

«Формирование у детей представлений о безопасности при использовании сети Интернет»

Почти 2 млрд. людей в мире подключены к сети Интернет. Ежегодно растет число пользователей, среди которых все больше – детей и подростков. Еще пять лет назад пользователями Интернета были преимущественно жители крупных городов. Сейчас же благодаря развитию мобильного Интернета, проникновение сети стремительно растет даже в небольших населенных пунктах, а возраст пользователей снижается до 6-7 лет.

С каждым годом все больше детей обращается к Интернету, используя доступ не только через компьютер, а и через мобильные телефоны, что актуализирует проблему онлайн-безопасности детей. По результатам исследования Института социологии «Знание и отношение к вопросу безопасности детей в Интернете» выяснилось, что 78% родителей не знают о проблемах безопасности детей в Интернете. Около 28% детей готовы переслать свои фотографии незнакомым людям, а увидев в Интернете рекламу алкоголя или табака, хотя раз пробовали их купить, 11% — пытались купить наркотики. Кроме того, 17% детей без колебаний соглашаются сообщить личную информацию о себе и своей семье, 22% детей периодически попадают на сайты для взрослых, и только в 18% случаев взрослые проверяют, какие сайты посещал ребенок.

Причины разные – кто-то не знает, какие ресурсы могут быть опасными, а кто-то попросту не умеет пользоваться журналом посещения сайтов. Большинство родителей опасаются, что у ребенка ухудшится зрение от компьютера, потому просто ограничивают время использования ребенком Сети. Только малая часть родителей знают о таких онлайн угрозах, как взрослый контент, азартные игры, онлайн-насилие, мошенничество и другие.

В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Наша задача сегодня – обеспечение безопасности детей, не способных иногда правильно оценить степень угрозы информации, которую они воспринимают или передают, так как темпы информатизации оказались столь быстрыми, что и семья и школа оказались не готовы к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Какие же опасности ждут школьника в сети Интернет? Прежде всего можно выделить следующие:

- суицид-сайты, на которых дети получают информацию о «способах» расстаться с жизнью;
- сайты-форумы потенциальных самоубийц;

- наркосайты. Интернет пестрит новостями о "пользе" употребления марихуаны, рецептами и советами изготовления "зелья";
- сайты, разжигающие национальную рознь и расовое неприятие;
- экстремизм, национализм, фашизм;
- сайты порнографической направленности;
- сайты знакомств. Виртуальное общение разрушает способность к общению реальному, "убивает" коммуникативные навыки подростка;
- секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам "проникнуть в мысли" и повлиять на взгляды на мир.

Это далеко не весь список угроз сети Интернет. Любой школьник может попасть на такие сайты случайно: кликнув по всплывшему баннеру или перейдя по ссылке.

Кроме этого, появились психологические отклонения, такие как компьютерная и Интернет–зависимость, игромания (зависимость от компьютерных игр).

ПРЕСТУПНИКИ В ИНТЕРНЕТЕ:

Пользуясь возможностями Интернета, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в Интернете способствует быстрому возникновению доверительных и дружеских отношений. Преступники этим и пользуются. Вы сможете защитить своих детей, если поймете возможную опасность общения через Интернет и будете в курсе того, чем они занимаются в Сети.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. 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. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаются ослабить моральные запреты, сдерживающие молодых людей. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

КАК УЗНАТЬ, НЕ СТАЛ ЛИ ВАШ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЮ ПРЕСТУПНИКА?

- Ваш ребенок проводит много времени в Интернете, особенно в чатах, закрывает дверь в свою комнату и скрывает, чем он занимается, сидя за компьютером.
- В семейном компьютере появились материалы откровенного содержания.
- Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам неизвестны.
- Ваш ребенок получает письма, подарки или посылки от неизвестного вам лица. Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки.
- Ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.

Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЮ ПРЕСТУПНИКА?

- Регулярно проверяйте компьютер на наличие материалов откровенного характера.
- Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта.
- 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.

ЧТО НАДО ЗНАТЬ О ВРЕДОНОСНЫХ И НЕЖЕЛАТЕЛЬНЫХ ПРОГРАММАХ В ИНТЕРНЕТЕ

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для

распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

ЧТО ТАКОЕ ВИРУС? Вирусы – это программы, которые мешают нормальной работе компьютера, перезаписывают, повреждают или удаляют данные. Они также распространяются между компьютерами в Сети и через Интернет, часто замедляя их работу и вызывая другие неполадки.

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.

КАК МОЖНО ОПРЕДЕЛИТЬ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН?

Ваш компьютер может начать работать медленнее или прекращать работать и перезагружаться каждые несколько минут. Иногда вирус атакует файлы, необходимые для запуска компьютера. В подобном случае вы можете, нажав кнопку запуска, обнаружить, что смотрите на пустой экран.

КАК СНИЗИТЬ РИСК ЗАРАЖЕНИЯ?

- Необходимо постоянно улучшать защиту вашего компьютера. Вирус запускается в тот момент, когда вы открываете вложенный инфицированный файл.
- Потребуйте от детей никогда не открывать никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда они ожидают получение вложения и точно знают содержимое такого файла.
- Если дети регулярно пользуются компьютером, они могут забрести на сайты или скачать файлы, которые могут заразить компьютер. Иногда ваши дети могут случайно заразить компьютер программой-шпионом, даже не осознавая этого.

Совет: Ключевое правило, которого следует придерживаться, – это скачивать файлы из надежных источников и обязательно читать предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности. Скажите детям, чтобы они спрашивали у вас разрешение перед тем, как загрузить что-либо из Сети.

ЧТО НАДО ЗНАТЬ ОБ ИНТЕРНЕТ-МОШЕННИЧЕСТВЕ И ХИЩЕНИЯХ ДАННЫХ КРЕДИТНОЙ КАРТЫ

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing», состоящая 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.

АЗАРТНЫЕ ИГРЫ В ИНТЕРНЕТЕ: КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ?

В ЧЕМ СОСТОИТ ОТЛИЧИЕ МЕЖДУ ИГРОВЫМИ САЙТАМИ И САЙТАМИ С АЗАРТНЫМИ ИГРАМИ.

Множество детей обожают искать развлечения (например, игры) в интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако им нельзя играть в азартные игры на деньги. Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ ОТ ИГР НА ДЕНЬГИ?

Родители должны решить, во что можно играть их детям. Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей. Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги. Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца. Получите информацию. Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры. Будьте в курсе, в какие игры и с кем играют ваши дети. Контролируйте чат и сообщения во время игр. Попросите детей сообщать вам, если другой игрок употребляет нецензурные слова. Требуйте от детей никогда не выдавать в игровом чате личную информацию (например, имя, пол или домашний адрес, фотографии) и не соглашаться на встречи.

КТО ТАКИЕ ИНТЕРНЕТ-ХУЛИГАНЫ И ЧТО ОНИ ДЕЛАЮТ? Их называют гриферами, задирами, дурными игроками и т.д. Есть вероятность, что один из

таких злодеев по крайней мере единожды побеспокоит вашего ребенка в таких многопользовательских играх, как, EverQuest, The SimsOnline, SOCOM и Star Wars Galaxies. Обидчики (гриферы), по сути, те же дворовые хулиганы; они получают удовольствие, хамя и грубя окружающим.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: О симптомах интерне-зависимости мы уже говорили, а как бороться?

- Навязчивое использование Интернета может быть симптомом других

проблем, таких, как депрессия, раздражение или низкая самооценка. И когда эти проблемы будут решены, зависимость от Интернета может пройти сама собой.

- Не запрещайте Интернет. Для большинства детей он является важной частью их общественной жизни. Вместо этого установите «Внутрисемейные правила использования Интернета»
- Помогайте ребенку участвовать в общении вне Интернета. Предложите альтернативы. Если вам кажется, что ваши дети интересуются только онлайн-овыми развлечениями, попробуйте предложить им автономный аналог. Например, если ваш ребенок получает удовольствие от игр на тему фэнтези, предложите ему почитать книги той же тематики.

Как обеспечить безопасность своих данных в соцсети

Социальные сети, такие как Одноклассники, Вконтакте, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными. По мере роста популярности таких сайтов растут и риски, связанные с их использованием.

Правила безопасности при использовании социальных сетей

- **Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.** Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.
- **Контролируйте информацию о себе, которую вы размещаете.** Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов

необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.

- **Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.** Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Точно также необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.
- **Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.** При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны указывать то, что эти адреса электронной почты будут использованы для этой данной, но зачастую не делают этого.
- **Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.** Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
- **Не добавляйте в друзья в социальных сетях всех подряд.** Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
- **Не регистрируйтесь во всех социальных сетях без разбора.** Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.
- **Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.** На большинстве

сервисов вы можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.

- **Проявляйте осторожность при установке приложений или дополнений для социальных сетей.** Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьезно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.
- **Старайтесь не посещать социальные сети с рабочего места.** Любая социальная сеть может стать средой для распространения вирусов и других вредоносных или шпионских программ, что может привести не только к заражению вашего компьютера и всей корпоративной сети, но и к потере данных, составляющих коммерческую тайну вашей компании.

10 Правил Интернет-безопасности для детей

ДЕТИ ДОЛЖНЫ:

1. **Никогда не показывать личную информацию в Интернете,** такую, как адрес, номер телефона, имя, расположение школы, имена родителей. Веб-сайты или другие онлайн-сервисы могут попросить детей дать информацию для того, чтобы участвовать в конкурсах или получить бесплатные подарки. Некоторые веб-сайты не позволяют доступа, если пользователь не дает им личной информации. Однако, как только личная информация дана, важно, чтобы ваши дети понимали, что их конфиденциальность может быть нарушена. Их имена могут в конечном итоге пойти на продажу в базе данных, или еще хуже, эта информация может быть использована для причинения вреда или их эксплуатации.
2. **Будьте осторожны при разработке веб-сайта.** Сейчас многие дети имеют свои личные веб-сайты. Дети должны знать, что никогда не следует оставлять домашний адрес, номер телефона или личную фотографию на сайте. Если дети хотят получать информацию от посетителей своего сайта, которые хотят связаться с ними, они могут размещать адреса электронной почты. Тем не менее, дети должны знать, что на адрес электронной почты они могут получать нежелательные письма. Они должны быть очень осторожными при открытии любой электронной почты от неизвестных адресов. Если дети получают сообщения, которые являются угрожающими или сексуальными, они должны немедленно сообщить своим родителям.
3. **Всегда информировать своих родителей, когда они сталкиваются с чем-нибудь в Интернете, что заставляет их чувствовать себя неловко**
4. **Никогда, ни при каких обстоятельствах не соглашаться встретиться лицом к лицу с виртуальным знакомым с кем переписывались в Интернете без разрешения**

родителей. Если всё-таки встреча состоится, - она должна быть в общественном месте и родители должны всегда сопровождать ребенка.

5. Избегать чатов, которые обсуждают секс или религиозные культы. Хотя эти вопросы могут показаться интересными сначала, они могут предоставлять опасность для ребёнка. Многие культы и секты охотятся на подростков в сети

6. Не доверять никому, кого они встречают в чатах , и кто пытается повернуть их против своей семьи, друзей, учителей или религии.

7. Выбрать гендерно-нейтральное (скрывающее пол) онлайн имя в чате, чтобы избежать преследований.

8. Никогда не отвечать на сообщения или объявления, которые являются сексуально непристойными, угрожающими, или заставляющими себя чувствовать неловко в любом случае.

9. Никогда не отправлять личные материалы для онлайн-друзей, такие, как адрес, номер телефона или фотографии, без предварительного информирования родителей.

10. Всегда напоминайте детям, что люди, которых они встречаются в Интернете могут быть не теми, кем они кажутся.

ЗОНЫ БЕСПРОВОДНОГО Wi-Fi

Соседи по зоне Wi-Fi обычно не представляют угрозу для конфиденциальности ваших данных, однако вам необходимо помнить о более серьезной опасности: [киберпреступниках](#). Эти технически грамотные хакеры располагают специальными инструментами, навыками и терпением для обхода тех недостаточных мер защиты, которые применяются в общедоступных зонах Wi-Fi. Некоторые киберпреступники используют психологические уловки, вынуждая пользователей Wi-Fi раскрыть конфиденциальную информацию. Так называемый фишинг- Wi-Fi, принцип тот же, что и оговаривался выше, все приводит к требованиям ввести какие-либо личные данные.

Советы по обеспечению безопасности в общественных зонах беспроводного доступа

Вы сами несете ответственность за собственную безопасность при использовании общественных зон беспроводного доступа. Запомните следующие рекомендации:

- Будьте внимательны к соседям. Убедитесь, что никто не подглядывает за вами, когда вы вводите данные учетной записи операционной системы, электронной почты, системы обмена мгновенными сообщениями и т. п.
- Не оставляйте портативный компьютер или карманное устройство без присмотра даже на секунду.

- Запретите автоматическое подключение адаптера Wi-Fi к ближайшей сети. Выбирайте общественную зону вручную.
- Проверьте имя сети и параметры подключения, чтобы убедиться в законности точки беспроводного доступа.
- Отключите совместный доступ к файлам и храните как можно меньше личных, конфиденциальных сведений на портативных компьютерах и мобильных устройствах. Обычно совместный доступ к файлам можно отключить в разделе параметров сети операционной системы.
- Не работайте с электронными банками и Интернет-магазинами, находясь в зоне беспроводного доступа. Выбирайте для этого более защищенную и управляемую среду.
- Не используйте электронную почту и мгновенные сообщения для передачи важной информации. При использовании мгновенных сообщений или электронной почты в общественных зонах беспроводного доступа никогда не отправляйте информацию, которую не следует знать посторонним. Рекомендуется создать отдельную учетную запись электронной почты для использования в общественных зонах Wi-Fi.
- Не просматривайте веб-сайты, о которых не должны знать посторонние люди.
- Выключайте адаптер Wi-Fi, когда вы его не используете.
- Находясь в общественной зоне беспроводного доступа, вы не можете знать, какие вирусы могут быть на других компьютерах или подключен ли хакер к сети.
- Принимайте обдуманные решения. Никогда не используйте общественные зоны беспроводного доступа для передачи важной информации.

