Рекомендации
для родителей (законных представителей)
по обеспечению интернет-безопасности несовершеннолетних

1. Введение

Интернет – это безграничный мир информации, где ребенок может найти много интересного для учебы и саморазвития. В Интернете можно общаться со знакомыми и даже заводить друзей.

Но кроме хорошего, в виртуальном мире есть и плохое. Неправильное или неосторожное поведение в Интернете может принести вред не только ребенку, но и родным и близким.

Чтобы обезопасить ребенка в Интернете, достаточно соблюдать некоторые правила. В этих правилах нет ничего трудного, отнеситесь к ним внимательно и расскажите о них своим детям.

Ниже будут даны рекомендации по поведению в сети Интернет для следующих случаев:

- вирусы (черви, трояны) и другие вредоносные программы;
- виртуальные мошенники (воры) и другие преступники в сети Интернет;
- грубияны и хулиганы (тролли, провокаторы);
- бесконтрольное распространение персональных данных;
- контент, представляющий угрозу для несовершеннолетних.

2. Опасности, которые подстерегают несовершеннолетних в сети Интернет и рекомендации по безопасному поведению

2.1. Вирусы (черви, трояны) и другие вредоносные программы

Ребенок заходит в Интернет через компьютер, телефон или планшет. Это может быть школьный или библиотечный компьютер; личный компьютер, телефон или планшет; компьютер или планшет, которым пользуется вся семья.

Любому из вышеперечисленных устройств могут нанести вред вирусы, их еще иногда называют вредоносными программами. Они могут уничтожить важную информацию, зашифровать её и потребовать выкуп, украсть ваши файлы, персональные данные и данные платежных карт (а значит и средства с этих карт) через Интернет.

Рекомендации:

1. Проследите чтобы для защиты компьютера на нём были установлены специальные защитные программы и фильтры. Как правило, операционная система подсказывает о необходимости настроек параметров безопасности – предлагает включить встроенный фильтр (брандмауэр) и установить антивирусное программное обеспечение. Проинструктируйте ребенка о том, чтобы он ничего не менял в настройках антивирусных программ и брандмауэра после их установки и настройки.
2. Следите за регулярным обновлением баз антивирусных программ.

3. Регулярно обновляйте операционную систему на компьютере, планшете, телефоне.

4. Используйте встроенные защитные механизмы интернет-браузеров (программ для просмотра интернет-сайтов). Современные отечественные интернет-бразуеры как правило оснащены такими механизмами.

5. Не забывайте об использовании антивирусных программ и браузеров с защитными механизмами и на планшетах и мобильных телефонах.

6. Систематически проверяйте свои домашние компьютеры и персональные устройства на наличие вирусов.

7. Если антивирусная защита компьютера или защитные механизмы браузера не рекомендуют, не заходите на сайт, который считается подозрительным.

8. Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.

9. Используйте только проверенные сайты.

10. Не сохраняйте подозрительные файлы из Интернета, и тем более, не открывайте их.

11. Никому не сообщайте свой логин с паролем (от почты, аккаунта в социальной сети и т.д.) и не выкладывайте их в Интернете, относитесь к ним так же бережно, как к ключам от квартиры.

12. Делайте резервную копию важных данных на другие устройства или носители данных.

13. Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

2.2. Виртуальные мошенники (воры) и другие преступники в сети Интернет

Все мы знаем, что вне дома и школы есть вероятность столкновения ребенка с людьми, которые могут причинить им вред или ограбить. В Интернете также есть злоумышленники – надо помнить об этом и научить ребенка вести себя так же осторожно, как и на улице или в незнакомых местах.

Способов мошенничества в Сети – множество, и постоянно появляются все новые и новые. Начиная от обмана при личном общении на форуме и в чате, заканчивая фишингом, спамом, взлом аккаунтов социальных сетей и т.д.

Рекомендации:

1. Нельзя сообщать свой адрес или телефон незнакомым людям в Интернете и нельзя публиковать эту информацию.

2. Нельзя выкладывать в Интернет свои фотографии или высылать их кому-то без разрешения родителей. Надо помнить, что преступники могут использовать эту информацию против ребенка или его родных.

3. Прежде чем участвовать в каком-то конкурсе, где надо указывать свои данные ребенок должен посоветоваться с родителями.

4. Ребенок никогда не должен соглашаться прийти в гости к человеку, с которым он познакомился в Интернете. Если назначается встреча, она должна

проходить в людном месте и желательно с присутствием родителей. Надо помнить, что под маской ровесника в Интернете может скрываться взрослый человек с преступными намерениями.

5. Используйте сложные пароли для аккаунтов в социальных сетях. Не используйте пароли, в которых упоминается информация, которая может быть известна другим людям – ваше имя или имена членов вашей семьи, дни рождения и т.д. Злоумышленники могут попробовать взломать ваш аккаунт в социальной сети простым подбором пароля по известным о вас данным, подбором пароля по словарю. Поэтому придумывайте уникальные пароли, либо используйте специальные генераторы сложных паролей, или двухфакторную аутентификацию там, где она возможна (это когда кроме одного фактора – логина и пароля для проверки личности пользователя при входе используется и второй, дополнительный фактор, например, высылается проверочный код через SMS, то есть кража логина и пароля не даст злоумышленнику возможности пройти проверку, не имея доступа к SMS-сообщениям в вашем телефоне).

6. Если знакомый в социальной сети вдруг попросил у вас перевести ему денег на карту или номер телефона, перезвоните ему и убедитесь в том, что это действительно он. Чаще всего такие сообщения являются свидетельством взлома аккаунта вашего знакомого в социальной сети.

7. Внимательно относитесь к письмам, которые вы получаете в электронной почте или ссылкам, которые вам предлагают открыть в чате или социальной сети. Даже если отправитель информации вам знаком, то это еще не означает, что ссылки ведут на надежные сайты.

8. Внимательно относитесь к письмам от почтовых сервисов, социальных сетей и других сайтов, где вы уже зарегистрированы, если в письме вас призывают пройти по ссылке на данный сайт и срочно совершить какие-то действия, особенно в тех случаях, когда вы не ожидаете каких-либо писем и уведомлений от данного интернет-ресурса. Чаще всего эти письмам является мошенничеством, которое называется «фишинг», когда по ссылке вас перенаправляют на фальшивый сайт, который выглядит как настоящий и после ввода логина и пароля ваш аккаунт на настоящем сайте (почтовом сервисе, социальной сети) будет тут же взломан. Вместо перехода по ссылке из письма вы всегда можете войти в почтовое приложение или социальную сеть через официальное приложение на телефоне или планшете, войти на требуемый сайт по прямой ссылке или закладке, сохраненной в браузере.

9. Не открывайте подозрительные вложения, присланные по электронной почте и через интернет-мессенджеры.

Взлом вашего аккаунта (учетной записи) в социальной сети может привести к краже персональных данных, ведению личной переписки от лица хозяина аккаунта, вымоганию денежных средств и шантажу. Если ваш аккаунт взломали, необходимо:

1. Получить доступ к аккаунту (при необходимости восстановить пароль).
2. Изменить пароль
3. В настройках безопасности аккаунта завершить все текущие сеансы на данном аккаунте

4. Проверить, какие изменения были сделаны не вами и при необходимости исправить их: удалить сообщения, добавленных друзей, отменить заявки на добавления в друзья, членство в группах, комментарии, фото на стене, публикации, изменения в личной информации и настройках безопасности.

5. Если злоумышленником были проведены банковские операции, заблокировать карту и сообщить в банк о недействительности операции.

6. В случае отсутствия доступа к телефону, к которому привязан аккаунт (кража или потеря), обратиться к оператору мобильной связи для блокировки старой сим-карты и получения новой.

2.3. Грубияны и хулиганы (тролли, провокаторы)

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть ребенка, прислать неприятную картинку или устроить травлю. Ребенок может столкнуться с такими людьми на самых разных сайтах, в социальных сетях, форумах и чатах.

Рекомендации:

1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.

2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.

3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни.

4. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов – читать такие высказывания так же неприятно, как и слышать.

5. Не надо реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда надо пытаться уладить конфликты с пользователями мирным путем, попробовать перевести в шутку или прекратить общение с агрессивным пользователем. Ни в коем случае нельзя отвечать на агрессию тем же способом.

6. Если ребенку угрожают по Интернету, надо не стесняться и сообщать об этом родителям. Надо помнить, что цель угроз – испугать или обидеть. Но подобные люди, которые это делают, боятся ответственности.

7. Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и публикуют все известные данные, включая доступную личную переписку. Никогда не надо участвовать в травле и не общаться с людьми, которые обижают других.

8. Если решить проблему мирным путем не удается, надо написать жалобу администратору сайта, потребовать заблокировать обидчика.

9. Если администратор сайта отказывается помочь по каким-либо причинам, можно прекратить пользоваться таким ресурсом и удалить оттуда свои данные.

10. Не надо использовать Сеть для распространения сплетен, угроз или хулиганства.

11. Не надо встречаться в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

12. Ребенку всегда надо советоваться с родителями во всех указанных случаях.

2.4. Бесконтрольное распространение персональных данных

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

- кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;
- кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;
- с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;
- с помощью фотографий, запускаемых вами онлайн-трансляций и чекинов можно определить ваше местоположение в данный момент;

и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Чем больше сайтов мы посещаем, чем больше мы проходим регистраций на различных форумах, социальных сетях, чем больше мы пишем комментариев,

загружаем фотографий – тем больше мы оставляем цифровых следов в сети, в том числе и персональных данных.

Как уже было сказано выше – на надо публиковать в сети или сообщать кому-то свой адрес и телефон, а также логины и пароли. Перед выкладыванием фотографий в сеть Интернет – всегда советоваться с родителями.

Необходимо помнить, что любая информация, которую вы опубликовали в социальной сети (публикация текста и фотографий, комментарии к чужим публикациям, фотографии и информация в открытой части профиля, геотеги – отметки о вашем географическом нахождении в определенный момент времени) или на каком-то другом сайте – тут же становится доступной всем. Любой может скопировать эту информацию, сохранить ее на своем компьютере или устройстве, а также опубликовать снова на другом сайте в сети Интернет. Это же могут сделать в автоматическом режиме сайты – агрегаторы персональных данных.

Рекомендации:

1. Никогда не следует публиковать в Интернете ту информацию, которую вы в последствии захотите удалить из сети, вы можете столкнутся с тем, что информация может быть уже размножена в сети Интернет, а возможно выйдет и за её пределы, и вы не сможете её удалить.
2. Изучите настройки приватности социальных сетей, которые вы используете. Обратите внимание, что многие социальные сети позволяют ограничить доступ к вашим персональным данным для других пользователей, в настройках приватности, как правило, можно указать, кто и какую информацию может о вас видеть в сети.
3. Ограничивайте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию, которую вы не хотели бы делать доступной для незнакомых людей.
4. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
5. Не публикуйте в Сети фотографии ваших документов, билетов и платежных чеков.
6. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.
7. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.
8. Используйте только сложные пароли, разные для разных учетных записей и сервисов. Старайтесь периодически менять пароли. Помните, что если вы используете один и тот же пароль на различных сайтах, то в случае взлома любого из этих сайтов и утечки данных о паролях пользователей, злоумышленники смогут получить доступ и ко всем остальным сайтам, где вы использовали тот же самый пароль. К сожалению случаи взлома сайтов и утечки данных пользователей, в том

числе и паролей – отнюдь не редкость, от этого на 100% не застрахованы даже самые крупные интернет-ресурсы.

9. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

10. Не пользуйтесь открытыми точками доступа Wi-Fi и выключайте Wi-Fi на устройстве, если не собираетесь его использовать.

11. Следите за тем, какие приложения в телефоне и на планшете используют личные данные.

2.5. Контент, представляющий угрозу для несовершеннолетних

В связи с развитием новых технологий в области виртуального пространства, в том числе с распространением сети Интернет, возникла проблема, связанная с доступом несовершеннолетних к информации сомнительного содержания и противоречащей общепринятой этике. В настоящее время любой человек, в том числе и несовершеннолетний, владеющий знаниями в области компьютерных технологий, может получить доступ к данным, хранящимся в Интернете или самостоятельно начать что-то публиковать, например, в социальных сетях. Отсутствие контроля со стороны родителей за использованием детьми сети Интернет - одна из причин доступности негативной информации несовершеннолетним. Что необходимо делать чтобы оградить ваших детей от информации сомнительного содержания и противоречащей общепринятой этике?

Рекомендации

1. Родители должны знать интересы и цели детей, которые используют сеть Интернет.

2. Рекомендуется допускать использование сети Интернет детьми в присутствии взрослых. Доступ к данному информационному ресурсу должен быть эффективным и безопасным.

3. Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Российской Федерации, может оказать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, азартные игры, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение, суицидальное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.).

4. С целью ограничения доступа детей к «вредным» материалам можно использовать:

- специальные тарифы доступа к сети Интернет, имеющие дополнительную услугу фильтрации контента – как при предоставлении услуги домашнего интернета, так и через сотовую связь («Детский интернет» и т.д.);

– специальное программное обеспечение, устанавливаемое на компьютер (планшет, телефон), имеющие опции «Родительского контроля» для блокировки информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков;
– детские браузеры и детские поисковые системы.

5. Если ребенок самостоятельно работает в Интернете, то необходимо контролировать, какие сайты посещает ребенок и какие поисковые запросы делает. Это можно узнать в истории поиска и истории посещений сайтов браузера.

6. Используйте инструменты мониторинга активности ребенка в социальной сети Вконтакте. Вы можете отследить попадание ребенка в опасные группы в данной социальной сети с помощью такого бесплатного инструмента как «Гердабот» (https://gerdabot.ru/).

3. Как защитить ребёнка от онлайн-рисков?

1. Развивайте доверительные отношения.
2. Установите правила пользования Интернетом для всех электронных устройств.
3. Регулярно разговаривайте об Интернете.
4. Будьте в курсе событий ребенка в реальной жизни и виртуальном пространстве.
5. Расскажите о нормах онлайн-этикета.
6. Объясните необходимость защиты персональной информации.
7. Проинформируйте о том, где можно получить помощь.
8. Станьте для ребенка примером ответственного онлайн-пользователя.

4. Что делать, если ребенок все же столкнулся с какими-либо рисками?

1. Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать.

2. Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;

3. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где вы не рассказали ему о правилах безопасности в Интернете;

4. Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о

встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

5. Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может вам пригодиться (например, для обращения в правоохранительные органы);

6. Если вы не уверены в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете, как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС и др.)

7. Куда можно обратиться:
   – Краевой детский телефон доверия 8-800-2000-122 (круглосуточно, анонимно, бесплатно);
   – Школа: учитель – заместитель директора – директор;
   – Департамент образования (управление образования города/района) – Министерство образования;
   – Уполномоченный по правам ребенка в Пермском крае;
   – Прокуратура;
   – Отдел по делам несовершеннолетних;
   – Комиссия по делам несовершеннолетних.

5. Перечень использованных источников

1. Памятка «Безопасный Интернет – детям. Полезные советы для тебя и твоих друзей». Министерство внутренних дел Российской Федерации, Управление «К»
2. Сайт http://персональныеданные.дети (дата обращения: 25.12.2018 г.)
3. Материалы выступлений докладчиков на родительских собраниях по теме «Безопасный Интернет» 26 апреля 2018 г., 01 декабря 2018 г.

Будьте внимательны при работе в сети Интернет,
берегите себя, своих родных и близких и свои персональные данные!