Безопасность в интернете

В наши дни мы все проводим много времени в интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг (травля), неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков.

Общие рекомендации

Детям и подросткам интернет необходим для выполнения школьных заданий, общения с учителями и другими учениками, интерактивных игр и выполнения других задач. Это прекрасное место для обучения и общения. Но родители должны быть в курсе того, что их дети видят и слышат в Интернете, с кем общаются и что рассказывают о себе. Ниже приведено несколько рекомендаций, которые помогут обеспечить безопасность детей в интернете.

Храните имена пользователей и пароли в безопасности

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. 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

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.

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.

Будьте внимательны в социальных сетях

Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. 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 вас, нужно внимательно относиться своим публикациям.

Используйте надежное решение для кибербезопасности

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.

Опасность передачи геоданных

Почти все современные приложения и веб-сайты имеют функции отметки геопозиции или передачи данных о местоположении. Вы 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.

Создайте список правил использования интернета

Один из лучших способов управлять использованием интернета детьми всех возрастов - это совместно составить список правил использования интернета в соответствии с потребностями. Дети и родители могут вместе выбрать сайты для детей и подростков, обсудить, если что-то, найденное в интернете тревожит или пугает. 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, а также публикации компрометирующих видеороликов - это не только некрасиво и нелицеприятно по отношению к другим, но также может повлечь разбирательство в суде в защиту чести и достоинства или от клеветы.

Не переходите по ссылкам фальшивых рекламных объявлений

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.

Опасность 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. Интернет-хищники или участники кибербуллинга (травли) могут скрываться, чтобы ребенок не понял, что общается с кем-то из интернета.

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 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.

- 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, iPod и КПК.

- 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 (например, 13 лет для Myspace и Facebook).

- Поощряйте посещение детьми соответствующих возрасту сайтов, таких как TweenLand. ClubPenguin и прочих.

- 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 использует ваш ребенок.

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

- 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.