РОДИТЕЛЯМ ОБ ИНТЕРНЕТ-УГРОЗАХ

1. Одна из новейших Интернет - угроз – так называемый «киберсуицид» или *согласованные самоубийства*. По Интернету подростки и молодые люди договариваются о совместном самоубийстве. В Сети довольно много сайтов, где подробно описаны и проиллюстрированы способы свести счеты с жизнью. Подростки, которых интересует подобный опыт, говорят о том, что вместе уйти из жизни проще, чем поодиночке, в сети находят поддержку своим суицидальным наклонностям, вступая в контакт с единомышленниками, которые, как и они сами, думают о самоубийстве.

2. В социальных сетях через программы мгновенного обмена сообщений ребенок может стать *жертвой педофилов*. Преступники представляются сверстниками и выманивают у детей адрес или маршрут следования из школы.

3. Пострадать ребенок может и от *поведения других детей.* В России набирает обороты киберхулиганство: подростки снимают на видео сцены унижения или избиения сверстника и выкладывают этот ролик в Интернет. Так об этом факте узнают десятки, а то и сотни ровесников жертвы, и начинается его настоящая травля.

4. Еще одной из проблем, подстерегающих в сети Интернет, является *пропаганда жестокости, экстремизма и нетерпимости*. Когда информация экстремистского содержания попадает в руки взрослого, знающего разницу между добром и злом, в руки полностью сформировавшейся личности это, в большинстве случаев, не принесет серьезного вреда, и совершенно другое дело, когда сайты экстремистского, националистического содержания попадают на глаза детей, личность которых еще только проходит этап становления.

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 – группы смерти;

44% боятся общения с незнакомыми;

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

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. 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.

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.

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.

Незнакомцы

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.

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.

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 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 «ВКонтакте» 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.

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.

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».

История с «синими китами» во многом тоже про, во-первых, общение 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.

КАК ОБЕЗОПАСИТЬ ДЕТЕЙ

Способы защиты детей от вредной информации в Интернете:

1. Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми.

По возможности находите совместные дела, интересуйтесь предпочтениями вашего ребенка.

2. Научите детей доверять интуиции.

3. Если их в интернете что-либо беспокоит, им следует сообщить об этом вам.

4. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире

5. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы — музыки, компьютерных игр и других программ — является кражей.

7. Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

8. Скажите детям, что не все, что они читают или видят в Интернете, — правда.

9. Приучите их спрашивать вас, если они не уверены.

10. **Используйте лицензионное программное обеспечение (оперативная система, антивирусная программа)**

11. Используйте специальные интернет-фильтры (Интернет Цензор - http://icensor.ru/soft/ - бесплатная программа). В основе программы лежит технология «белых списков», гарантирующая 100% защиту от опасных и нежелательных материалов.