## Безопасность в социальных сетях

**Уважаемые родители! Предлагаем ознакомиться с памяткой "Безопасность детей в социальных сетях", разработанной компанией "Касперский".**

**С полной версией статьи можно ознакомиться здесь:**[**https://blog.kaspersky.ru/simple-rules-kids-social/4137/**](https://blog.kaspersky.ru/simple-rules-kids-social/4137/)

***Хотите вы того или нет, но средства общения наших детей впечатляюще изменились за последнее десятилетие. Они реже встречаются и созваниваются, зато постоянно на связи в социальных сетях. В каком-то возрасте между 11 и 14 годами, в зависимости от подростковой моды и отчасти местного законодательства, ваш сын или дочь захотят завести себе учетную запись в Facebook и «ВКонтакте», но значительная мера ответственности за то, как у них пойдут дела онлайн, лежит на родителях.***

**Запрет бесполезен**

Некоторые родители ждут какой-то волшебной круглой даты вроде шестнадцатилетия или иного события, запрещая регистрироваться в соцсети до тех пор. Это безнадежный путь, потому что подросток сделает это тогда, когда в его классе иначе станет невозможно. И если вы это запрещаете, то все произойдет тайком от вас, только и всего. Вы этого не хотите. Сопротивляться этому нельзя, а значит, надо возглавить.

**Много экранов**

Если вы поставили домашний компьютер в гостиной и считаете, что теперь сетевая активность ребенка будет под присмотром, то вы упустили смартфоны, планшеты, школьные компьютеры, телевизоры, игровые приставки и, кажется, холодильники. Общаться с друзьями можно с помощью всего вышеперечисленного, и главным инструментом будет смартфон, никак иначе. В этом факте есть ряд опасностей, о которых должны знать и вы, и ребенок.

**Личная безопасность**

Наедине с компьютером или смартфоном легко забыть, что в Сети миллиарды людей и до любого пара кликов. В том числе до вашего ребенка. В Сети им могут заинтересоваться мошенники разного рода, тролли разной степени небезобидности, а также еще более опасные персонажи вроде педофилов. Чтобы максимально обезопаситься от подобных угроз, нужно научиться правилам сетевой безопасности, которые столь же важны, как правила дорожного движения. Правила просты — не выдавать людям свои имя, место учебы и проживания, сообщать родителям или другим доверенным взрослым о любых разговорах на тревожные темы, внимательно контролировать публикуемый в Сети контент. Особенно опасны фото и видео, поскольку по изображениям можно понять, где происходит дело, а смартфоны еще и заботливо снабжают фотографии геометками. Во избежание проблем на смартфоне подростка эту функцию лучше вовсе отключить.

***Главным экраном для ребенка будет смартфон. Помните об этом и учитывайте, устанавливая правила.***

**Главное правило**

Главная ошибка, подстерегающая в Сети и взрослых, и детей, — ощущение, что все это игра. Не видя перед собой лицо человека, не получая привычный отклик в виде жестов, интонации и мимики, легко почувствовать, что все это понарошку, и сказать лишнее. Вторая ошибка — непонимание, насколько широкий круг знакомых и незнакомых людей, а также бездушных роботов увидит любое слово, сказанное в Сети. Именно поэтому одна из важнейших вещей, которую надо объяснить подростку на всю оставшуюся жизнь, звучит так: не пиши в Интернете того, что не сможешь сказать человеку в глаза, стоя перед всем классом и всеми знакомыми. Только того, кто понял и прочувствовал это правило, можно выпускать на просторы соцсетей.

Для простоты понимания можно разделить эту истину на две части: «Написать опаснее, чем сказать» и «За каждым словом и действием всегда следят посторонние».

***"Не пиши в Интернете того, что не сможешь сказать человеку в глаза, стоя перед знакомыми"***

**Договоритесь «на берегу»**

Даже если вы уверены, что ребенок понял все правила, родительское сердце нет-нет да и захочет удостовериться, что дела идут благополучно. Не делайте это тайком, в идеале договоритесь с сыном или дочерью, как будет работать контроль. Комфортно ли будет ребенку открыть пароль от своей учетной записи? Добавить родителя в друзья? Или сдаться на милость специализированной программы родительского контроля? При разумном использовании последний вариант может быть наименее болезненным, поскольку качественные программы способны поднимать тревогу в определенных ситуациях (например, при появлении в переписке ключевых слов), не вынуждая при этом изучать всю переписку.

**Также желательно заранее озвучить возможные «административные меры», такие как блокировка доступа в Сеть со всех устройств до того, как сделаны домашние задания, или лишение личного смартфона за серьезные провинности. Конечно, здесь важно соблюдать меру и минимально ограничивать свободу ребенка, когда он ведет себя социально приемлемо.**

**Опасайтесь травли**

Одна из самых опасных вещей, которая происходит с подростками в соцсетях, — это онлайновая травля со стороны ровесников (в последнее время для этого явления часто используется калька с английского — кибербуллинг). Исследователями доказано, что это нешуточное явление имеет долговременные последствия, влияющие на судьбу жертв. По сравнению с обычными неприятностями в школе у онлайновой травли есть два больших опасных отличия: онлайновые преследования идут все время, не заканчиваясь после школьных часов, а также в отсутствие вышеупомянутого личного контакта принимают еще более уродливые и гипертрофированные формы.

Вариантов может быть много — подсмотреть пароль недруга и от его имени написать что-то в соцсети, выложить на обозрение одноклассников фото, ставящее жертву в неловкое положение, разгласить посторонним что-то поведанное по секрету и так далее. Эти виды травли не очень бросаются в глаза взрослым, но сильно угнетают подростка, поэтому при любых сомнениях, непонятном плохом настроении и так далее надо приложить серьезные усилия — от разговоров до мониторинга средствами родительского контроля, чтобы разобраться и прекратить травлю. В разных странах для этого есть различные организации, помогающие родителям, но даже в их отсутствие есть неплохой вариант — обратиться за помощью в школу, где учатся подростки. Также возможно обратное — вы обнаружите, что это ваш ребенок травит других. Реакция тоже должна быть незамедлительной и полномасштабной — нужно объяснить, насколько это серьезно и опасно, к каким последствиям может привести (уже бывали случаи суицида жертв и привлечения обидчиков к настоящей уголовной ответственности).

**Знайте, чем интересуются дети**

Социальные сети — не единственное, чем интересуются современные дети. Наши коллеги регулярно собирают статистику KSN (Kaspersky Security Network), основанную на нотификациях модуля «Родительский контроль». Она позволяет оценить, на какие категории сайтов с нежелательным контентом дети попадают чаще всего. Данная статистика собирается анонимно с тех компьютеров, где работает модуль «Родительский контроль», вне зависимости от того, отмечена ли категория родителями (блокируется ли она «Родительским контролем»). Мы исключили из анализа социальные сети и составили рейтинг посещений сайтов десяти выбранных нами категорий в России:

Стоит отметить, что в России выше, чем в остальных анализируемых странах, процент посещаемости сайтов категории «Оружие» и «Нецензурная лексика» — только у нас эти категории оказались в первой тройке рейтинга. Более подробно с рейтингом можно ознакомиться на сайте SecureList.

**Станьте попутчиком**

Лучший способ не потерять контакт с ребенком по мере его погружения в сетевой мир — делать что-то вместе. Помогите ему завести учетную запись ФБ и правильно настроить уровень конфиденциальности. Читайте профильные новости (например, на нашем сайте и у наших друзей с Threatpost) и рассказывайте ребенку, что фотографии в Snapchat вовсе не являются самоуничтожающимися, а по контекстной рекламе на веб-страницах можно догадаться, что подросток ранее искал в Google. Подростки всерьез озабочены вопросами конфиденциальности, поэтому, став единомышленником ребенка в этом вопросе, родитель может заработать немало очков в рейтинге доверия.