Так, например, Internet Explorer включает компонент Content Advisor, а Kaspersky Internet Security компонент «Родительский контроль».

Объясните детям, что им разрешено, а что запрещено делать в интернете:

• Регистрироваться в социальных сетях и на других сайтах.

• Совершать покупки в интернете.

• Скачивать музыку, игры и другой контент в интернете.

• Использовать программы мгновенного обмена сообщениями.

• Посещать чаты.

Если детям разрешено использовать программы мгновенного обмена сообщениями или посещать интернет-чаты, расскажите им об опасностях общения или отправки сообщений людям, которых они не знают и которым не доверяют.

• Установите надежную антивирусную программу, способную защитить компьютер от вредоносных программ и хакерских атак. Многие продукты для обеспечения безопасности в интернете сочетают в себе возможности антивирусной защиты и расширенные функции родительского контроля, которые помогают защитить детей, когда те находятся в интернете.

Контроль переписки через социальные сети с помощью функции «Родительский контроль» позволяет:

Сформировать списки контактов, переписка с которыми будет разрешена или запрещена.

Задать ключевые слова, наличие которых будет проверяться в сообщениях.

Указать личную информацию, пересылка которой будет запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные этому контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. Для каждой учетной записи пользователя компьютера можно посмотреть краткую статистику переписки через социальные сети, а также подробный отчет о событиях.

По материалам: Центра развития ребёнка — детский сад «Улыбка» с.п. Салым.
Рубрика: Информационная безопасность.