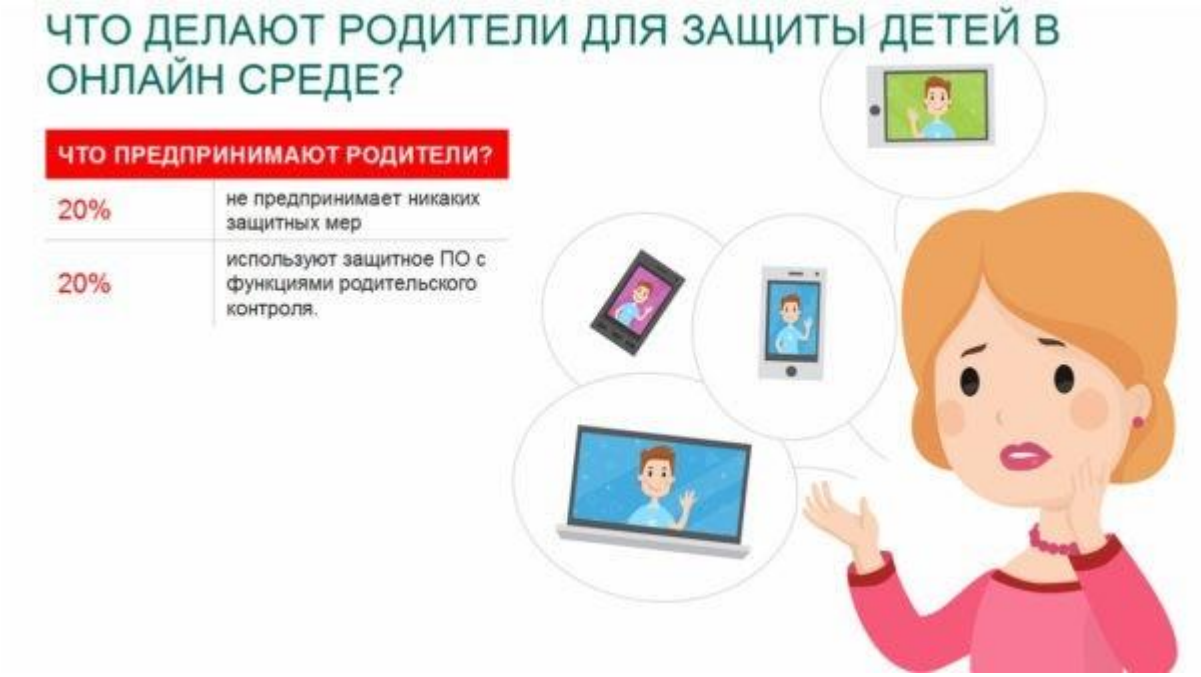
По статистике большинство детей дружат в интернете с незнакомцами, указывают в интернете личные данные и скрывают от родителей часть своей виртуальной жизни. Мария Наместникова, эксперт «Лаборатории Касперского» по детской онлайн-безопасности, рассказала «Правмиру» о том, чего следует опасаться в интернете и как защитить своего ребенка.

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?

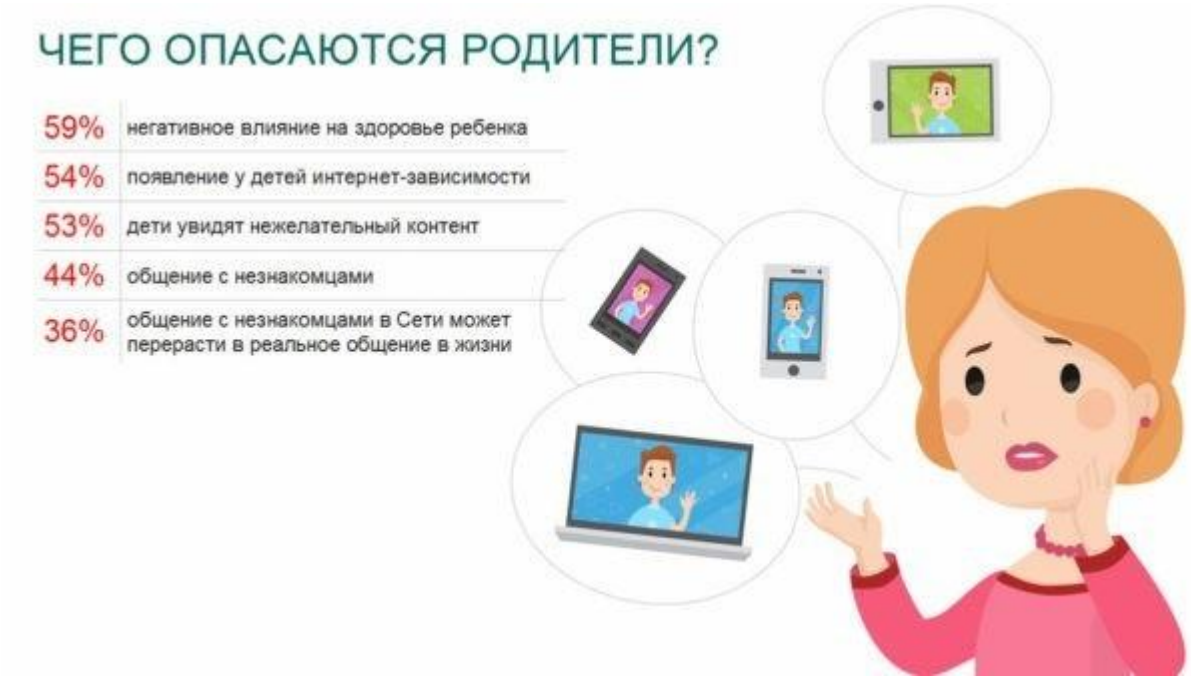
59% родителей боятся негативного влияния интернета на здоровье (зрение, осанка);

54% опасаются интернет-зависимости, потому что СМИ любят тиражировать истории про детей с интернет-зависимостью – когда ребенку запретили интернет и он сделал что-то ужасное;

53% родителей боятся, что ребенок увидит в интернете нежелательный контент, причем, как правило, под нежелательным контентом имеется в виду порнография, на втором месте – сцены насилия, и на третьем с весны прошлого года – группы смерти;

44% боятся общения с незнакомыми;

36% боятся того, что общение с незнакомцами в Сети перейдет в реальную жизнь.



1. Утрата денег

Первый вид опасностей – те, которые связаны с кражей денег.

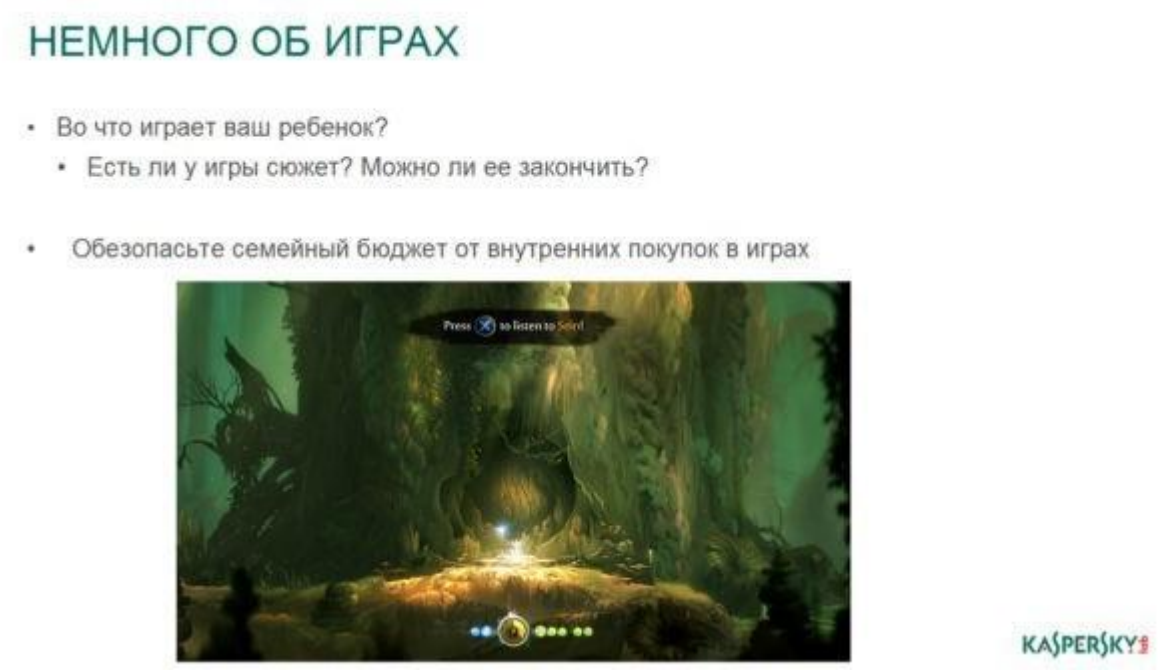
Фишинг – это выманивание паролей от различных сервисов, в том числе личных страниц во «ВКонтакте» или Steam, чем дети-подростки обычно очень дорожат. Их крадут, чтобы получить доступ к персональной информации, чтобы делать спам-рассылки, чтобы продолжать использовать – например, аккаунты игровой платформы Steam, где распространяются игры и есть своя социальная сеть.

Steam – это рекордсмен по числу онлайн-пользователей, их там больше, чем даже в YouTube. Поскольку участники покупают игры на свой аккаунт, «развивают» своих персонажей в многопользовательских онлайн-играх, «заливают» туда деньги и время, эти аккаунты могут достаточно дорого стоить – страничка с 1000 наигранных часов в какую-нибудь популярную многопользовательскую игру с очень развитым персонажем продастся на черном рынке за весьма неплохие деньги.

Еще одна техническая опасность – **вредоносный код**: например, пользователь перешел по какой-то ссылке, и компьютер заблокировался, и теперь пользователь видит только сообщение «Заплатите деньги туда-то, и компьютер разблокируется». Причем гарантии, что он разблокируется после оплаты, к сожалению, нет. Есть и другой вредоносный код: тот, что незаметно работает на компьютере, отправляя злоумышленникам те же логины/пароли или данные платежных карт.

Обычное мошенничество – в интернете встречается так же часто, как и в реальной жизни. Его можно охарактеризовать всем известной поговоркой «Бесплатный сыр бывает только в мышеловке». Например, предлагается купить смартфон по цене значительно ниже рыночной, человек отправляет деньги, но телефон так и не получает. Это очень популярная схема мошенничества: дорогой товар за небольшие деньги. И это очень хорошо срабатывает в ситуации с подростками, потому что они часто прицельно копят деньги на какой-нибудь игровой компьютер, и если они внезапно видят его не за 60, а за 20 тысяч рублей, то могут с радостью заказать его и перевести деньги.

Определенную опасность для семейного бюджета представляют также и онлайн-игры – в них часто есть **встроенные внутренние покупки**. Чтобы обезопасить себя от этих трат, убедитесь, что ребенок не может тратить деньги с вашей карточки, привязанной к онлайн-игре, в том числе и если он зайдет в вашу игру.



Это может происходить, если система запрашивает подтверждение не каждый раз при совершении покупки, а, например, раз в полчаса, раз в сутки. За полчаса можно многое успеть. Одна английская девочка четырех лет, играя, пока папа варил макароны, потратила больше 1000 фунтов, причем ругать ее было за это бесполезно: она просто играла и даже не знала, что тратит деньги, нажимая на «да» и «купить».

2. Зависимость

Интернет-зависимость чаще всего ассоциируется с играми, и родители, когда говорят о зависимости, имеют в виду прежде всего именно ее.

Сегодня играют все дети, но в разные игры. Глобально их можно разделить на две группы: первая – это **просто игры**, в которые играют час-другой в день, проходят за несколько недель, и все.

Вторая – это так называемые **массовые мультиплеерные онлайн-игры**, в которые можно играть годами, развивая своих персонажей, приобретая для них какие-то качества или оборудование и так далее.

Если ребенок играет в такую игру, надо серьезно подумать, как это ограничивать, потому что такие игры действительно вызывают привыкание как у детей, так и у взрослых.

Происходит это за счет того, что такие игры вбрасывают в детей якоря: один якорь – это социальные связи с другими игроками, которыми ребенок обрастает за время игры, второй – это финансовые вложения: я купил крутой танк, надо на нем покататься, я уже столько

сюда вложил, что жалко бросать, третий – это потраченное время: как отказаться от игры, если я играю в нее уже полтора-два года.

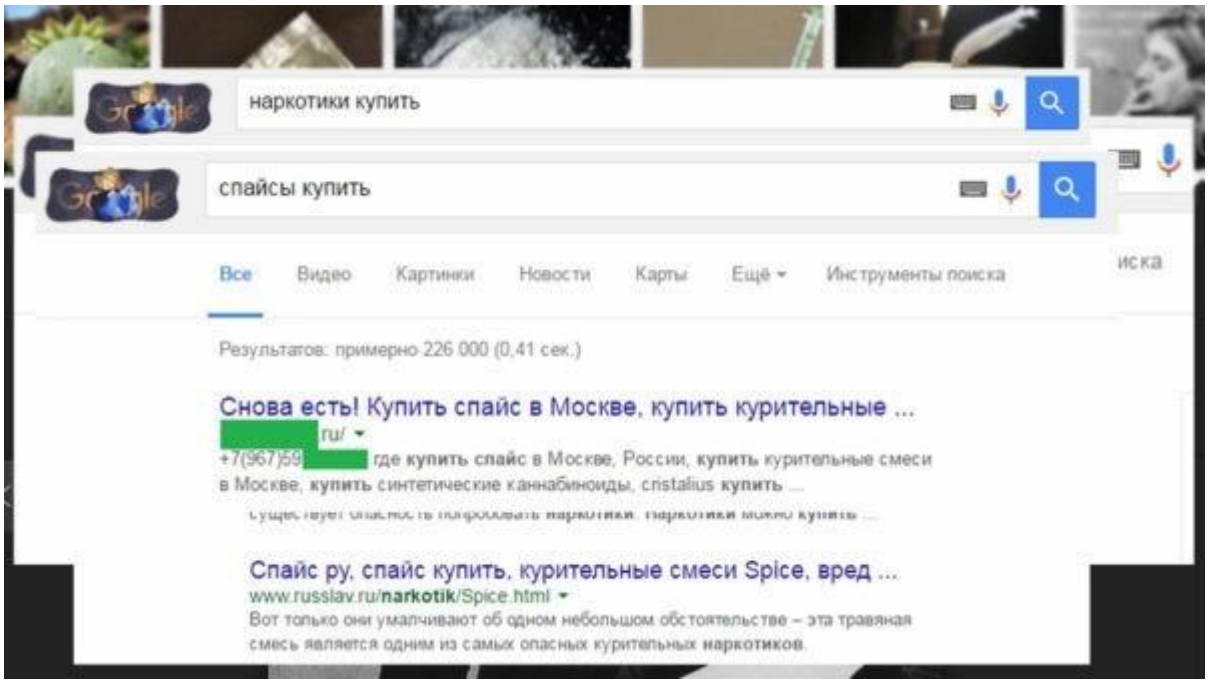
Зависимость – это болезнь, к ней следует так и относиться, и если ребенок ради игры начинает отказываться от еды, от сна, и тем более если проявляет агрессию, когда ему не дают играть, то надо идти к специалисту.

3. Нежелательное содержание

Помимо порнографии, которая безусловно лидирует в списке того, что родители не хотели бы, чтобы видели их дети, в незащищенном интернете можно увидеть массу других нежелательных вещей. На сайтах новостей достаточно часто появляются фотографии и видеозаписи с мест катастроф, где можно видеть сцены убийства, насилия, аварии, теракты и их последствия. Более того, такие иллюстрации могут оказаться в самых неожиданных местах – например, на безобидном на вид сайте-агрегаторе смешных (!) картинок.

При попытке поиска наркотиков через поисковые системы можно обнаружить на первой же странице результатов не рассказ о последствиях их приема, а контакты продавцов, причем, возможно, сами сайты заблокированы Роскомнадзором и зайти на них нельзя, но контакты могут быть видны на странице поисковых результатов.

И, к сожалению, такие сайты появляются быстрее, чем Роскомнадзор успевает их блокировать. Кроме того, это может быть объявление на сайте, который блокировке не подлежит, – например, в форуме реабилитирующихся. Конечно, через пару часов модераторы его удалят, но какое-то время оно повисит.



Помимо этого, безусловно нежелательным для ребенка контентом является все, что относится к самоубийствам и способам их осуществления, а родителям девочек следует обратить особое внимание на интерес дочерей к картинкам с анорексичными моделями – часто они распространяются как образец для подражания, и из-за этой пропаганды,

особенно если она исходит от подруг, девочки начинают терзать себя диетами и отказываются от еды.

4. Незнакомцы

На занятиях я объясняю подросткам – а они этому обычно очень удивляются, – что у взрослых, как правило, нет первоочередной цели пообщаться, в отличие от подростков, которые идут в интернет в основном за этим.

У нормального взрослого человека нет безудержного желания общаться с незнакомыми детьми, добавлять их в друзья, начинать с ними интенсивную коммуникацию, и, как правило, если взрослый человек приходит к незнакомому подростку, значит, ему наверняка что-то от него нужно.

По нашим исследованиям, 90% московских школьников получают в интернете предложение о дружбе от незнакомых людей, и 53% их принимают. Разговаривая об этом с детьми, я привожу такой пример: к тебе на улице подходит молодой человек лет тридцати пяти, называет тебя по имени и говорит: «Аня, давай дружить!» Большинство, конечно, отвечают, что они убегут. Однако когда то же самое происходит в сети, они совершенно спокойно начинают с этим человеком общаться.

Проблема состоит в том, что многие подростки чрезвычайно доверчивы, и незнакомец, который с какой-то целью хочет «подружиться» с ребенком, может за считанные недели в его глазах стать самым близким его человеком, единственным, кто его понимает и так далее. Достигается это с помощью манипулятивных техник и самых простых приемов, вплоть до активного слушания, когда ребенок что-то рассказывает собеседнику, собеседник повторяет это своими словами, и ребенок думает: о, он меня понимает, как никто! (Кстати, попытка втереться в доверие ребенка с тем, чтобы в дальнейшем его как-то использовать, называется **онлайн-грумминг**.)

Ребенок начинает относиться к этому человеку как к действительно близкому и заслуживающему того, чтобы с ним делились и самой интимной информацией, и контактными данными, и фотографиями, не предназначенными для чужих глаз.

Если хотите, проведите эксперимент: возьмите в интернете фото какого-нибудь юного мулата, назовите его, например, Хорхе Домингос, сделайте аккаунт во «ВКонтакте», напишите, что ему 15 лет и попробуйте добавиться в друзья к подросткам. Вы увидите, как они легко и быстро внесут вашего Хорхе в свой список друзей – никому из них не придет в голову проверить имя, фамилию и фотографию, а если вдруг и придет, то вы можете вздохнуть и сказать: да, это правда, я не Хорхе, я на самом деле Ваня Иванов, вот мое фото – и пошлете другую чужую фотографию, и тогда они уж точно будут уверены в том, что вы написали правду.

Я в принципе против общения с незнакомыми людьми в интернете – именно потому, что нет никакого способа убедиться в том, что этот человек – тот, за кого он себя выдает, и если из ста случаев всего один – это человек с преступными намерениями, все равно это повод, чтобы никому не доверять. Вы просите фото, чтобы удостовериться в том, что пол и возраст соответствуют заявленным – и получаете того же условного Хорхе Домингоса.

Разговор по скайпу дает большую уверенность, но если это, например, группа педофилов, у них может быть «на крючке» ребенок, которого они с этой целью используют. Конечно, это достаточно сложная конструкция, но некоторая вероятность такого варианта есть, а значит, этот вариант тоже не дает стопроцентной уверенности.

Самый надежный способ убедиться в том, что человек – тот, за кого он себя выдает, и это же самый опасный способ – личная встреча. Если ребенок пришел на встречу, и там оказался его ровесник, и они два часа прообщались, и его не завербовали в секту, не

продали ему наркотики и не посадили в машину к взрослому дядьке, который не увез его в лес и не оставил там убитым, то на следующей встрече вряд ли произойдет что-то из перечисленного, но, конечно, проверять таким способом, случится ли все это, нельзя.

Кстати, несмотря на то, что большинство родителей думает: ладно, пусть общается с кем угодно в интернете, он же умный и на личную встречу не пойдет, 55% детей по нашим опросам положительно отвечают на вопрос «Принимаете ли вы приглашения дружить от незнакомых людей» и 45% из них готовы встречаться лично, а многие пишут в анкете: «А я уже встречался!»

Более или менее безопасная встреча – это когда встречаются целой группой с форума по интересам или из игры – например, командой игроков в танки (пять человек) или даже целой гильдией (тридцать, пятьдесят человек). Встретились, посмотрели друг на друга, убедились, что это реальные люди, соответствующие заявленному возрасту и полу. Если мы говорим об играх, то убедиться в том, что товарищи по игре – те, за кого они себя выдают, позволяет TeamSpeak: система коллективного общения через гарнитуру во время игры. Так слышно, по крайней мере, мужчина там или женщина, взрослый или ребенок.

Проверка IP-адреса, геопривязки фотографий и прочего – это занятие для профессионалов из, скажем, МВД или ФСБ, в домашних условиях получить достоверную информацию в результате такого «расследования» сложно.

Безусловно, незнакомец может действительно оказаться ровесником ребенка, который просто хочет общаться по причине сходства интересов, потому что понравилась фотография и т.д., но, поскольку достоверно установить это нельзя, ребенок должен понимать, что там, где размещается его персональная информация, он должен к каждому относиться с недоверием.

Периодически разработчики предлагают технологии, позволяющие устанавливать личность каждого человека, входящего в интернет, но мы же все против. Идея того же входа во «ВКонтакт» по паспортам была отвергнута, потому что мы за тайну частной жизни и приватное общение. Безопасность и приватное общение всегда на весах друг против друга, и сегодня общество выбирает приватность.

Педофилы. В Америке педофилы состоят на учете в национальной базе – в нее попадают те, чья вина была подтверждена, или они отбыли наказание, или у них в ходе обследования психотерапевтом обнаружились такие симптомы, и прочие люди, по разным причинам попавшие под подозрение. Все соседи информируются о том, что рядом с ними живет человек, находящийся в этой базе. У нас такой системы, к сожалению, нет, и поэтому люди с подобными расстройствами чувствуют себя достаточно свободно. С появлением интернета они получили новые возможности для знакомства с детьми и новые способы реализации своих наклонностей.

В США 20% детей получают сообщения нежелательного характера, 25% получивших рассказывают об этом родителям, а 75%, соответственно, не рассказывают.

Современные педофилы далеко не всегда хотят лично встретиться с ребенком, сегодня они гораздо чаще хотят получить от него порнографический контент – фотографии интимного содержания, это называется **секстинг**.

Для этого ребенка могут обманывать, называясь модельным агентством (девочки часто легко верят в такие истории) или втираясь в доверие и влюбляя его в себя, уговаривать, ссылаясь на его знакомых («Твои друзья давно все прислали»), а потом шантажировать, чтобы получить еще («Я твое фото покажу маме, разошлю твоим одноклассникам»), запугивать. Передача таких фотографий – это совершенно не безобидно, потому что может дойти до вовлечения ребенка в порно-индустрию. Кстати, представители МВД говорят, что, как правило, у одного педофила «в разработке» одновременно может быть от 10 до 30 детей.

Но истории, когда конечная цель – личная встреча, тоже бывают. В Америке был случай, когда педофил два года (!) выстраивал отношения по переписке с девушкой, у них была виртуальная любовь, прежде чем он предложил встретиться. В результате он оказался мало того, что гораздо старше заявленного возраста, но и к тому же не один, и девушку сначала насиловали, а потом должны были убить, и ее спасло чудо: этот дом был под наблюдением у ФБР, и они как раз планировали операцию по его захвату, так что ей просто повезло. Теперь она ездит по школам и рассказывает свою историю, предостерегая подростков.

Наркоторговцы. Изначально преследуют ту же цель, что и педофилы – войти в доверие, поэтому точно так же могут долго общаться с ребенком, устанавливая контакт, могут представиться сверстником и ждать подходящего момента. Подходящий момент – это когда у ребенка возникает проблемная ситуация, о которой его «друг»-наркоторговец от него же и узнает, потому что ведь они друзья: ребенок поругался с родителями, поссорился с друзьями, у него проблемы с девушкой, ему плохо, он страдает, и «друг» тут как тут: готов помочь, пожалеть, подсказать, а заодно у него есть классное лекарство от всех печалей.

Секты. Если раньше у метро стояла женщина или парень, которые пытались поймать прохожего за рукав и в течение минуты поговорить с ним о Боге, то теперь этих людей там нет – они все в интернете. И подростки – важная для них аудитория. Действуют они по той же схеме: давай дружить, я пообщаюсь с тобой несколько месяцев, стану твоим лучшим другом, а потом, когда тебе станет плохо, я поговорю с тобой о Боге, и ты будешь со мной в одной секте. Кстати, увести ребенка в секту может и ровесник, который сам состоит в секте, но не ставил своей задачей вовлечение в нее ребенка – он просто с ним общался.

Кибербуллинг. Буллинг – достаточно новый для нас термин, означающий хорошо знакомое явление – травлю. Кибербуллинг – это травля в интернете. Травля существует столько, сколько существует школа. В основном это делают знакомые люди, но может возникнуть ситуация, когда ребенка травят в интернете, и тут к нему в друзья стучится симпатичный ровесник, начинает с ним дружить, ребенок рассказывает ему какие-то достаточно личные вещи про себя, а в результате оказывается, что этот «симпатичный ровесник» – один из тех, кто травит его в параллельной ветке, и эта информация используется против него.

Кстати, кибербуллинг более опасен, чем травля в реальном мире, потому что, во-первых, он незаметен для учителей и родителей (в отличие от травли в школе), и во-вторых,

потому что ребенок уходит из школы и отдыхает от травли, а кибербуллинг может происходить круглосуточно.

«Синие киты». У меня большие претензии к СМИ из-за этой истории. Да, действительно были суицидные группы, и знали про них, условно говоря, несколько десятков подростков, которые были в этих группах. После того как об этом написали, все впали в истерику, все дети-подростки об этом узнали, и теперь меня в каждой детской аудитории спрашивают: «Что вы думаете про «синих китов»?» Слава Богу, этой осенью все это наконец пошло на спад.

История с «синими китами» во многом тоже, во-первых, об общении с незнакомцами в Сети, а во-вторых, об открытости персональных данных. Читая рассказы тех, кто имел к этому отношение, можно часто видеть, как «кураторы» говорили: если ты не сделаешь то-то и то-то, мы убьем твою семью – и при этом упоминали, как зовут родителей, где они работают и так далее, но в этом нет ничего таинственного: всю информацию они брали из тех же соцсетей, где в статусе ребенка обозначено, кто его мама, а в статусе мамы – вся информация о месте ее работы, а доступ к персональной информации дети давали сами, добавляя к себе в друзья незнакомых людей.

Конечно, никто никого не убивал, но это были очень эффективные «страшилки» за счет того, что в них было очень много персональных данных.

Сколько детей реально совершили попытку суицида из-за «синих китов», никто точно не знает, потому что предъявляемые статистики противоречивы и не дают представления об истинных мотивах детей. Мы, исследователи интернета, со своей стороны можем только сказать, что эта наша история настолько громко прозвучала, что распространилась по всему миру.

КАК ОБЕЗОПАСИТЬ ДЕТЕЙ

Малышам интернет не нужен

Я считаю, что 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 мы рекомендуем 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 – я его не люблю, но 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». Хотя, повторю, я считаю, что детям до 7 лет делать в интернете нечего, в том числе и на YouTube.

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 и про наркотики читать, если ему очень интересно, и порнографию смотреть, если ему очень хочется, но при этом вам все равно будут приходить уведомления от программы родительского контроля о том, что ребенок искал в интернете наркотики или порнографический контент.

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

Мне часто говорят родители, что «не смогут настроить» такую программу, или даже не знают, где ее взять и как установить. 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.

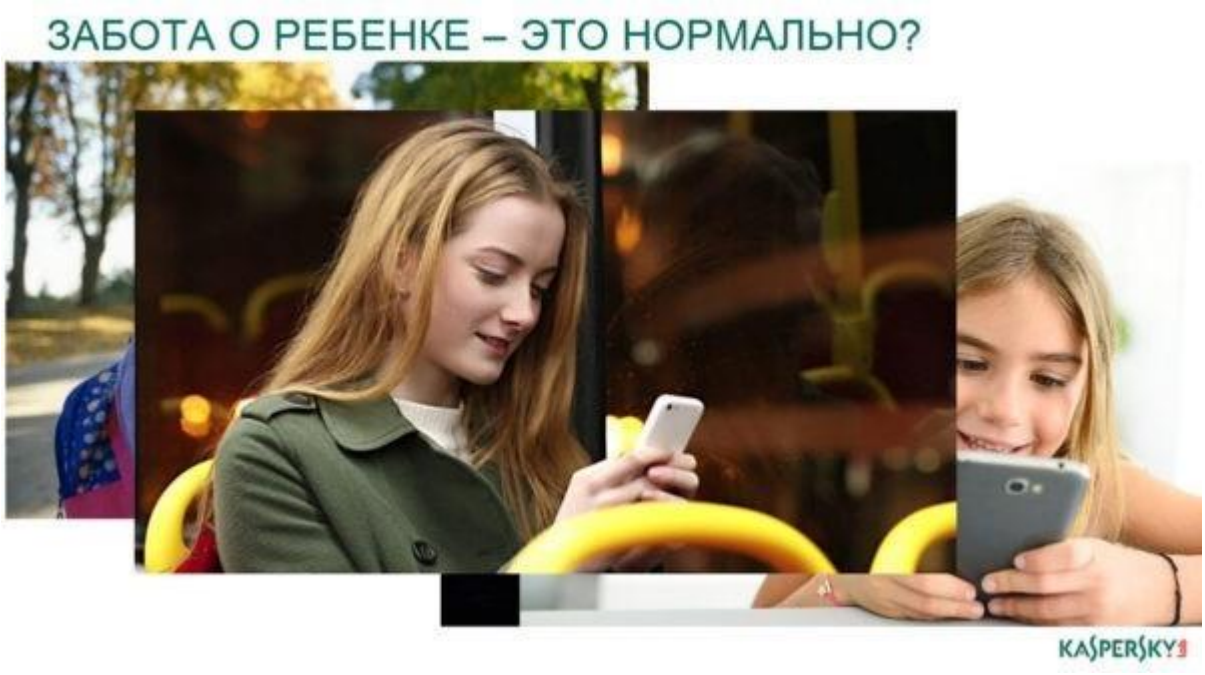
«Яндекс» и Google умеют фильтровать свои результаты, и если у вас включен безопасный поиск, то когда ребенок ищет что-то спорное, например, «трава» или «травка» – а он вполне может искать рисунок травки, – то ни Google, ни «Яндекс» не выдадут ему ничего про марихуану.

Или если ребенок ввел в поисковое поле «учительница» или «школьница», при включенном безопасном поиске он не увидит сомнительных фотографий, которых будет много, если он не включен. Если включен безопасный поиск, то основные поисковые системы умеют реагировать на запросы типа «Как совершить самоубийство» тем, что они начинают предлагать линию помощи.

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 не спрячет от маленького ребенка те мультфильмы, о которых я говорила, но 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.

Более того – эти запросы приходят, даже если программа бесплатная, что очень удобно. В Apple вообще есть масса полезных настроек, типа ограничения времени работы устройства. Android, к сожалению, этого делать не умеет, а вот в Apple можно много всего настроить, даже не используя специальных программ, но вот интернет фильтровать, например, он не умеет.

В общем, я очень рекомендую работать с настройками того софта, которым вы пользуетесь.

Что контролировать, а что нет?

Я против чтения детских переписок – все-таки есть безопасность, а есть приватность, и они должны быть в равновесии, но это вопрос, на который каждый родитель отвечает самостоятельно.

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, причем если коллеги из «Лиза Алерт» рекомендуют это делать раз в месяц, я считаю, что это надо делать чаще, потому что дети совершают, не задумываясь, глупости в интернете круглосуточно! Если у ребенка много «друзей», с которыми нет контакта в реальной жизни, это повод, чтобы бить тревогу.

Используйте для таких проверок специальное программное обеспечение – например, наша программа Safe Kids умеет говорить родителям про новые знакомства (и особо подчеркнет, если разница в возрасте с новым «другом» большая, или у них нет общих знакомых), про группы, причем не про все – ребенок добавился в 150 групп, и вам пришло 150 уведомлений, – а если он добавился в группу, относящуюся к насилию, алкоголю, наркотикам, самоубийствам и другим опасным темам. Программа позволит вам проверять все это, даже если у ребенка закрытый аккаунт, если вы знаете его логин и пароль.

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.

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.