ПОДРОСТКИ В СОЦИАЛЬНЫХ СЕТЯХ: БЕЗОПАСНОЕ ПОВЕДЕНИЕ

На данный момент в мире возникло устойчивое понимание того, что проблема безопасности детей в интернете — это проблема, требующая срочного вмешательства специалистов. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности — родителей и детей, а также профессиональной информационной культуры учителей.

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования.

Социальные сети как угроза безопасности жизнедеятельности подростка

Самый главный риск общения в социальных сетях – 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 подростка, может очень повлиять на него сейчас и в будущем. Например, подросток может показывать, что ты лентяй или может 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 на работу.

-Подросток может заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии своей семьи, сообщая куда он с семьей поедет на каникулы, ребенок может заинтересовать воров.

-Подросток может спровоцировать травлю себя со стороны пользователей сети.

-Также через социальные сети возможно заражение его 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 различие предложения, которые кажутся очень интересными.

-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 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 пользователь практически безвозвратно теряет свою почту и все свои аккаунты, зарегистрированные на нее.

-В интернет-кафе, а также у друзей, которые хотели бы получить чужой 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 любой 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 подростка, 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.

-Предложениями 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.

Правила безопасного поведения в социальных сетях

Тонны сокровенных подробностей, о которых сказать незнакомому человеку на улице даже в голову не придёт, выкладываются в социальные сети, где к этим деталям личной жизни потенциально имеют доступ миллионы незнакомых людей. «Чепуха! Очередная паранойя. Я могу себя чувствовать уютно и в безопасности в кругу своих друзей, т.к. безупречная настройка приватности меня защитит» - то о чём, скорее всего, Вы подумали сейчас.

Только проблема в том, что своей личной жизнью мы делимся не лично с человеком, а с его аккаунтом... Наивно полагать, что его аккаунт полностью защищён. Он может быть взломан. А возможно, ваш друг не сильно заботится о конфиденциальности своего общения в сети и у него все время активно подключение к социальным сетям или включено автозаполнение паролей, дабы экономить время, а вход в операционную систему без пароля. Чем и не преминул воспользоваться только что вышедший на волю жуткий троюродный брат по двоюродной тётке вашего друга, зашедший к нему в гости.

Многие люди любят оповещать о своём местонахождении в социальных сетях. Особенно, если в этом месте потрясающая архитектура или песок, солнце и океан. Тем, кто имеет доступ к вашей странице не нужно знать, где Вы находитесь в режиме 24/7.

Касательно вашего месторасположения нужно использовать только прошедшее время, а не настоящее и будущее.

Не размещайте в социальных сетях ту информацию, разглашение которой нежелательно для Вас, даже если Вы на сто процентов уверенны, что она будет доступна только определённым людям.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее

люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.
В мире цифровых технологий может быть непросто сформировать свой новый образ. Даже если ты не хочешь, чтобы о твоих старых приятелях стало известно, эта информация остается в Интернете, и любой сможет ее найти. Свидетельства неприличного поведения тоже будет невозможно скрыть.
То, что когда-то казалось подходящим для публикации, в один прекрасный день может всплыть на поверхности и причинить тебе различные неприятности.

Если ты хочешь узнать, что о тебе можно узнать, то набери свое имя и фамилию в поисковую систему и посмотри, какая информация выдается. Если что-то тебе не понравится, то постарайся удалить это.

Но у всего есть и хорошая сторона. Если ты формируешь свой положительный образ, то ты делаешь все правильно. Например, это может быть размещение информации об участии в каком-то конкурсе, ссылка на твою статью в школьной газете или просто грамота. Также это позволяет продемонстрировать сферу твоих достижений, что пригодится в будущем при обучении и продвижении по карьерной лестнице, а также позволит установить связи с людьми, имеющими схожие интересы. Важно, что это должно быть правдой.
Около 85% сотрудников отделов кадров говорят, что учитывают цифровую репутацию, решая, принять ли человека на работу. Поэтому твоя цифровая репутация очень важна, а думать над этим лучше уже сейчас.

Одна из опасностей социальных сетей-секстинг. Это пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.
Обычно наши ровесники используют камеры, встроенные в мобильные телефоны, чтобы сфотографировать себя в обнаженном или полуобнаженном виде и отправить эти картинки своим друзьям, подругам или одноклассникам. Некоторые отправляют эти фотографии только одному человеку, а уже тот в свою очередь пересылает их другим людям.

Секстинг выглядит как забава или какая-то игра до тех пор, пока кто-нибудь не пострадает, а скорее всего, пострадаешь именно ты. Проблема секстинга заключается в том, что конфиденциальные фотки могут быстро стать достоянием общественности. Смелая фотка, отправленная сегодня твоему другу или подруге, завтра может начать бесконтрольно распространяться, в результате чего автор станет посмешищем в школе, на него выльется много грязи и сплетен. Когда фотография становится доступной в Интернете, то практически невозможно удалить все ее копии.

В некоторых странах, в частности в Российской Федерации, секстинг является уголовным преступлением, а если на интимных фотографиях изображен несовершеннолетний, то это считается детской порнографией. Причём виновными могут быть признаны оба: как человек, отправивший фотографии, так и получивший их — это классифицируется как производство и хранение детской порнографии соответственно. Кроме того, лицу, пославшему свои фотографии в обнажённом виде, могут быть предъявлены обвинения в сексуальном домогательстве.

Памятка по технике 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.

ПАМЯТКА ДЛЯ ДЕТЕЙ И ПОДРОСТКОВ

«ПРАВИЛА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В ИНТЕРНЕТЕ»

1. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.

2. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д) считается плагиатом (умышленное присвоение авторства чужого произведения).

3. Не верьте всему, что в видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.

4. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, номер школы, любимые места для игр и т.д.).

5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чем-то, что требует указания идентификационного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит никакой личной информации.

6. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично.

7. Нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.

8. Научитесь доверять интуиции. Если что-нибудь в интернете будет вызывать у вас психологический дискомфорт, поделитесь своими впечатлениями с взрослыми.

Основные правила для школьников младших классов

Вы должны это знать

1. Всегда спрашивайте родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в интернете, спросите у родителей как безопасно общаться.

3. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.

4. Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели ваши личные фотографии.

5. Не встречайтесь без родителей с людьми из интернета вживую. В интернете многие люди рассказывают о себе неправду.

6. Общаясь в интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.

7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

Основные правила для школьников средних классов

Вы должны это знать

1. При регистрации на сайтах старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Также не рекомендуется размещать свою фотографию, давая тем самым представление о том, как вы выглядите посторонним людям.

2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан.

3. Нежелательные письма от незнакомых людей называются «спам». Если вы получили такое письмо, не отвечайте на него. В случае, если вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.

4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.

6. Если вас кто-то расстроил или обидел, расскажите все взрослому.

Основные правила для школьников старших классов

Вы должны это знать

1. Нежелательно размещать персональную информацию в интернете.

2. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и личные фотографии.

3. Если вы публикуете фото или видео в интернете — каждый может посмотреть их.

4. Не отвечайте на спам (нежелательную электронную почту).

5. Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

6. Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)

7. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

https://youtu.be/TSQN-dMehFA

https://youtu.be/zD1PrSu2_iQ