Управление образования
администрации Новооскольского городского округа

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по информационной безопасности для родителей

НОВЫЙ ОСКОЛ, 2024 г.

ОБЩИЕ РЕКОМЕНДАЦИИ

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

Храните имена пользователей и пароли в безопасности

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. Убедитесь, что дети знают, что эту информацию нельзя передавать никому, даже друзьям. Возможно, никто не хочет причинить ребенку никакого вреда, но даже в розыгрышах из лучших побуждений что-то может пойти не так и доставить неприятности. Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.

Периодически меняйте пароли

Наряду с напоминанием детям о том, что никому нельзя сообщать свои пароли, также рекомендуется периодически менять пароли. Утечки данных происходят постоянно, а утечка паролей подвергает риску кражи личных данных и другим проблемам с кибербезопасностью. Настройте расписание смены паролей учетных записей каждые 3-6 месяцев или каждый раз, когда платформа сообщает о взломах или утечках данных. Вы можете использовать менеджер паролей, чтобы отслеживать все свои пароли в интернете и упростить их поиск вашим детям.

Не разглашайте личную информацию в интернете

Дети и подростки не должны сообщать никому в интернете свое полное настоящее имя, адрес, район проживания, номер телефона и прочие данные. Общее правило: никогда не сообщать информацию, которая могла бы помочь интернет-хищникам найти их. Даже небольших деталей, таких как название школы или спортивной команды, достаточно, чтобы раскрыть личность. Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.

Будьте внимательны в социальных сетях

Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии и видео, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. Напомните детям, что все опубликованное в интернете сразу становится общедоступным, и любой может увидеть это. Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

Проверяйте возрастные ограничения

Многие приложения и веб-сайты имеют собственные возрастные ограничения для создания учетных записей, просмотра и регистрации. Но проблема в том, что на большинстве таких сайтов фактически нет функции проверки возраста. Например, Facebook, Snapchat и Myspace разрешают доступ только с 13 лет, но дети могут указать другой возраст и зарегистрироваться в любом случае.

Объясните опасность передачи геоданных

Почти все современные приложения и веб-сайты имеют функции отметки геопозиции или передачи данных о местоположении. Дети и подростки должны знать, чем опасно сообщать о своем местоположении, и что не следует неосознанно соглашаться с таким условием во всплывающих окнах приложений. Публичная демонстрация данных о местоположении подвергает детей различным опасностям: от сетевых интернет-хищников, которые могут найти их, до риска кражи личных данных. Убедитесь, что дети понимают, что означает, когда в приложении спрашивается, можно ли передавать данные о местоположении.

Создайте список правил использования интернета

Один из лучших способов управлять использованием интернета детьми всех возрастов – это сесть и совместно составить список правил использования интернета в соответствии с их потребностями. Вы можете показать ребенку сайты для детей и подростков, поговорить о том, почему важно установить правила, и попросить их поделиться, если он чувствуют себя некомфортно или ему угрожает что-то, найденное в интернете, и т. д. Установите границы, но будьте реалистом.

Используйте одинаковые правила при общении онлайн и лично

Научите детей тому, что к онлайн и к личному общению применимы одни и те же правила. При общении в интернете и написании комментариев лучше оставаться добрым и вежливым, не следует писать ничего такого, что не смогли бы сказать в лицо. Это также применимо и при анонимной публикации сообщений. Публикация обидных и грубых вещей – это не только некрасиво и нелицеприятно по отношению к другим, но также может навредить репутации вашего ребенка.

Установите родительский контроль

Настройте и пересмотрите параметры родительского контроля на всех своих устройствах в соответствии с возрастом ваших детей. Это поможет защитить детей от доступа к неприемлемому контенту в интернете. Параметры контроля можно настроить несколькими способами, например, обеспечить доступ детей только к соответствующему их возрасту контенту, установить время использования устройства, контролировать активность и запретить передачу личной информации. В дополнение к родительскому контролю можно также использовать инструменты фильтрации и мониторинга. Периодически проверяйте и обновляйте эти программы.

Используйте антивирусные программы

Помимо родительского контроля, используйте на всех устройствах антивирусные программы. Они защищают подключенные к интернету устройства от входящих угроз, а также выявляют, уничтожают и предупреждают о возможных угрозах для системы. Антивирусные программы не отстают от современных угроз и помогают обнаруживать новые постоянно появляющиеся вирусы.

Расскажите о существовании фальшивых рекламных объявлений

Обсудите с детьми рекламные программы и мошенничество, связанное с фальшивыми рекламными объявлениями, с которыми они могут столкнуться в интернете. Некоторые объявления выглядят как реальные предложения, побуждающие загрузить фальшивое приложение, зарегистрироваться для участия в розыгрыше или предоставить личную информацию в обмен на бесплатные продукты. Они также могут быть представлены в виде ссылок, которыми можно поделиться с друзьями или опубликовать в социальных сетях. Если дети знают о существовании таких видов рекламы и мошенничества, они с меньшей вероятностью попадутся на них, столкнувшись в Интернете.

Объясните детям об опасности личных встреч с незнакомцами

Дети никогда не должны лично встречаться с незнакомцами, с которыми они общались в интернете, если за такой встречей не наблюдает родитель. Объясните детям и подросткам, что не следует общаться с незнакомцами лично. Интернет-хищники или участники кибербуллинга (травли) могут скрываться, чтобы ребенок не понял, что общается с кем-то из интернета.

Мониторинг истории поиска в интернете

Родителям детей любого возраста рекомендуется периодически проверять историю браузера, чтобы понять, какие сайты посещают их дети. Убедитесь, что в настройках браузера включено отслеживание истории, и проверяйте ее на всех устройствах с доступом в интернет. Если вы столкнетесь с подозрительными сайтами, спросите о них у ребенка. Продемонстрируйте детям максимальную открытость при отслеживании их действий в интернете, чтобы они не ощущали, что за ними шпионят.

Как защитить несовершеннолетних от вовлечения в деструктивные сообщества в сети Интернет

В Интернете действует большое количество преступников, чьей целью является вовлечение все новых и новых пользователей в деятельность таких опасных сообществ. Такие лица называются «вербовщиками». Чаще всего вербовка начинается с личного и очень навязчивого общения. Вербовщики пытаются завладеть всем вниманием и временем пользователя. Один из основных способов вербовки – маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами. После этого происходит

отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообществ. Особенностями таких групп может быть персональный доступ к ним только членам сообщества (особенно если общение происходит через мессенджеры). То есть родители или иное лицо не сможет попасть в группу, используя свои телефон или компьютер. После этого пользователи приступают к выполнению заданий в реальном мире.

К опасным сообществам в социальных сетях относятся:

1. Группы, пропагандирующие экстремистскую и нацистскую идеологию: террористические группировки, (в том числе движение «Колумбайн», признанное террористическим движением на основании решения Верховного суда РФ), шутеры, нацистские, неонацистские движения и др.

2. Группы и каналы, пропагандирующие опасные увлечения: зацепинг, опасные квесты, группы с пропагандой наркотиков, трэш-стримеры, шок-контент и др.

3. Группы, пропагандирующие причинение вреда себе или окружающим: селфхарм (буквально переводится как «вред себе»), пиплхейт (движение, пропагандирующее ненависть к людям), депрессивно-суицидальные группы («синий кит» и аналогичные), анорексию и др.

4. Группы, пропагандирующие нетрадиционные духовно-нравственные ценности: оккультизм, сатанизм, чайлдфри, феминизм, нетрадиционные сексуальные отношения, смену пола, гендерную идентичность и пр.

5. Аниме-сообщества. В отличие от традиционной японской культуры аниме, современные аниме могут быть очень опасны, поскольку нередко пропагандируют насилие, сексуальные извращения, каннибализм, убийства и самоубийства. По данным исследователей через «кровавое аниме» популяризуется даже скулшутинг. Аниме-продукция также является лидером по депрессивно-суицидальному контенту.

По данным опроса экспертов из числа сотрудников подразделений по делам несовершеннолетних органов внутренних дел, многие несовершеннолетние, имевшие опыт суицидального поведения, увлекались данной субкультурой.

Как гарантировать безопасность ребёнка в опасной среде?

Ребенок должен знать об опасностях общения с незнакомцами в интернете, а также доверять своим родителям.

Важно, чтобы в случае опасности, появления странных друзей или попытки втянуть ребенка в сомнительную деятельность, он, в первую очередь, обращался за помощью к родителям.

Спрашивайте или аккуратно проверяйте, с кем ведёт переписку ребёнок в личных сообщениях.

Обращайте внимание на поведение и новые интересы ребёнка: аниме, депрессивная литература, специализированные книги об оружии и стрельбе.

Замечайте изменения круга общения ребёнка, спрашивайте о его новых друзьях.

Обращайте внимание, если ребенок в реальной жизни выполняет задания, полученные в Интернете, так называемые, челленджи. Они могут содержать опасные для здоровья действия, например: сделать фото в экстремальных условиях или пробраться на закрытую территорию.

Возрастные рекомендации

В дополнение к общим, существуют также возрастные рекомендации, которые следует учитывать при использовании интернета детьми.

2 – 4 года

Не допускайте самостоятельного времяпрепровождения в интернете.

Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.

Не позволяйте детям переходить по ссылкам.

Ограничьте время, проводимое за компьютером.

Прививайте базовые навыки работы с компьютером с помощью соответствующих возрасту игр и образовательных программ.

5 – 7 лет

Не допускайте самостоятельного времяпрепровождения в интернете или с телефоном.

Не допускайте никаких пугающих изображений, ни реальных, ни вымышленных.

Не позволяйте детям переходить по ссылкам.

Используйте удобные для детей поисковые системы с родительским контролем.

Настройте фильтры по возрасту.

Ограничьте время, проводимое в интернете.

Ограничьте детей списком любимых сайтов, который вы составите вместе.

Убедитесь, что подключенные к интернету устройства находятся в открытом доступе, где вы можете их наблюдать.

Заблокируйте использование средств обмена мгновенными сообщениями, электронной почты, чатов, мобильного интернета, обмена текстовыми, графическими и видео сообщениями, а также доступ к доскам сообщений.

Научите детей никогда не разглашать личную информацию в интернете.

8 – 10 лет

Обсудите с детьми, что им интересно в интернете.

Расскажите детям об опасностях, скрывающихся в интернете.

Научите детей никогда не разглашать личную информацию.

Избегайте пугающих образов.

Объясните детям, как правильно общаться с друзьями в интернете.

Попросите детей рассказывать вам о случаях, когда они сталкиваются в интернете с чем-то, что вызывает у них чувство неловкости.

Проводите время в интернете совместно с детьми или ограничьте им доступ только набором одобренных сайтов.

Размещайте подключенные к интернету устройства в открытой общей зоне.

Установите родительский контроль, соответствующий возрасту ребенка.

Используйте инструменты фильтрации и мониторинга.

Используйте удобные для детей поисковые системы.

Запретите использование средств обмена мгновенными сообщениями, чатов и сайтов социальных сетей, предназначенных для более взрослой аудитории.

Попросите ребенка использовать тот же адрес электронной почты, который используете вы сами, или специальный адрес, к которому у вас есть доступ.

Просите детей открыто рассказывать о своих действиях в интернете.

11 – 13 лет

Не размещайте устройства, подключенные к интернету, в детских комнатах.

Установите родительский контроль, соответствующий возрасту ребенка.

Используйте инструменты фильтрации и мониторинга.

Контролируйте все устройства с доступом в интернет: сотовые телефоны, игровые устройства и тд.

Просите детей рассказывать об их действиях в сети и людях, с которыми они общаются.

Запретите детям разглашать личную информацию без вашего разрешения.

Объясните детям, что не следует организовывать личные встречи с людьми, с которыми они познакомились в Интернете.

Требуйте у детей доступ к их электронной почте и чатам.

Ограничьте общение посредством мгновенных сообщений списком друзей, который вы одобряете.

Заблокируйте доступ к чатам.

Научите детей общаться с незнакомцами в интернете.

Расскажите детям о неэтичном поведении в интернете, в том числе о буллинге (травле), распространении сплетен, угрозах, ненормативной лексике и прочих неприятностях.

Проверяйте историю браузера, чтобы отслеживать поведение детей в интернете.

Соблюдайте минимальный возраст для регистрации в социальных сетях.

Поощряйте посещение детьми соответствующих возрасту сайтов.

Не позволяйте детям публиковать фотографии или видео без вашего разрешения.

14 – 18 лет

Составьте список правил использования интернета для вашего дома.

Установите родительский контроль, соответствующий возрасту ребенка.

Используйте инструменты фильтрации и мониторинга.

Ознакомьтесь с приложениями для обмена сообщениями, которые используют ваш ребенок.

Контролируйте устройства с выходом в интернет, помимо компьютеров, такие как сотовые телефоны, игровые устройства и тд.

Храните устройства с доступом к интернету на виду, вне детских комнат.

Обсуждайте с подростками друзей, с которыми они познакомились в интернете, и говорите об их действиях в сети.

Поговорите с подростками о том, что не следует общаться с незнакомцами посредством мгновенных сообщений, и совместно составьте список друзей.

Убедите подростков спрашивать у вас одобрения, прежде чем заводить знакомства в сети.

Сопровождайте подростков на встречу с людьми, с которыми они познакомились в интернете, но еще не знают лично.

Научите подростков не разглашать личную информацию.

Расскажите подросткам о неэтичном поведении в интернете, в том числе о буллинге (травле), распространении сплетен, угрозах, ненормативной лексике и прочих неприятностях.

Защитите подростков от спама, объяснив им, что не следует раскрывать свой адрес электронной почты в интернете и отвечать на нежелательную почту.

Расскажите подросткам о законах об авторском праве и ответственном поведении в интернете.

Отслеживайте все финансовые операции, совершаемые подростками в интернете, в том числе заказ, покупку или продажу товаров.

Просите подростков рассказывать вам о неприемлемых материалах или нежелательных комментариях сексуального характера, которые они получили в интернете.

Расскажите подросткам, на что нужно обращать внимание или запрашивать перед загрузкой файлов из интернета.

Выборочно проверяйте историю браузера, чтобы узнать, какие сайты посещал подросток.

Обеспечение безопасности детей в интернете так же важно, как и в реальном мире. Существует множество причин, по которым дети хотят и должны использовать интернет: от выполнения школьных заданий до посещения виртуальных мероприятий, внеклассного обучения и интерактивных игр с друзьями. Интернет – это богатый ресурс и интересное место для общения, если дети и подростки знают, как использовать его безопасно и избегать потенциальных угроз.

Безопасность в интернете достигается постоянными разговорами с детьми о том, как и для чего используется интернет, и знанием, как обеспечить их защиту. Понимание того, почему дети выходят в интернет, с кем они там взаимодействуют и какие сайты посещают, очень важно для обеспечения их безопасности. Также крайне важно информировать их о рисках, связанных интернетом, о безопасном и вежливом общении в интернете и о действиях в случае, если они столкнулись с чем-то неуместным.