Центр поддержки семьи «Детство в надежных руках»

Безопасный интернет для детей: правила поведения и родительский контроль

Что рассказать детям о кибербезопасности

Современные дети много времени проводят в интернете, поэтому важно научить их безопасному поведению в цифровом пространстве

Что угрожает детям в интернете

Взлом аккаунта

Если не защищать аккаунты, злоумышленники могут взломать их и использовать личную информацию. Например, шантажировать ребёнка фотографиями, фактами из переписки

или рассылать от его лица просьбы о помощи или спам. А кража игрового аккаунта может стать ударом для подростков, увлечённых киберспортом

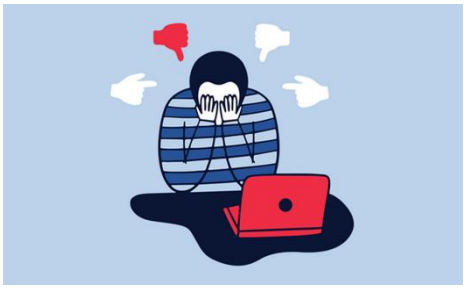
Сбор личной информации

Некоторые подростки делятся на своих страницах в соцсетях подробностями частной жизни, чтобы произвести впечатление на друзей. Опубликованные фото квартиры с дорогой техникой могут привлечь грабителей, а фото из отпуска подскажут им, когда никого не будет дома

Фишинг — использование поддельных ссылок.

Мошенники могут использовать доверчивость детей и вынудить их перейти по фишинговым ссылкам на сообщения с информацией о выигрыше, выгодном предложении и т. д. Злоумышленники создают поддельные сайты, чтобы похищать логины, пароли, платёжные данные. Также при переходе по фишинговой ссылке может загрузиться программа, которая заразит компьютер или гаджет вирусом

Кибербуллинг — травля в интернете



В цифровом пространстве дети могут подвергаться травле. Обидчик может быть анонимным, поэтому его сложно вычислить. Кроме того, виртуальные издевательства происходят в личной переписке и родители могут не узнать, что ребёнка преследуют. Последствия кибербуллинга для детей сравнимы с реальной травлей: негативные эмоции, депрессия, проблемы с учёбой.

Встречи с незнакомцами и груминг

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье.

Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, оскорбления, запугивания и домогательства. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети.

Контентные риски

К контентным рискам относятся материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Что делать родителям

Расскажите о правилах защиты аккаунтов

Прежде всего — это надёжный пароль. Он должен состоять не менее чем из 12 знаков, включать строчные и заглавные буквы, цифры и специальные символы. Легко запомнить фразу, связанную с жизненной ситуацией, и превратить её в надёжный пароль, например «Я_люблю_лето_2022!».

Для каждого аккаунта нужно использовать разные пароли, желательно менять их раз в полгода. Порекомендуйте ребёнку использовать

двухфакторную аутентификацию, например ввод пароля и код доступа на телефон. Злоумышленник, сумевший добыть чужой пароль, не сможет попасть в аккаунт без одноразового кода из смс.

Как создать надёжный пароль

Поговорите о важности настроек приватности

Вряд ли дети согласятся полностью закрыть свою страницу от всех, кроме друзей, однако можно ограничить возможности других пользователей. Например, запретить посторонним присылать сообщения, комментировать посты и фотографии. Также можно настроить видимость постов: слишком личные оставить видимыми для друзей или только некоторых из них

Объясните ребёнку, что он может блокировать пользователей, которые угрожают ему, оскорбляют или обижают.

Расскажите, что можно и что нельзя публиковать в соцсетях

Не следует постить фото дорогих вещей, техники в квартире, тем более с геометками. Такие фото лучше оставить для личной коллекции. Даже если они были отправлены в сообщениях, такие фото могут стать предметом шантажа

Кроме того, нельзя публиковать фото документов, билетов на концерт и другую конфиденциальную информацию. Всё это не стоит хранить даже в закрытых постах или альбомах, потому что в случае взлома аккаунта или самого сервиса данные окажутся в руках мошенников.

Научите распознавать фишинг

Главное правило — не переходить по ссылкам из сообщений, которые пришли от подозрительного отправителя. Типичные признаки фишинга — выгодное предложение, информация о выигрыше. Иногда мошенники имитируют рассылки от настоящих сервисов или интернет-магазинов. В этом случае их можно определить по некорректному адресу отправителя. Часто он вообще не соответствует подлинному, а иногда отличается от него одной или двумя буквами, например admin@notify.wk.com вместо admin@notify.vk.com

Попросите не пользоваться важными приложениями при подключении к бесплатному вайфаю.

Часто публичные сети плохо защищены. Иногда мошенники сами создают точки доступа, которые выдают за бесплатный вайфай кафе или парка. Благодаря этому злоумышленники перехватывают и могут подменить любую информацию, в том числе логины и пароли от аккаунтов и платёжную информацию.

Расскажите об опасностях интернета

Дети часто воспринимают виртуальную среду как более безопасную по сравнению с реальной. Но в интернете надо соблюдать те же правила, что и в реальной жизни: не общаться с незнакомыми людьми, не доверять им и рассказывать обо всём родителям. Не стоит посещать сомнительные ресурсы, скачивать пиратские программы или медиаконтент.

Объясните, что в интернете нужно быть вежливым

Это поможет не провоцировать агрессию. Если ребёнок стал объектом кибербуллинга, можно заблокировать обидчика и сообщить о происходящем администраторам соцсети. Негативный комментарий может появиться под любой публикацией. Объясните ребёнку, что к нему это не относится и подобные комментарии нужно игнорировать или отвечать на них юмором.

Резюме для детей

- ✓ Использовать надёжные пароли;
- ✓ Подключить двухфакторную аутентификацию;
- ✓ Настроить приватность в соцсетях;
- ✓ Блокировать пользователей, которые пишут негативные комментарии;
- ✓ Не переходить по ссылкам из подозрительных сообщений;
- ✓ Не публиковать в соцсетях информацию, которая может быть полезна преступникам;
- ✓ Не общаться с незнакомыми людьми;
- ✓ Не пользоваться важными приложениями при подключении к бесплатному вайфаю;
- ✓ Не провоцировать агрессию и не отвечать на неё.

Памятка

Правила безопасности в сети Интернет

Для детей 7-8 лет:

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

✓ Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером.

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

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

✓ 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.

✓ 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. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Для детей 9-12 лет к, вышеуказанным, правилам добавляем:

✓ 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.

✓ 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.

Для подростков 13-17 лет к, вышеуказанным, правилам добавляем:

✓ Обговорите с ребёнком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

✓ Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

✓ Необходимо знать, какими чатами пользуются Ваши дети.

✓ Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

✓ 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.

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

РОСПОТРЕБНАДЗОР

ЕДИНЫЙ КОНСУЛЬТАЦИОННЫЙ ЦЕНТР РОСПОТРЕБНАДЗОРА 8-800-555-49-43

О РЕКОМЕНДАЦИЯХ ПО РАБОТЕ С ГАДЖЕТАМИ ДЛЯ ШКОЛЬНИКОВ

ОБЩАЯ ПРОДОЛЖИТЕЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ ЭСО* НА УРОКЕ НЕ ДОЛЖНА ПРЕВЫШАТЬ:

	класс	время (минуты)		
для интерактивной доски	1-3	4-11		
	20	30		
для интерактивной паненли	1-3	4	5-6	7-11
	10	15	20	25
для компьютера и ноутбука	1-2	3-4	5-9	10-11
	20	25	30	35
для планшета	1-2	3-4	5-9	10-11
	10	15	20	20

СУММАРНАЯ ЕЖЕДНЕВНАЯ ПРОДОЛЖИТЕЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ ЭСО* В ШКОЛЕ И ДОМА НЕ ДОЛЖНА ПРЕВЫШАТЬ:

	класс	время (минуты)		
для интерактивной доски	1-3	4	5-9	10-11
	80	90	100	120
для интерактивной паненли	1-3	4	5-6	7-11
	30	45	80	100
для компьютера и ноутбука	1-2	3-4	5-9	10-11
	120	140	180	240
для планшета	1-2	3-4	5-9	10-11
	110	135	180	230

*ЭСО – электронные средства обучения.

ВАЖНО!

Занятия с использованием ЭСО* в возрастных группах до 5 лет не проводятся.

Подробнее на www.rospotrebnadzor.ru

Центр поддержки семьи «Детство в надежных руках»

Консультация предоставлена в рамках реализации национального проекта «Образование».

Уважаемые родители! Если у Вас возникли вопросы, связанные с воспитанием образованием и развитием Вашего ребенка, обращайтесь в Центр поддержки семьи «Детство в надежных руках»
по телефону 8-952-849-59-69

Наши специалисты бесплатно окажут Вам психолого-педагогическую, методическую и консультационную помощь в соответствии с Вашими потребностями!