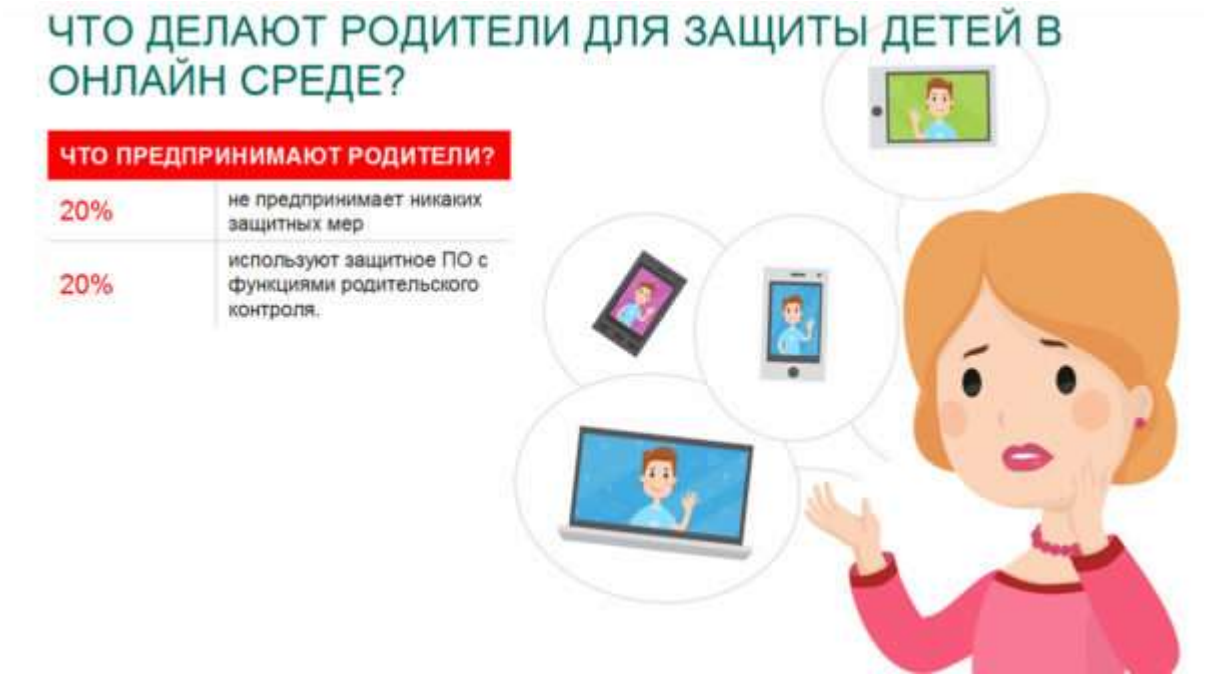
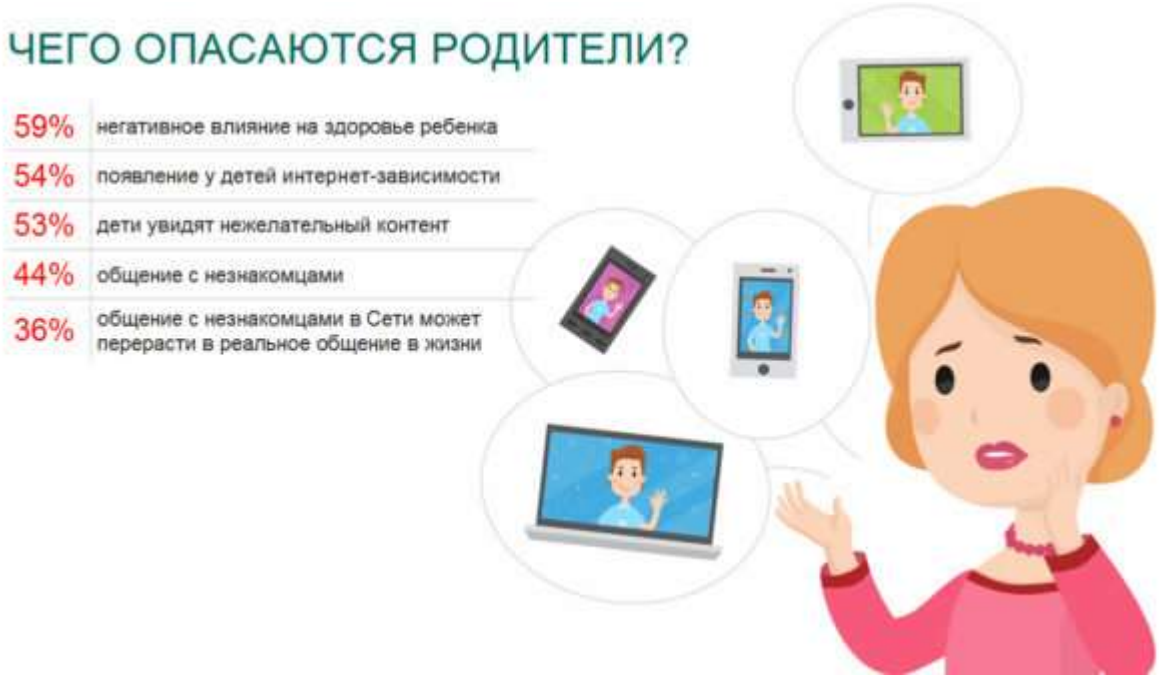
По статистике большинство детей дружат в интернете с незнакомцами, указывают в интернете личные данные и скрывают от родителей часть своей виртуальной жизни.

По исследованиям «Лаборатории Касперского», на вопрос «Волнуетесь ли вы, что интернет окажет негативное влияние на ваших детей?» 95% родителей отвечают: «Волнуемся». Если же спросить: «Что вы делаете, чтобы обезопасить детей?», то выясняется, что большинство ничего не делают, только волнуются.

А также 58% детей сообщают, что они что-то скрывают от родителей из того, что делают в интернете – заходят на нужные им сайты через анонимайзеры, тор-браузеры, но чаще всего просто выходят в интернет тогда, когда родителей нет дома.



Чего боятся родители в интернете?



КАК ОБЕЗОПАСИТЬ ДЕТЕЙ

Малышам интернет не нужен

Маленьким детям вообще в интернете делать нечего, им все можно скачать. Скачайте им игры, мультфильмы и не выпускайте в интернет.

Есть специальные программы – детские лаунчеры. Вы устанавливаете лаунчер на свой телефон, при запуске он у вас спрашивает, какие программы можно ребенку показывать, а какие нельзя, и работает защитной оболочкой. То есть когда вы даете ребенку свой телефон, лаунчер блокирует в нем интернет и показывает ребенку только игры, только мультики, только то, что вы для ребенка скачали, и на время становится детским.

То же самое умеют делать программы родительского контроля, если покопаться в настройках и указать им, что нельзя, а что можно. Поэтому ребенка до 7 лет, до того момента, как начнется школа, в интернет не пускать, обеспечивая его всем необходимым в офлайне. Если ребенок оказывается в интернете раньше, это наша родительская блажь, потому что необходимости в этом нет. Чтобы выбрать новые игры, мультики или раскраски, ему совсем не нужно быть в Сети одному, вы можете (и должны!) быть при этом рядом.

Но обычно ребенок довольно рано оказывается в YouTube –его очень любят родители, и у большинства детей это первое место, с которым они знакомятся в интернете.

Родители сажают их смотреть мультики, показывают, как включить следующий мультфильм, и, довольные, занимаются своими делами. Но ребенок перелистнет пару видео и откроет мультфильм – сейчас это почему-то очень популярная странная тема – про диснеевских персонажей, где очень натуралистично изображаются секс, насилие и всякие неприятные физиологические процессы.

Например, он смотрел «Машу и Медведя», а потом на экране с рекомендацией «Предлагаем посмотреть» вылез этот мультфильм. Ребенок, может, еще даже читать не умеет, он ткнет в этот мультик и будет смотреть на секс в исполнении диснеевских героев. Поэтому, запуская ребенка на YouTube, родители должны ему объяснить: «Я тебе разрешаю смотреть только «Машу и Медведя» – видишь иконки с «Машей и Медведем»? Они выглядят вот так, и ни на какие другие ты не нажимаешь».

Ребенок выходит в интернет

Если ребенок начинает ходить в интернет, следует предварительно ему объяснить, что там может быть что-то нехорошее. Сразу же установите программу родительского контроля, и ребенок должен знать о том, что она установлена. Объясните ему, что вы поставили такую программу, чтобы он не увидел ничего страшного, чтобы не сидел в интернете слишком долго, потому что от этого испортится зрение, что эта программа – его защитник, потому что если вдруг вы решите поставить такую программу, когда он уже станет, например, подростком, он может воспринять это не как защиту, а как контроль или, еще хуже, попытку слежки.

Скажите ему, что если он увидел вот такое уведомление, значит, он случайно чуть не попал на сайт, на который ему нельзя ходить. Ребенок должен понимать, зачем ему нужна эта программа, почему периодически он видит такие уведомления – а видеть он их будет, потому что те же баннерные сети есть везде, они есть даже на детских сайтах, причем сайт может быть полностью с детским содержимым, а баннерная сеть совсем не детская: «Сенсация! Ученые удивились!..»

Когда ребенок только вышел в интернет, программа родительского контроля должна быть закручена по максимуму.

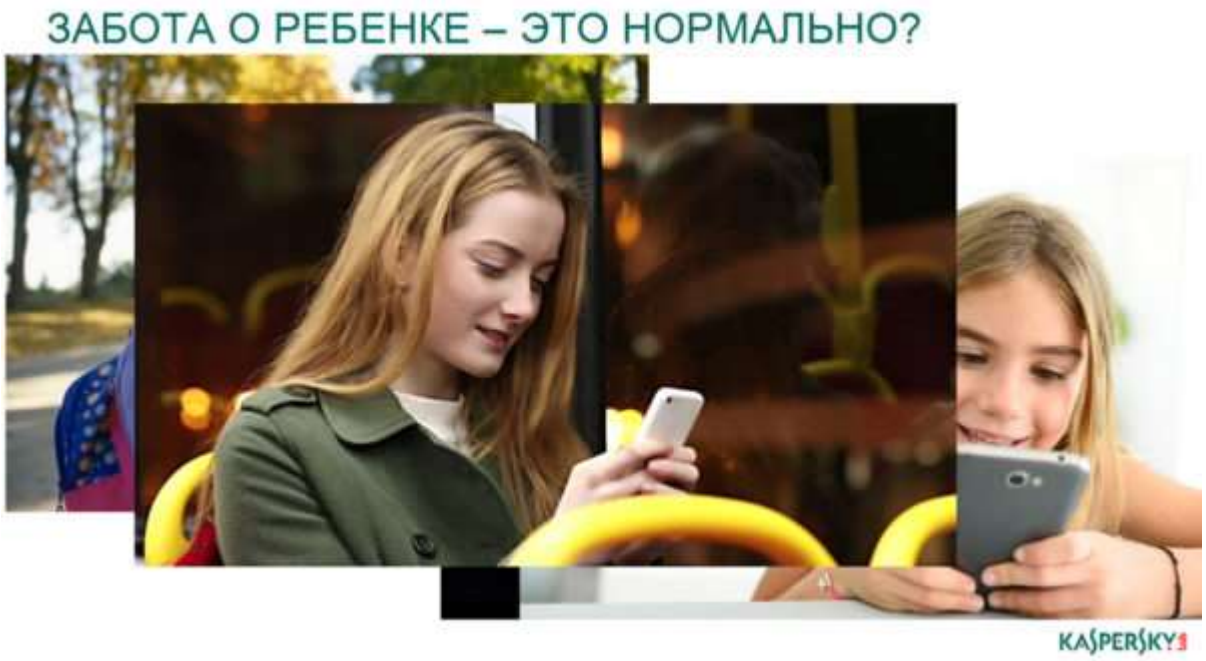
Ребенок растет, и мы потихоньку снимаем ограничения, и к условным 16 годам у него, может, ограничений и не останется, у него будет возможность читать все, если ему очень интересно, но при этом вам все равно будут приходить уведомления от программы родительского контроля о том, что ребенок искал в интернете.

Конечно, ребенок, зная о программе родительского контроля, может воспользоваться гаджетом приятеля, но сначала он поищет эти условные «запретные вещи» все-таки у себя в телефоне, и вы благодаря такой программе не будете последним человеком, который узнает об этом интересе.

Программа родительского контроля – это инструмент для «ленивых»: она очень нужна, если родители хотят заботиться о детской безопасности, и поможет родителям даже тогда, когда они не хотят много чего делать, да и не знают, что именно и где нужно сделать. Она удобна, потому что в ней все настройки в одном месте, а управляете вы ею со своего гаджета. Но и без программы родители могут настроить безопасность и приватность страниц, которые посещает ребенок, например, безопасный поиск, который программа родительского контроля включает автоматически.

То есть у родителя есть выбор: можно самостоятельно все настроить и постоянно отслеживать, какие появились новые сервисы для настраивания, а можно установить специальное программное оборудование (программа родительского контроля), и с этим справится кто угодно, даже те, кто считает, что он вообще не способен что-то самостоятельно сделать на компьютере.

Во всех социальных сетях также есть и безопасный поиск, и настройки приватности и безопасности, их тоже нужно настроить вместе с ребенком, сделать так, чтобы информацию видели только друзья и чтобы возможность писать сообщения была только у друзей, чтобы абы кто не начинал ребенка, например, троллить.



В YouTube есть возможность настроить безопасный режим, но он работает странно: он может не показывать ребенку видео, которое другие пользователи отметили как неприемлемое. Это,

к сожалению, не защищает маленьких детей, потому что, например, трейлер фильма ужасов никто не отметит как неприемлемое видео, а, скажем, трехлетний ребенок может, посмотрев его, получить серьезную травму.

В аккаунтах Google и Apple есть настройки семейного доступа, которые позволяют отфильтровать выдачу программ, фильмов и прочего по возрастному рейтингу, чтобы ребенку не был доступен контент с пометкой 18+.

Есть защита от нежелательных покупок – это тоже очень важно, потому что многие родители «привязывают» к аккаунту ребенка свою карточку – мол, если он что-то купил, мне приходит СМС-уведомление, но это не лучший вариант, лучше сделать семейный доступ, он очень легко настраивается – тогда ребенок сможет платить карточкой родителей, но только с вашего одобрения, то есть СМС придет не постфактум, что что-то уже куплено, а с запросом на разрешение покупки, причем вы увидите, что именно ребенок хочет купить..

Что контролировать, а что нет?

Совет: если ребенок завел аккаунт в соцсетях, добавьте его в друзья, дружите с открытыми глазами. Вы увидите – ваши отношения выйдут на другой уровень, станут лучше, потому что для них общение там – основное. Перекидывайтесь мемами и гифками, обменивайтесь смайликами и пишите друг другу на стене. Если вы знаете, что ребенок общается в соцсетях только со своими реальными друзьями, и следите, чтобы это было так, то незачем лезть в переписки. Но, само собой, все, что есть в публичном доступе – группы, общение в группах – ребенок от вас скрывать не должен. И проверять время от времени – что за новые друзья у него появились и в какие группы он вступил – надо обязательно. «Если у ребенка много «друзей», с которыми нет контакта в реальной жизни, это повод, чтобы бить тревогу.

ЧЕМУ УЧИТЬ РЕБЕНКА

Интернет-самозащита

Если ты заводишь страничку в социальной сети, то первым делом ты должен решить – у тебя будет публичный аккаунт или приватный. Сегодня есть такая странная профессия – блогер, и многие хотят ими быть, но нельзя сидеть на двух стульях и рассчитывать на то, что и вас будут лайкать все подряд, и аккаунт будет приватным.

Соответственно, если аккаунт предполагается **публичным**, в нем следует повесить только свою фотографию, назвать имя-фамилию или назваться так, как вы бы хотели, чтобы вас называли, и больше никаких данных не публиковать. В друзья в публичный аккаунт добавляют обычно тех, кто нужен, чтобы его раскручивать, и в целом к ведению этой странички следует относиться как к работе. Публичный аккаунт – это как сцена, на которую ты выходишь, и перед тобой сидит аудитория незнакомых людей. Есть некоторая вероятность, что после этого «выступления» они начнут задавать вопросы, но все это должно происходить не в личных сообщениях, а в публичных комментариях – это же работа, а если общение переходит в личную зону, оно должно продолжаться в тех же рамках, каких оно придерживается в публичном пространстве.

Если ты решаешь, что аккаунт **приватный** и что ты хочешь его использовать для общения со своими одноклассниками, родителями, друзьями и прочими, ты должен сразу пойти в настройки и сделать так, чтобы страничка была доступна только для друзей.

Относись к интернету как к реальному миру и сравнивай поступки, которые ты совершаешь в интернете, с тем, что ты делаешь в реальной жизни.

Готов ли ты запускать в свой дом, в свою комнату всех подряд? Так же и в интернете: твой приватный аккаунт – это твой дом, и не следует туда пускать незнакомцев. Готов ли ты сплясать голым на столе перед своими одноклассниками, соседями и родителями? Если нет, то вряд ли стоит размещать фото и видео, где ты это делаешь, в интернете и в своем аккаунте.

Дружить в приватном аккаунте стоит только с теми, кого ты знаешь в реальном мире или с теми, с кем ты бы мог познакомиться в реальном мире. Например, твоя подруга ходит на курсы французского и решает познакомить тебя со своим другом из группы. Лет 15 назад ей бы пришлось вас обоих звать в кино или в кафе, а сейчас она кинет ему ссылку на твой аккаунт, тебе – на его, и вот вы подружились. Это совершенно нормальная ситуация.

Во всех остальных случаях с незнакомыми людьми в социальных сетях общаться нельзя, потому что у нас там обычно много персональных данных: например, 20% подростков публикуют в аккаунте номер телефона, а 80% указывают номер школы. Кстати, когда ты размещаешь персональную информацию и личные фотографии на своей закрытой страничке и считаешь, что она таким образом защищена, не забывай, что аккаунты сплошь и рядом взламывают – наверняка ты часто слышишь о таких случаях, и вся информация становится доступна неизвестно кому.

Анонимно можно общаться вне социальных сетей с кем угодно, но если ты это делаешь, ты не делишься персональной информацией, не сообщаешь свое имя и фамилию, потому что по именам и фамилиям в соцсетях можно легко найти человека.

Не общайся в приватном пространстве с незнакомыми людьми и всегда имей в виду, что никогда нельзя быть уверенным в том, что человек – тот, за кого он себя выдает. Мы, конечно, всегда ищем для себя наиболее комфортное объяснение и думаем: да нет, вряд ли это маньяк-педофил, наверное, у него просто нет друзей, или я ему просто понравилась, он где-то нашел мою фотографию, я такая классная, но проблема в том, что мы никогда не получим достоверного ответа на этот вопрос.

Интернет-гигиена

Не реагируй ни на какие просьбы срочно переслать деньги или перейти по какой-то ссылке – ни в социальной сети, ни в электронной почте. Ходи по проверенным страницам с включенным антивирусом, потому что вирусы заражают и большие сайты!

В этом году, например, были два случая, когда были заражены страницы крупнейших новостных агентств.

Это миф, что вирусы водятся только на каких-то подозрительных порнографических страницах, и если туда не ходить, то все будет в порядке.

Антивирусная программа дает 99,999…% гарантии – но всегда есть новые программы, которые еще не успели добавиться в базу.

Чтобы защититься от них, не ходи по баннерным сетям и не кликай на них, не ищи, где скачать бесплатно новые фильмы. Для безопасного скачивания софта следует пользоваться не торрентами, а сайтами разработчиков, для просмотра фильмов – лицензионными видеосервисами. Это то, что называется базовой интернет-гигиеной.

Помни, что в интернете, как и в реальной жизни, есть мошенники. Не бросайся покупать что-то, что тебе обещают в три раза дешевле, отнесись с подозрением к сообщению от друга с просьбой кинуть туда-то 50 рублей или проголосовать за него – не поленись уточнить, например, в WhatsApp, от него ли это сообщение, потому что, как правило, это мошеннические схемы.

Материал подготовлен при помощи интернет-ресурсов: http://stop-ugroza.ru/, https://lizaalert.org/, https://www.kaspersky.ru/