ПРИЛОЖЕНИЕ

Информационные материалы для участников образовательного процесса по вопросам безопасного поведения в Интернет-пространстве, профилактики Интернет – зависимости, предупреждения рисков вовлечения в противоправную деятельность

ИНТЕРНЕТ-зависимость - это миф или реальность?

Термин «интернет-зависимость» определяет проведение за компьютером в Интернет-пространстве большей части времени. Сегодня всё чаще явление интернет-зависимости прослеживается в возникающих виртуальных девиациях у наиболее незащищенных в психологическом плане социальных слоев населения, в частности, у детей и подростков. По мнению психолога Войскунского А. Е. информационные технологии способны обеспечивать широкие возможности активного взаимодействия на сознание и подсознание индивида, на его психофизиологическое и физиологическое состояние. Доказано, что интернет-зависимость угрожает нервно-психическому здоровью человека.

Основной группой риска в России становятся подростки в возрасте от 13 до 18 лет.

Вместе с тем, современный мир уже невозможно представить без интернета – он прочно вошел в повседневную человеческую жизнь. Можно привести *положительные* стороны интернет-взаимодействий, обеспечивающие реализацию базовых потребностей человека:

•познавательных (поиск новой информации, повышение квалификации, получение экспертного мнения);

• коммуникативных (родственное, интимное, дружеское, деловое общение);

•потребности в саморазвитии (творческая реализация, самообразование, демонстрация достижений);

• рекреации (игры, досуг, увлечения);

•создании отношений с другими людьми (новые знакомства, сотрудничество, поиск единомышленников, сопричастность к группе, партнерство). Виртуальные взаимодействия выступают и как способ провести время и как способ осуществить за более короткое время множество межличностных контактов, что отражает реалии «скоростного века», в котором мы живем.

Поэтому, главное руководствоваться принципом «золотой середины». Известно, что любая чрезмерная увлеченность человека чревата неблагоприятными воздействиями на его здоровье: это может выражаться от элементарного переутомления до появления зависимости.

Важно использовать интернет-пространство в разумных пределах, целесообразно (в познавательных; исследовательских целях и т.п.), осознавая, что Интернет - это не весь мир. В реальной жизни есть еще книги, спорт, друзья во дворе, наконец — родители.

Родителям следует установить правила использования домашнего компьютера и постараться найти разумный баланс между нахождением в Интернет и физической

нагрузкой ребенка. Кроме того, добиться того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых.

Даже пресловутая дилемма об увлечении детей компьютерными играми в Интернете решается в этом случае просто. Если использовать НЕРОЛЕВЫЕ логические и обучающие компьютерные игры в разумных пределах (не более 1 часа в сутки с перерывами через 15-20 минут для ребенка 6-9 лет), то они могут принести положительный результат: научат детей счету, иностранному алфавиту, улучшат мыслительные операции и т.д. Детское восприятие устроено таким образом, что для запоминания и усвоения информации нужны ассоциации, игра.

В чем всё же проявляется интернет-зависимость?

Часть современной молодежи, вместо того, чтобы активно включаться в социальные институты, организовывать семейные союзы и ориентироваться на созидательную деятельность регулярно погружается в «виртуальную реальность». Несмотря на получение бесценного опыта межличностного общения с новыми людьми, поддержание интернет-общения с несколькими получателями приводит, как правило, к поверхностным связям с коммуникаторами. В информационном пространстве интернет-общения подростков и молодежи типичным становится интолерантное поведение, которое в настоящее время часто наблюдается. Исследования, проводимые в этом направлении, показывают, что многие контакты в современном безличном городском пространстве начинаются с ненавязчивого общения, которое на последующих стадиях знакомств, незаметно превращаются в назойливые действия. Далее начинается процесс анонимного или явного преследования, когда для получения сведений о партнере по коммуникации требуются новые источники добычи информации, необходимой для продолжения и развития социальных и личных отношений в виртуальном или оффлайновом мире.

Кроме этого негативными последствиями неограниченной доступности контактов являются информационные перегрузки и психоэмоциональное напряжение. Как показывают исследования социологов, психологов и медиков, среди людей, выявленных как неумело и патологичным образом использующих интернет, нередко встречаются индивиды, страдающие разного рода сексуальными расстройствами, испытывающие навязчивые мысли, чувство страха и одиночества.

Что может способствовать вовлечению детей и подростков в интернет-зависимость?

Условно выделяемые «внешние» факторы:

• широкое распространение домашних компьютеров;

•легкость подключения к интернет-сети;

• компьютеризация школьных и студенческих программ обучения;

•большое количество клубов и интернет-салонов, особенно в крупных городах.

«Внутренние» факторы»:

• неуверенность в себе и отсутствие возможности самовыражения;

• попаданию человека в интернет-зависимость часто сопутствует явление депривации (состояние, при котором люди испытывают недостаток того, в чем они

нуждаются). Таким образом, депривация представлена как ограничение, лишение человека чего-либо, возникающее в таких жизненных ситуациях, когда затрудняется удовлетворение некоторых его потребностей в достаточной мере или в течение длительного времени.

Кто в ответе за наших детей в интернете?

1. *Государство*. Должны быть законы, которые смогли бы оградить детей от вредной информации в Интернете. Так в России все школы обязали установить программы контентной фильтрации в классах информатики.

2. *Поисковики*. Многие поисковые сервисы такие как Yandex, Ramler имеют в своем арсенале большое количество настроек и виджетов, помогающих родителям оградить детей от нежелательного контента в Интернете. А так же есть поисковые системы, предназначенные специально для детей.

3. *Семья*. Только родители могут полностью контролировать своих детей.

Как родители могут предотвратить появление Интернет-зависимости у детей?

• Уделяйте достаточное внимание своим детям, будьте в курсе их проблем. Дети и подростки нуждаются в самовыражении. За не имением других средств выражения своих мыслей и энергии они обращаются к компьютеру и Интернет-пространству, которые создают иллюзию реальности безграничных возможностей, лишенной ответственности. Это оказывает разрушительное действие на психику. В таких случаях родители должны поддержать ребенка и помочь ему разобраться с возникшими проблемами.

• Не критикуйте ребёнка, проводящего слишком много времени за компьютером. Это может только углубить проблему и отдалить ребенка от родителей. Основной мерой предотвращения возникновения зависимости любого типа у детей является правильное воспитание ребенка. *При этом важно не ограничивать детей в их действиях* (например, запрещать те или иные игры), *а объяснять, почему то или иное занятие или увлечение для него не желательно*.

• Ограничьте доступ детей к играм и фильмам, основанным на насилии. В то же время, если ребенок все же встретился с такой информацией нужно в доступной форме объяснить ему, почему такая информация для него опасна и почему он не должен стремиться узнать ее. Категорический запрет того или иного вида информации безо всяких объяснений только увеличит интерес ребенка к этой информации, а существование запрета сделает невозможным обсуждение проблемы между родителями и ребенком.

• Если ребенок страдает игровой зависимостью, нужно постараться понять его и в какой-то мере разделить его интерес к компьютерным играм. Это не только сблизит ребенка с родителями, но и увеличит его доверие к ним, а значит, ребенок с большей уверенностью будет следовать советам родителей и с большим доверием делиться с ними своими проблемами. Критика воспринимается ребенком, как отказ родителей понять его интересы и потому вызывает замкнутость и в некоторых случаях агрессию.

Как родители могут обезопасить исследование детьми интернет-пространства?

• Обращайте внимание на то, чем занимаются ваши дети в Интернете и с кем они там общаются. Родители, помните, что безопасность ваших детей в Интернете, на 90% зависит от вас. Создайте доверительные отношения между вами и вашим ребенком. Посещайте его любимые сайты иногда вместе. Если ребенок ведет дневник, время от времени прочитывайте его.
• На домашнем компьютере, который дети используют для выхода в Интернет, установите специальный фильтр, чтобы оградить детей от посещения нежелательных сайтов.
•Обсудите основы безопасного поведения в сети Интернет, опираясь на зрелость ваших детей и семейные ценности. Составьте список правил работы детей в Интернете и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без ограничений. Сейчас много интересных обучающих ресурсов для детей создается с целью обучения безопасному поведению в Сети (например, Nachalka.com)
Расскажите детям о *необходимости сохранения конфиденциальных данных в тайне и о том, как лучше это сделать*. Вот несколько простых правил, которых следует придерживаться:
- при общении использовать только имя или псевдоним (ник);
- номер телефона, свой адрес, место учебы нельзя никому сообщать;
- не пересылать свои фотографии;
- без контроля взрослых не встречаться с людьми, знакомство с которыми завязалось в Сети. Объясните, что люди в Сети часто выдают себя совсем за других. Поэтому встречаться с ними не стоит.
Поясните, *что в сети, несмотря на кажущуюся безнаказанность за какие-то проступки, там действуют те же правила, что и в реальной жизни*: хорошо - плохо, правильно - не правильно. Научите детей следовать нормам морали, быть воспитанными даже в виртуальном общении. Обязательно расскажите о правах собственности, о том, что любой материал, выставленный в Сети, может быть авторским. Незаконное копирование чужой работы — музыки, компьютерных игр и других программ — является кражей. Неправомерное использование такого материала может быть уголовно наказуемым.
Научите детей *развивать и доверять интуиции*. При малейших признаках беспокойства, путь рассказывают об этом вам.
Если детям по каким-либо причинам нужно вводить регистрационное имя, помогите его придумать так, чтобы оно не несло в себе никакой личной информации.
Объясните, что далеко не все, что можно увидеть в Интернете – правда. При сомнениях, пусть лучше уточнит у вас. Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты.

Семейное соглашение о работе в Интернет
Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно

описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:
Какие сайты могут посещать ваши дети и что они могут там делать;
Сколько времени дети могут проводить в Интернет;
Что делать, если ваших детей что-то беспокоит при посещении Интернет;
Как защитить личные данные;
Как следить за безопасностью;
Как вести себя вежливо;
Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

Учет возрастных и психологических особенностей детей при обеспечении безопасности использования Интернет-ресурсов.

Что могут делать дети в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

– В таком возрасте желательно работать в Интернет только в присутствии родителей.

– Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.

– Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети.

– Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM).

– Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

– Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье.

– Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В

результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.
Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

Что можно посоветовать в плане безопасности в таком возрасте?

– Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

– Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

– 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.

– Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля.

– Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

– Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

– Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

– Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

– Научите детей не загружать файлы, программы или музыку без вашего согласия.

– Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах http://www.microsoft.com/rus/athome/security/email/fightspam.mspx .

– Не разрешайте детям использовать службы мгновенного обмена сообщениями.

– В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

– Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

– Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых».

– Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст 9-12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

– Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

– Не забывайте беседовать с детьми об их друзьях в Интернет.

– Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.

– Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

– Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

– Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

– Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

– Расскажите детям о порнографии в Интернет.

– Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

– Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст 13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

– Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных

сайтов («черный список»), часы работы в Интернет руководство по общению в Интернет (в том числе в чатах).

– Компьютер с подключением к Интернет должен находиться в общей комнате.

– Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями чтобы убедиться, что эти люди им знакомы.

– Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

– Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте чтобы дети не общались в приватном режиме.

– Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет.

– Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

– Приучите себя знакомиться с сайтами, которые посещают подростки.

– Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

– Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните что дети не могут играть в эти игры согласно закона.

ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

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

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- 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.
- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
- 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.

–

При подключении к Интернету выполняйте следующие основные правила для обеспечения защиты устройств, информации и членов семьи

Защитите свой компьютер

• Постоянно обновляйте все программное обеспечение (включая веб-браузер),
• Установите законное антивирусное и антишпионское программное обеспечение.
• Брандмауэр должен быть всегда включен. Брандмауэр – это программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.
• Установите защиту с помощью пароля.
• Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер. Если на них имеется вирус, этот вирус может заразить ваш компьютер.

Используйте надежные пароли и храните их в секрете

• Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. Не храните пароль в браузере или на каком-либо сайте. Нельзя использовать одинаковые пароли для разных сайтов и нескольких аккаунтов (информация, при помощи которой любая система распознает Вас, проще говоря, авторизует для доступа), особенно для аккаунтов электронной почты.

Обеспечьте защиту секретной личной информации

• Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка ( ) рядом с адресной строкой, который обозначает безопасное соединение.

Основы безопасного поведения в сети Интернет

1. Посещайте веб-страницы с осторожностью. Не открывайте всплывающие окошки и яркую рекламу — это могут быть скрытые ссылки на вирусные программы. Не отвлекайтесь на баннеры с предложениями сыграть в игру или получить выигрыш. Мошеннические способы привлечения посетителей на порнографические или фальшивые сайты становятся все более изобретательными. Можно дополнительно установить специальную программу для браузера, которая будет отключать большинство всплывающих окон.
2. Прежде чем открывать вложение или переходить по ссылке, приведенной в сообщении электронной почты, мгновенном сообщении или в социальной сети, убедитесь, что отправитель действительно отправлял сообщение. Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.
3. Никогда не предоставляйте секретные сведения (такие как номер счета или пароль) в ответе на сообщение электронной почты, мгновенное сообщение или социальной сети.
4. Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на

сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

5. Безопасно используйте социальные сети. Откройте *пункт «Настройки» или «Параметры»* в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей. Никогда не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений.

Подходите избирательно к предложениям дружбы. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас.

Советы учителю, организующему обучение с помощью Интернет-ресурсов, по обеспечению безопасности:

- приучайте детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями сети (презентации; слайд-шоу и т.п.);
- поощряйте обучающихся использовать различные источники, такие как библиотеки;
- используйте закрытые среды обучения, например, учебные блоги, где могут оставлять свои комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог;
-научите ребенка пользоваться поиском в Интернет. Покажите, как использовать различные поисковые машины для осуществления поиска;
- формулируйте конкретную учебную задачу: что хочу найти? где? как использую?
- опирайтесь на список проверенных учителем ресурсов, с которых предлагается использовать информацию;

Полезные сайты:

Сайт «Защита детей от вредной информации в Интернет» - www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html;

Сайт «Личная безопасность» - www.obzh.info;

Сообщество «Начальная школа» - http://www.nachalka.com/bezopasnost

Советы по обеспечению родительского контроля в Интернете с помощью Родительского контроля в Windows Vista, средств Родительского контроля, встроенных в Kaspersky Internet Security - http://www.oszone.net/6213/

ОСНОВНЫЕ РЕКОМЕНДАЦИИ ПРИРАБОТЕ В СЕТИ ИНТЕРНЕТ, ОПУБЛИКОВАНЫ НА САЙТЕ HTTP://СЕТЕВИЧОК.РФ, РЕКОМЕНДОВАНОМ МИНОБРАЗОВАНИЕМ РФ

ПРОБЛЕМЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

Нужно ли отвечать на сообщения со спамом?

Этого не стоит делать, т.к. спамеры могут узнать о том, что твой email действующий и могут дальше отсылать тебе спам.

Прислали письмо с файлом, отправитель мне незнаком. Что делать?

Скорее всего это файл с вирусом. Чтобы знать точно, запусти проверку этого файла антивирусной программой. Но лучше сообщение удалить.

Пришло письмо с файлом от знакомого отправителя, но я не ждал этого файла. Можно ли открывать файлы от знакомых отправителей?

Не исключено, что электронная почта твоего знакомого взломана и в этом сообщении находится вирус. Если отправитель тебя не уведомлял, что планирует отправлять файлы, то лучше позвонить ему или отправить запрос по электронной почте либо в социальной сети, уточнив от него ли это сообщение.

Какой лучше выбрать адрес электронной почты?

Лучше выбрать тот адрес электронной почты, который не содержит никаких личных сведений. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «петя13».

ОБЩИЕ ВОПРОСЫ

Что такое маркировка и как она может повлиять на меня?

Маркировка - это возрастной значок, который показывает возраст, начиная с которого можно использовать данный продукт/сайт. Таким образом создатели этого контента предупреждают, что например «смотреть данный фильм можно только с 16 лет» или «играть в эту игру можно только с 6 лет». Обычно маркируются игры, фильмы и сайты. Маркировка носит рекомендательный характер для тебя, однако в магазине у тебя могут попросить предоставить документы, подтверждающие твой возраст.

Меня шантажируют видео/фотографией, что делать?

Необходимо обратиться за помощью к взрослым. Если ситуация критическая, то необходимо обращаться в полицию. В Российской Федерации есть закон о шантаже и вымогательстве, который сможет тебя защитить.

Кибербуллинг (киберзапугивание) является нарушением закона?

Кибербуллинг не попадал до недавнего времени под действие закона, но с 20012 года это является правонарушением. Для доказательства оскорбления в суде необходимо у нотариуса зафиксировать оскорбление в сети и подавать в суд.

Что такое личная информация?

Это информация о тебе: твое полное имя, фамилия и отчество, адрес, где ты проживаешь и где бываешь, номер твоей школы, твои контакты, типа мобильного телефона или логина в Skype.

Если я хочу поделиться со своим другом игрой, нарушаю ли я закон?

Да, нарушаешь закон об авторском праве . Копирование музыки, фильмов и игр, загрузка и обмен ими — это пиратство. Можно предоставить только во временное пользование диск с игрой.

ПРОБЛЕМЫ С МОБИЛЬНОЙ СВЯЗЬЮ

Мне приходят СМС с оскорблениями и унижающими текстами

Об этом нужно проинформировать родителей и вместе с ними обратиться к оператору сотовой связи с просьбой выяснить, кто это делает и заблокировать его. Если же обидчик будет продолжать свои действия, то необходимо обратиться в полицию.

Могут ли посторонние подключаться к моему Bluetooth и является ли это угрозой?

Bluetooth является угрозой в том случае, когда он открыт и на нем нет пароля доступа. Люди в зоне действия Bluetooth могут получить доступ к файлам в твоем телефоне и твои контакты.

Украли мобильный телефон. Что мне делать?

Первое – проинформируй родителей о случившемся, потом обратись к оператору сотовой связи и попроси заблокировать сим-карту, таким образом ты сохранишь свои деньги. Также необходимо предупредить всех знакомых, которые у тебя были добавлены в телефонную книгу, о том, что у тебя украли телефон, и возможно им будет идти спам от твоего имени.

Купив новый телефон и восстанавливая телефонные контакты, скопируй их на компьютер или перепиши в записную книжку.

ПРОБЛЕМЫ В СЕТИ

Надо мной издеваются в интернете

Первое, что необходимо предпринять – это собрать доказательства издевательств над тобой. Потом отправь жалобу администраторам данного ресурса с просьбой принять меры против забияки. Второе, заблокируй отправку сообщений от обидчика. И третье, прояви выдержку и не ввязывайся в конфликт.

Кто-то в сети разместил фотографию/видео со мной без моего разрешения…

Обратись к человеку, который непосредственно разместил у себя твою фотографию. Попроси его удалить эту фотографию. Если же человек отказывается, то обратись к администраторам ресурса, на котором была размещена твоя фотография. Если же и администраторы откажут, то необходимо обратиться в суд, но это ты уже должен сделать вместе с родителями.

На многих сайтах теперь можно зайти через аккаунт в социальной сети. Безопасно ли это?

Да, это безопасно. Если ты хочешь авторизоваться через какую-то социальную сеть, то должно появиться окно браузера, где будет открыт сайт этой социальной сети и у тебя уточнят, хочешь ли ты предоставить этому сайту доступ к твоему аккаунту. Если все эти условия будут выполнены, то твоя сессия от имени твоего аккаунта будет безопасна.

Какой пароль является надежным?

Восемь или не менее 8 символов в длину и содержать комбинацию букв, цифр и символов. Вот пример сложного пароля: $tR0ng!

Ты можешь оценить свой пароль на разных ресурсах, которые проверяют надежность паролей.

На мой мобильный телефон пришла смс от администрации социальной сети, где я зарегистрирован. Они просят меня в рамках проверки достоверности аккаунта выслать свой пароль. Должен ли я отправлять им свои данные?

Нет. Скорее всего, это мошенники, которые хотят получить доступ к твоему аккаунту. Тебе необходмио уведомить техподдержку социальной сети о случае фишинга.

Где я могу скачать игру бесплатно и без вирусов?

Есть несколько вариантов. Можно использовать игры, которые раздаются бесплатно, и скачивать их лучше с официального сайта игры, сайта разработчика или его официального партнера. Во всех остальных случаях никаких гарантий безопасности нет.

Зачастую в сети размещают программы, в том числе игры, в которые включают вредоносный код, чтобы затем взломать устройство пользователя.

Мой аккаунт взломали в социальной сети. Что мне делать?

Отправь администраторам ресурса письмо, где сообщи о том, что твой аккаунт взломали и попроси заблокировать его. Также необходимо предупредить всех друзей, которые у тебя добавлены в сети, о том, что тебя взломали и от твоего имени могут приходить сообщения. Проверь компьютер на наличие вирусов. Полезной мерой также может стать смена паролей на других сервисах и сайтах, так как злоумышленники, получив один пароль, могут получить доступ к твоим аккаунтам на других сайтах.

Какой контент является в интернете незаконным и как я могу помочь в борьбе с ним?

Порнография с участием детей (детская порнография), пропаганда наркотиков и детских суицидов подпадают под действие закона № 139-ФЗ, смысл которого в том, что государство блокирует в интернете подобный контент через систему «черных списков» сайтов, который ведет Роскомнадзор. Если ты нашел подобный материал, то ты можешь сообщить об этом .

В адресной строке браузера появляется значок ключа. Что он означает?

Это означает, что браузер установил безопасное соединение с просматриваемым веб-сайтом. Это происходит, когда ты набираешь конфиденциальную информацию типа логин и пароль.

Как я могу узнать, что обо мне думают другие люди в интернете?

Введи полное ФИО, или адрес электронной почты или имя пользователя в поисковой системе, и посмотри, какая информация выдается.

В игре у меня не сложились отношения с человеком и он меня преследует. Что мне делать?

Заблокируй его в списках своих друзей, подобная функция есть во многих онлайн играх. Если это приложение в социальной сети, то блокировка недругов осуществляется через блокировку профиля. Также можно пожаловаться администраторам игры на этого человеке, но необходимо будет предъявить доказательства.

Я познакомился с человеком в сети и он предлагает мне секс..."

Скорее всего, это педофил. Эта ситуация опасна, поэтому сообщи об этом своим родителям и обратись с ними в полицию.

Мой компьютер повис, когда я зашел на какой-то сайт. Что мне делать?"

Используй комбинацию клавиш control-alt-delete или control+shift+esc, закрой браузер, где был открыт этот сайт.

Что такое файлы Cookie и нужно ли их удалять?

Файлы Cookie - это маленькие текстовые файлы, которые содержат логин и пароль пользователя для доступа к каком-то сайту. Таким образом, человек, который возвращается на этот сайт, входит без авторизации. Большинство файлов Cookie создается сайтами, которые посещает пользователь, и эти файлы предназначены для работы самого сайта.

Однако некоторые файлы Cookie создаются на компьютере без твоего ведома, с целью изучить как и что ты делал на каком-то ресурсе. Также они могут быть использованы и во вред, поэтому ты можешь их удалять. Также это сделает сам браузер, когда ты из него выйдешь.

СОЦИАЛЬНЫЕ СЕТИ

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.

«Новый тренд» в Интернете, социальные сети, начались в 1995 году с американского портала Classmates.com («Одноклассники» являются его русским аналогом). Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление десятка похожих сервисов. Но официальным началом бума социальных сетей принято считать 2003—2004 годы, когда были запущены

LinkedIn, MySpace и Facebook. В Россию мода на социальные сети пришла двумя годами позже — в 2006-м, с появлением Одноклассников и ВКонтакте.

И если LinkedIn создавалась с целью установления деловых контактов, то владельцы MySpace и Facebook сделали ставку в первую очередь на удовлетворение человеческой потребности в самовыражении. Социальные сети стали своего рода Интернет-пристанищем, где каждый может найти базу для создания своего виртуального «Я». При этом каждый пользователь получил возможность не просто общаться и творить, но и делиться плодами своего творчества с многомиллионной аудиторией той или иной социальной сети.

Однако многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Информацию об участниках социальных сетей могут найти их работодатели, бывшие или настоящие жены или мужья, сборщики долгов, преступники, правоохранительные органы и так далее.

Известен случай проявления психологического расстройства на почве зависимости от общения в социальных сетях. В Белграде девушка Снежана Павлович попала в психиатрическую клинику после того, как её заметка в социальной сети Facebook не вызвала интереса среди её друзей. Врачи клиники назвали этот случай «синдром Снежаны», объясняя поведение пациентки как обычный стресс от неудовлетворенности социальной потребности индивидуума в современном мире.

КАКИЕ РИСКИ СУЩЕСТВУЮТ В СОЦИАЛЬНОЙ СЕТИ

- Самый главный риск – это потеря персональных данных и информации для доступа к аккаунту. Потеря контроля за профайлом (краткие сведения о пользователе: дата рождения, имя, ник, когда зарегистрирован, увлечения и прочая информация) может привести к различным последствиям, таким как рассылка спама и зараженных файлов от твоего имени или опубликование твоей переписки с друзьями;
- Информация, которая появляется в интернете в отношении тебя, может очень повлиять на тебя сейчас и в будущем. Например, ты можешь показывать, что ты лентяй или можешь быть очень вульгарным в общении в социальной сети, что характеризует тебя с плохой стороны. Именно такой вывод сделает менеджер по персоналу, который будет принимать решение о приеме тебя на работу.
- Ты можешь заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии твоей семьи, сообщая куда ты с семьей поедешь на каникулы, ты можешь заинтересовать воров;
- Ты можешь спровоцировать травлю себя со стороны пользователей сети;
- Также через социальные сети возможно заражение твоего компьютера.

Стоит отдельно рассказать про взлом профайла, и о том, как злоумышленники получают доступ к аккаунту. Вот некоторые самые популярные методы получения пароля:

- Метод обмана – очень распространенный метод доступа к личным данным. Сюда входят предложения:

- Программные методы. Этот метод взлома доступен знающим людям и состоит в поиске ошибок в коде сайтов, позволяющих получить доступ к базе данных с паролями. В таком случае данные могут восстановить только администраторы;
- Получить доступ к твоему профайлу можно через отсылку письма с просьбой перейти по ссылке и там ввести свои данные, или просто выслать свои данные для перерегистрации, представляясь сотрудниками портала. Вариантов много, а цель одна – через письмо человек вводит свой пароль, а злоумышленники его получают. В этом случае ты практически безвозвратно теряешь свою почту и все свои аккаунты, зарегистрированные на нее;
- В интернет-кафе, а также у друзей, которые хотели бы получить твой пароль. Киберпреступники могут использовать программы, называемые KeyLogger-ами – это клавиатурные шпионы, перехватывающие нажатия на клавиатуру и записывающие их в файл, таким образом, злоумышленник сможет получить твой пароль. Такая программа может быть установлена на любом общественном компьютере, в том числе в интернет-кафе;
- Путем прямого контакта с жертвой и выяснения, что может быть паролем. Метод очень опасен для тебя, если применяется опытным человеком. Не надо никому сообщать свои личные данные, даже если этот человек будет представляться сотрудником техподдержки или администрации;
- посредством перебора пароля по словарю или ручного подбора самых часто используемых простых паролей;
- скачать всевозможные программы, на самом деле являющиеся опасными вирусами, которые не всегда сразу определяются антивирусами
- загрузить фото вместо граффити, установить новые смайлики
- отправить cookies, логин и пароль в адрес неких людей, которые представляются сотрудниками техподдержки или администрации.
- Взлом твоего компьютера, где киберпреступники находят пароли. Это очень сложный способ и очень часто антивирусные программы замечают подобную деятельность. Обычно используются троянские программы.

ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Используй настройки конфиденциальности аккаунта. Настрой просмотр содержимого твоей учетной записи "только для друзей”. Таким образом, незнакомые люди не увидят твою личную информацию;

- Принимай запросы в друзья только от тех людей, которых ты знаешь и которым доверяешь;
- Не используй веб-камеру для общения с людьми, которых ты не знаешь;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Будь осторожен - некоторые пользователи могут представляться кем угодно;
- Если ты действительно хочешь встретиться с человеком, с которым познакомился в интернете, то договорись о встрече в общественном месте и желательно взять с собой кого-то еще, например, друга. Если твой сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу;
- Не размещай фотографии и видео со своими друзьями без их разрешения. Обращайся к друзьям, чтобы они также соблюдали конфиденциальность и не размещали твои фотографии и видео в общем доступе;
- Никогда не открывай подозрительные ссылки, даже если они пришли от твоих друзей. Удостоверься в том, что друг тебе выслал эту ссылку сам, а его аккаунт не контролирует киберпреступник. После взлома аккаунта злоумышленники в первую очередь делают рассылку по адресной книге, а поскольку доверие друзей друг другу выше, то вероятность заражения вирусами резко вырастает;
- Чтобы попасть в свою социальную сеть или на какой-либо другой сайт лучше используй закладки или окно быстрого доступа. Таким образом, ты точно попадешь на те порталы, которые безопасны и которыми ты пользуешься. При наборе адреса есть риск того, что ты ошибешься с адресом и не заметишь этого.

Фото digitaltrends.com

КИБЕРБУЛЛИНГ ИЛИ ВИРТУАЛЬНОЕ ИЗДЕВАТЕЛЬСТВО

Первый случай кибербуллинга был зафиксирован в 2002 году. Американский подросток Жислен Раза ради развлечения снял видеоролик, в котором он, подобно герою фильма «Звездные войны», фехтовал бейсбольной битой вместо лазерного меча. Одноклассники разместили в сети это видео с целью позабавиться над Жисленом. Эту запись посмотрели миллионы людей, через несколько дней был создан специальный сайт с исходным видео и пародиями на него. Насмешки сломали психику Жислена Раза и его родители были вынуждены обратиться к психиатру. Против одноклассников, разместивших исходное видео в интернете, был подан судебный иск.

Спектр целей кибер-преследователей широк, но всех объединяет стремление нанести жертве психологический ущерб. Это могут быть шутки, которые просто уязвят жертву, а может быть психологический террор, который приведет к суициду.

ЕСТЬ ВОСЕМЬ ОСНОВНЫХ ВИДОВ КИБЕРБУЛЛИНГА:

- Флейм (от английского «flame») или виртуальная перепалка.
- Обмен эмоциональными репликами в открытом доступе. Вначале все воспринимается как активное обсуждение, но оно может зайти дальше и нанести человеку психологический вред.
- Атаки
- Буллинг по сотовой связи сводится к отправке жертве повторяющихся оскорбительных сообщений или звонков.
- На форумах и в чатах преследователи понижают авторитет жертвы, если такая форма ранга предусмотрена на форуме.
- Оказывают давление в обсуждениях, реагируют на сообщения жертвы унижающими и оскорбительными сообщениями и совместным обсуждением реальных и мнимых недостатков жертвы. Обычно этим занимается целая группа преследователей.
- В online играх преследователи играют не ради победы, а с целью понизить игровой опыт жертвы целенаправленным давлением.
- Клевета. Распространение оскорбительной и неправдивой информации в виде фото, сообщений, песен. Нередко это может быть не отдельная жертва, а целая группа подростков, которые попадают под критику и шутки одноклассников.
- Самозванство. Преследователь представляется жертвой или, используя доступ к ее аккаунту, или создавая фейк (фальшивый аккаунт). От имени жертвы распространяет в блогах, социальных сетях и системах мгновенных сообщений негативную информацию, провоцируя окружающих на конфликт с жертвой.
- Распространение закрытой информации. Получив конфиденциальную информацию о жертве, преследователь передает ее тому, кому она не предназначалась, вызывая конфликт.
- Изоляция. Любому человеку присуще желание быть частью общества (класса, группы подростков во дворе, в сообществе в социальной сети). Ощущение себя частью сообщества является необходимой потребностью каждого человека, как физиологические потребности в пище, воздухе и потребность в самореализации. Изоляция человека от общества наносит серьезную травму человеку. Формы изоляции в киберпространстве могут быть разными, начиная от создания закрытого сообщества до игнорирования сообщений жертвы.
- Киберпреследование. Скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.
- Хеппислепинг («Happy Slapping» с английского «счастливое похлопывание»). Заключается в избиении жертвы и с записью этого на видео, с последующим выкладыванием ролика в сети. Подобные ситуации не редкость в новостях по телевизору.

ВОТ НЕСКОЛЬКО СОВЕТОВ, КОТОРЫЕ ПОЗВОЛЯТ ТЕБЕ ПОЛУЧИТЬ ИММУНИТЕТ НА КИБЕРБУЛЛИНГ:

Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт. Кроме того, преследователь только и ждет, когда ты выйдешь из равновесия.

- Управляй своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом. Так что в случае нанесения реального вреда, найти злоумышленника можно.
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.
- Соблюдай свой виртуальную честь смолоду.
- Храни подтверждения фактов нападений. Если тебя расстроило сообщение, картинка, видео и т.д. обратись за помощью и советом к родителям. Сохрани или распечатай страницу.
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии. Лучший защита от нападения – игнор.
- Если ты свидетель кибер-буллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- Не стоит игнорировать агрессивные сообщения, если они содержат угрозы, особенн систематические. Следует скопировать эти сообщения и обратиться в правоохранительные органы. По поводу размещения оскорбительной информации, размещенной на сайте, следует обратиться к администратору с требованием ее удаления.

БЕЗОПАСНОСТЬ В ПУБЛИЧНЫХ WI FI СЕТЯХ

Сейчас, когда у многих появились смартфоны, а значительная часть населения страны уже зарегистрировалась в социальных сетях, у людей есть потребность в доступе к интернету, а желательно - в бесплатном и без проблем, типа проводов и зоны покрытия.

Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Как ты уже понял, что Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Любое оборудование, соответствующее стандарту IEEE 802.11,

может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными. Какие угрозы несут в себе Wi-Fi сети?

- Перехват данных - это одна из самых популярных угроз. База или хот-споты Wi-Fi подобны радиоприемнику, который принимает сигнал с данными. Это означает, что с помощью другого приемного устройства и специальных программ-сканеров можно также принимать и расшифровывать информацию. Именно этим и занимаются злоумышленники;
- Wi-Fi ловушки. Ты нашел сеть без пароля и подключился через нее к интернету. В это время владелец точки осуществляет с помощью специальных программ запись всего трафика;
- Существуют специальные программы, с помощью которых злоумышленники могут получить доступ к твоему аккаунту в социальной сети;
- Подмена точек раздач с помощью другого имени точки, где установлены программы по контролю за твоим устройством;
- Взлом сети. Злоумышленники могут найти ошибки в работе алгоритма и расшифровать данные.

КАКИЕ ЕСТЬ СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI?

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера. Чтобы сделать что-то важное, нужно воспользоваться более защищенными источниками сети;
- Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.