Работа с родителями и детьми по использованию

ИКТ и Интернет-безопасности

***Видео по безопасности школьников в сети Интернет***

1.[Урок по безопасности школьников в сети Интернет](https://youtu.be/9OVdJydDMbg)

2. [Мультфильм «Безопасный интернет»](https://youtu.be/InAUvJzTnaY)

3. [10 советов по безопасности сети Интернет](https://youtu.be/1IiEiPo3tzQ)

***Советы родителям для обеспечения безопасности детей при работе в Интернете.***

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. Все большее количество детей получает возможность работать в Сети. **И**нтернет это полезная и интересная вещь, если правильно ею пользоваться, но у всякой медали есть своя оборотная сторона. Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.
 **Возможные опасности, с которыми сопряжен доступ детей к Интернету:**- Неприемлемые материалы. В Интернете ребенок может столкнуться с материалами, связанными с сексом, наркотиками, страницами, подталкивающими молодежь к самоубийствам, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;

- Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов;

- Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол, и информация о семье могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации;

- Угроза заражения вредоносным ПО. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, “червь”, “троянский конь”, “зомби” или другой код, разработанный со злым умыслом.

**Меры предосторожности:**Побеседуйте с детьми. Первое, что необходимо сделать, — это объяснить детям, что нахождение в Интернете во многом напоминает пребывание в общественном месте. Многие опасности, подстерегающие пользователя Интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт, лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности.

**Разработайте правила пользования Интернет:**- Четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при пользовании Интернетом. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами;

- Пароли. Предупредите детей о том, что они не должны никому сообщать свои пароли, даже если человек утверждает, что является сотрудником вашего поставщика Интернет-услуг (например представляется вашим провайдером). Поставщик услуг Интернета никогда не будет спрашивать, какой у вас пароль;

- Разработайте “домашнюю” политику. Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании Интернета. Например: Нельзя разглашать информацию личного характера. Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию. Ребенок ни в коем случае не должен соглашаться на личную встречу с “виртуальным” другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых;

* Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

- Следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемыми и поддерживается заслуживающей доверия компанией или организацией;

- Установите компьютер в помещении, используемом всеми членами семьи, а не в комнате ребенка. Это упростит контроль за пребыванием детей в Интернете. Воспользуйтесь современными технологиями;

- Контролируйте входящие и выходящие сообщения электронной почты своего ребенка. Знакомьтесь с его “виртуальными” друзьями подобно тому, как вы знакомитесь с “реальными”;

- Регулярно просматривайте журнал веб-обозревателя. Из него вы узнаете, какие веб-узлы посещали ваши дети и как часто они это делали;

* Настройте веб-обозреватель в режиме обеспечения безопасности;
* Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
* Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

**Помните!**Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании Интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.

***Интернет и дети***

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Рассмотрим распространенные опасности и правила борьбы с ними:

**Преступники в интернете: что можно сделать для снижения опасности**

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию.

КАК УЗНАТЬ, НЕ СТАЛ ЛИ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

* Ребенок проводит много времени в Интернете.
* В компьютере появились материалы откровенного содержания.
* Ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы.
* Ребенок получает письма, подарки или посылки от неизвестного вам лица.
* Ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.
* Ребенок использует чью-то чужую учетную запись для выхода в Интернет.

ЧТО ДЕЛАТЬ, ЕСЛИ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

* Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.
* Контролируйте доступ ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.
* Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.
* Если ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

**Вредоносные и нежелательные программы в интернете**

ЧТО ТАКОЕ ВИРУС? Вирус – это программа, которая может проникнуть в компьютер различными путями (через электронную почту, Интернет, различные виды дисков и т.д.) и вызвать эффекты, начиная от просто раздражающих до очень разрушительных, способны размножаться, заражая другие файлы и программы.

ЧТО ТАКОЕ НЕЖЕЛАТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ? Под выражением «нежелательное программное обеспечение» понимаются программы, которые выполняют на компьютере некие задачи без вашего согласия. Они могут показывать рекламные сообщения, объявления или собирать личные данные о вас и вашей семье.

ВРЕДОНОСНЫЕ ПРОГРАММЫ МОГУТ ВЫПОЛНЯТЬ СЛЕДУЮЩИЕ ДЕЙСТВИЯ:

* устанавливать соединение с вашего компьютера наружу;
* разрешать управление вашим компьютером извне;
* собирать вашу конфиденциальную информацию (шпионские программы);
* отображать нежелательную и рекламную информацию (рекламные программы);
* отслеживать нажатие клавиш (кейлоггеры);
* гарантировать повторное заражение даже после очищения (руткит).

КАК СНИЗИТЬ РИСК ЗАРАЖЕНИЯ?

Необходимо постоянно улучшать защиту компьютера. Есть три основных шага, которые необходимо сделать, чтобы обеспечить защиту своего компьютера:

* применяйте межсетевой экран;
* выполняйте обновления;
* применяйте новейшие антивирусные программы.

**Материалы нежелательного содержания: как избежать?**

ЧТО ЗНАЧИТ НЕЖЕЛАТЕЛЬНОЕ СОДЕРЖАНИЕ.

Материалы порнографического, ненавистнического содержания, материалами суицидальной направленности, сектантские материалы, ненормативной лексики.

КАК ПОМОЧЬ ДЕТЯМ ИЗБЕЖАТЬ НЕНАВИСТНИЧЕСКИХ МАТЕРИАЛОВ?

* Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®).
* Контролируйте использование Интернета и наблюдайте за детьми.
* Научите детей критически относиться к содержанию онлайновых материалов и не доверять им.

**Интернет-мошенничество и хищения данных кредитной карты**

Интернет-мошенники – хакеры применяемые технику «phishing», состоящую в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

**СНИЖЕНИЕ РИСКА ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ**.

* Самостоятельно набирайте в обозревателе адрес веб-сайта или пользуйтесь ссылкой из «Избранного» (Favorites);
* Никогда не щелкайте на ссылку, содержащуюся в подозрительном электронном письме.
* Как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации
* 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.

ЧТО ДЕЛАТЬ В СЛУЧАЯХ ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ?

* Измените пароли.
* Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
* 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.
* Записывайте и сохраняйте абсолютно все.
* После выполнения всех действий всегда делайте копии документов.

**Памятка для детей по безопасному поведению в интернете**

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, предпринимайте следующие меры предосторожности при работе в Интернете:

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

2. Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

3. Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.

4. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

6. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

7. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.