10 СОВЕТОВ РОДИТЕЛЯМ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

1. **Стройте открытые и доверительные отношения с ребенком.** Обсуждайте устройства и проводимое время в Интернете спокойно, чтобы ребенок всегда чувствовал и знал, что он может к вам обратиться, если попадет в неприятную ситуацию.

2. **Больше времени проводите вместе с ребенком в реальной жизни.** Отвлекайте его от Интернета и отвлекайтесь сами. Играйте с ребенком в активные игры, читайте, смотрите фильмы и общайтесь.

3. **Закладывайте полезные привычки** и помогайте ребенку развивать социальные и эмоциональные навыки, такие как уважение к другим, сопереживание, критическое мышление и ответственное поведение.

4. **Используйте устройства в хорошо просматриваемом месте в доме.** Это поможет следить за тем, с кем общается ваш ребенок в сети, когда пользуется телефоном, планшетом, телевизором, игровой приставкой и другими подключенными к Интернету устройствами.

5. **Установите ограничения**, чтобы время, проводимое перед экраном электронного устройства, было в балансе со временем в реальном мире. Грамотно сформировать ожидания по части того, где и когда допустимо пользоваться электронными устройствами, можно с помощью распорядка «электронного дня» всей семьи. Введите запрет на использование ребенком компьютера, планшета и смартфонов в ночное время. Учите ребенка, подавая пример. Чтобы привить ребенку правила цифровой безопасности, их следует понимать и соблюдать самим. Не лишним будет заключить семейное соглашение об использовании устройств и Интернета.

6. **Будьте в курсе того, какие приложения, игры и социальные сети использует ребенок. Убедитесь, что они соответствуют его возрасту.** Выставляйте в приложениях и играх ограничения на функции обмена сообщениями или чата в Интернете и передачи геолокации, так как это делает ребенка уязвимым для нежелательных контактов и раскрывает его местоположение.

7. **Проверьте настройки конфиденциальности** в играх и приложениях, которые использует ваш ребенок. Убедитесь, что в них выставлены наиболее строгие критерии. Ограничьте список лиц, которые могут посылать ребенку сообщения и попросите его советоваться с вами, прежде чем принимать приглашения в друзья от других пользователей.

8. **Используйте функции родительского контроля.** Это позволяет фильтровать опасные материалы, следить за тем, как ребенок использует подключенные к Интернету электронные устройства, ограничивать или блокировать на них доступ к сети и другие функции, например, камеру или покупки в приложениях.

9. **Обращайте внимание на настроение и поведение ребенка.** Смена привычек может свидетельствовать о том, что он попал в неприятную ситуацию. Важно, чтобы ребенок знал, что в любой ситуации, ему следует довериться и рассказать об этом вам.

10. **Обеспечьте безопасность персональной информации своей семьи.** Следите за тем, чтобы ребенок не размещал в Интернете информацию о себе и своей семье: личные или семейные фотографии, свою фамилию, данные о месте жительства, пребывания, учебы, работы родителей, маршрутах своего передвижения, реальных имен своих друзей или людей из круга общения родителей, данные свидетельства о рождении, паспорта или иных документов, номера телефонов, банковских карт, логины, пароли и тому подобную информацию. 50% детей указывают в Интернете свой настоящий возраст и делятся настоящими фотографиями, 10% пишут свой мобильный номер, а 9% указывают геолокацию (по данным Лаборатории Касперского).

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ВЕРБОВКА И ОТБОР ДЕТЕЙ В ДЕСТРУКТИВНЫЕ СООБЩЕСТВА В СОЦИАЛЬНЫХ СЕТЯХ

Реальность опасности для детей в сети

Социальные сети являются самым эффективным и широким по охвату инструментом, с помощью которого злоумышленники могут вербовать пользователей в разные преступные организации.

К опасным сообществам в социальных сетях относятся:

- Группы, пропагандирующие экстремистскую и нацистскую идеологию: террористические группировки, (в том числе движение «Колумбайн», признанное террористическим движением на основании решения Верховного суда РФ), шутеры, нацистские, неонацистские движения и др.
- Группы и каналы, пропагандирующие опасные увлечения: зацепинг, опасные квесты, группы с пропагандой наркотиков, трэш-стримеры, шок-контент и др.
- Группы, пропагандирующие причинение вреда себе или окружающим: селфхарм (буквально переводится как «вред себе»), пиплхейт (движение, пропагандирующее ненависть к людям), депрессивно-суицидальные группы («синий кит» и аналогичные), анорексию и др.
- Группы, пропагандирующие нетрадиционные духовно-нравственные ценности: оккультизм, сатанизм, чайлдфри, феминизм, нетрадиционные сексуальные отношения, смену пола, гендерную идентичность, зоофилию и пр.
- Аниме-сообщества. В отличие от традиционной японской культуры аниме, современные аниме могут быть очень опасны, поскольку нередко пропагандируют насилие, сексуальные извращения, каннибализм, убийства и самоубийства. По данным исследователей через «кровавое аниме» популяризуется даже скулшутинг. Аниме-продукция также является лидером по депрессивно-суицидальному контенту. По данным опроса экспертов из числа сотрудников подразделений по делам несовершеннолетних органов внутренних дел, многие несовершеннолетние, имевшие опыт суицидального поведения, увлекались данной субкультурой.

Ключевой вопрос

Как гарантировать безопасность ребёнка в опасной среде?

Внимание!

Ребенок должен знать об опасностях общения с незнакомцами в Интернете, а также доверять своим родителям.

Важно, чтобы в случае опасности, появления странных друзей или попытки втянуть ребенка в сомнительную деятельность, он, в первую очередь, обращался за помощью к родителям.

82% детей получают заявки в друзья от незнакомых людей, 29% детей получают заявки от незнакомых взрослых (по данным Лаборатории Касперского)

Деструктивные сообщества могут:

1. **Нанести непоправимый вред психическому и физическому здоровью ребенка. Могут быть опасны для жизни ребенка.**
2. **Сформировать нетрадиционные духовно-нравственные ценности, опасные взгляды и убеждения, основанные на насилии и мизантропии.**
3. **Заставить ребенка причинить вред себе или окружающим.**

В Интернете действует большое количество преступников, чьей целью является вовлечение все новых и новых пользователей в деятельность таких опасных сообществ. Такие лица называются «вербовщиками».

Чаще всего вербовка начинается с личного и очень навязчивого общения. Вербовщики пытаются завладеть всем вниманием и временем пользователя. Один из основных способов вербовки – маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами. После этого происходит отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообществ. Особенностями таких групп может быть персональный доступ к ним только членам сообщества (особенно если общение происходит через мессенджеры). То есть родители или иное лицо не сможет попасть в группу, используя свои телефон или компьютер. После этого пользователи приступают к выполнению заданий в реальном мире.

Полезные советы

1. Спрашивайте или аккуратно проверяйте, с кем ведёт переписку ребёнок в личных сообщениях.
2. Обращайте внимание на поведение и новые интересы ребёнка: аниме, депрессивная литература, специализированные книги об оружии и стрельбе.
3. Замечайте изменения круга общения ребёнка, спрашивайте о его новых друзьях.
4. Обращайте внимание, если ребенок в реальной жизни выполняет задания, полученные в Интернете, так называемые, челленджи. Они могут содержать опасные для здоровья действия, например: сделать фото в экстремальных условиях или пробраться на закрытую территорию. Такие челленджи начинаются с простых и безобидных действий, а заканчиваются потенциальной угрозой для здоровья и жизни ребенка.
5. В случае обнаружения нежелательных контактов в соцсетях ребенка и потенциальной угрозе, необходимо сообщать в полицию, прикладывая все имеющиеся доказательства: ссылки на группы и сообщества, скриншоты переписки, ссылки на аккаунты преступников и т.д.

6. По возможности обеспечьте регистрацию ребенка в социальных сетях со своего компьютера или номера телефона, что позволит отслеживать его действия в Интернете. Следует помнить, что ребенок, вовлеченный в деструктивные сообщества, заводит второй (третий) аккаунт в социальных сетях, который держит в тайне от родителей.
7. Не стесняйтесь читать сообщения и переписку своего ребенка. Это не является нарушением его прав, но есть непременное условие обеспечения его безопасности. Не забывайте регулярно проверять в компьютере несовершеннолетнего историю его запросов и поиска в Интернете. В настройках браузера находится вкладка «История» («Закладки», «Загрузки», «Журнал»), где можно найти страницы недавних посещений ребенка. Если вы обнаружили, что ребенок регулярно стирает историю поиска, то это может быть тревожным знаком, требующим особого внимания.
8. Необходимо помнить, что первым этапом вовлечения ребенка в деструктивные сообщества является его отдаление от родителей и близких людей, провоцирование конфликтов между ними, культивирование претензий, ненависти и агрессии к родным и друзьям. Поэтому не всегда вызывающее и агрессивное поведение ребенка по отношению родителям является искренним желанием и осознанным поведением несовершеннолетнего, а лишь результатом манипуляции его сознанием со стороны преступников. Поэтому очень важно не ссориться с ребенком и не конфликтовать, а пытаться всегда оставлять возможность для диалога, искать подлинную причину его поведения и устранить ее. Старайтесь постоянно поддерживать своего ребенка.
9. Постарайтесь сдерживать внешние проявления бурных реакций на агрессивное и неконструктивное поведение ребенка или содержимое его переписки. Пытайтесь говорить с ребенком спокойно, без негативных эмоций объяснить ему недопустимость его поведения или почему тот или иной контент может представлять угрозу. Ребенок должен знать об опасностях общения с незнакомцами в Интернете, а также доверять своим родителям. Важно, чтобы в случае опасности, появления странных друзей или попытки втянуть ребенка в сомнительную деятельность, он, в первую очередь, обращался за помощью к родителям.
10. Поддерживайте контакты с друзьями и одноклассниками ребенка, а также их родителям, информация от которых может быть весьма полезной для общего понимания интересов, сложностей и проблем ребенка, а также для принятия своевременных мер.

Личный пример

Интересуйтесь (с определенной регулярностью!), на какие группы и сообщества в соцсетях подписан ребёнок.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ НАЙТИРЕБЕНКА.РФ

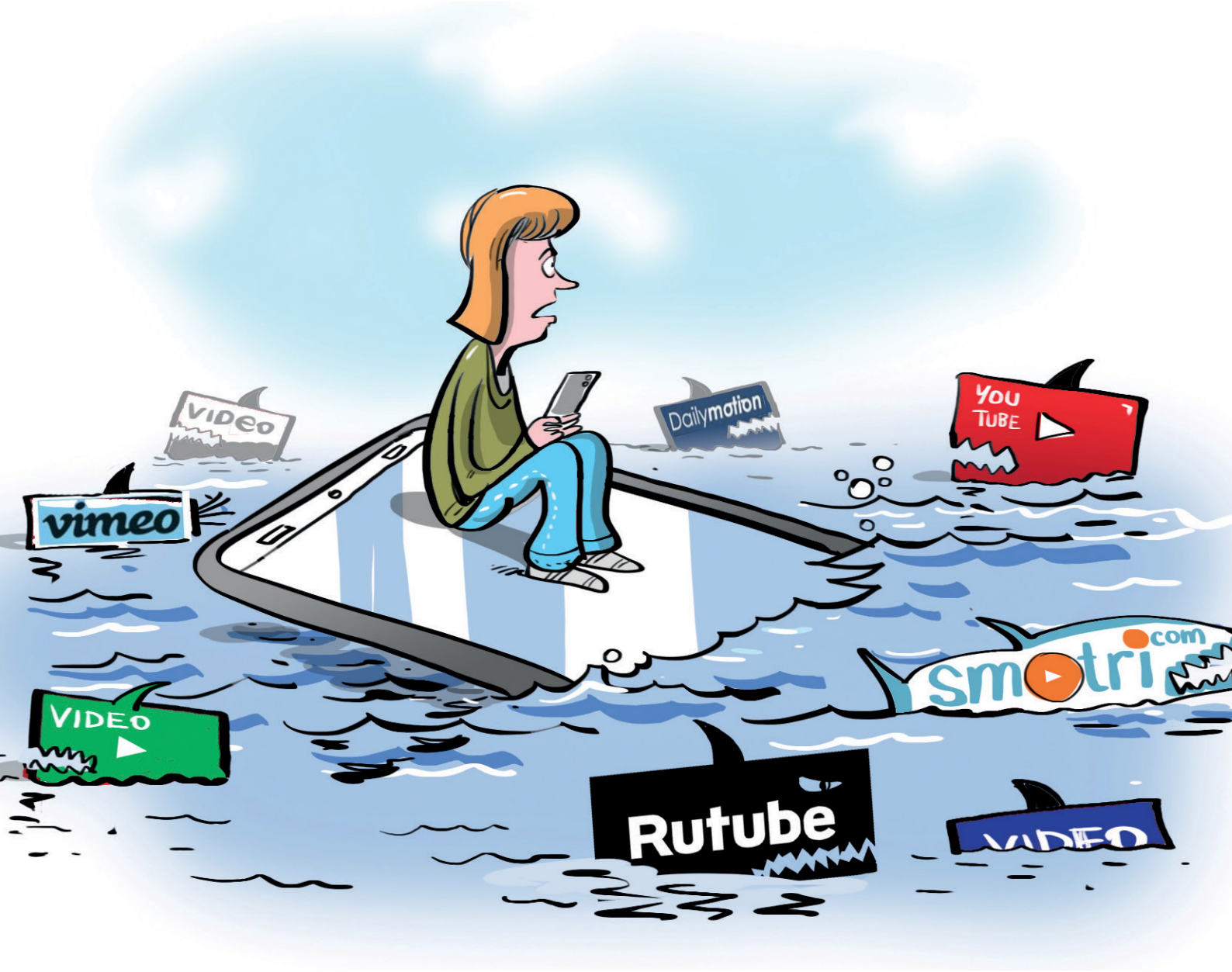
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ВИДЕОХОСТИНГИ

Видеохостинги – специальные сайты, где пользователи могут загружать и просматривать видео, делиться ими со своими друзьями. С помощью видеохостингов любой пользователь, в том числе ребенок или подросток, получает доступ к огромному количеству разнообразного контента. Создатели видео учитывают интересы детей и размещают такие вирусные видео, которые дети будут смотреть снова и снова. Это формирует у детей и подростков настоящую зависимость.

Среди миллионов видео, которые ежедневно загружаются на видеохостинги, присутствует большое количество опасного, деструктивного и неприемлемого для детей и подростков контента. Зачастую дети получают к этому контенту доступ, несмотря на возрастные ограничения и опасное содержание таких видео.



Чем опасны видеохостинги?

- На многих сайтах обмена видео **нет возможности ограничить круг лиц**, которые могут смотреть видео, загруженные пользователем.

- Как и в случае с онлайн-трансляциями, в записанных видео **подростки могут случайно выдать личную информацию**. Например, названия школы может хватить, чтобы злоумышленники могли вычислить место жительства ребенка.

- Функция комментирования видео дает пользователям **возможность писать неуместные и оскорбительные сообщения**.

- Модерация некоторых видеохостингов (**YouTube, Twitch) не удаляет видеозаписи противоправного, деструктивного или экстремистского характера**: пропаганду наркотиков, ЛГБТ, экстремизма, опасных для жизни увлечений и т.п.

- Рекомендательные алгоритмы видеохостингов **показывают пользователю деструктивные и противоправные видео**, даже если пользователь не интересуется этой тематикой.

- Опасные видеоматериалы **делают детей агрессивными** и повышают риск возникновения психических расстройств.

- Видеохостинги **формируют зависимость от просмотра видео**, «затягивают» настолько сильно, что ребенок теряет счет времени и не может отличить реальную жизнь от виртуальной.

Самый популярный видеохостинг в России и в мире – «YouTube». Именно он представляет наибольшую опасность для жизни, здоровья и психики детей. **Опасный контент на YouTube не удаляется и намеренно продвигается среди детей и подростов в России.**

В 2021 году американские исследователи обнаружили, что рекомендательные алгоритмы YouTube предлагают пользователям видеоролики, которые нарушают собственные правила онлайн-площадки. Согласно данным эксперимента, подобные материалы составили 71% от общего количества просмотренных участниками исследования видео.

На YouTube неоднократно были случаи, когда после просмотра мультиков и подростковых программ про спорт и разные увлечения, рекомендательный алгоритм выдавал детям контент откровенно фейкового и антироссийского содержания со сценами насилия и жестокости. Об этом многие родители детей сообщали в Лигу безопасного Интернета.

Видеохостинг является одним из мест, где кибербуллинг происходит чаще всего – о таких случаях заявили 79% детей, пользующихся YouTube. В России данная статистика сочетается с крайне высокой уверенностью родителей в том, что их дети не подвергаются кибербуллингу.

При просмотре некоторых роликов на YouTube дети имеют все шансы столкнуться с опасными материалами, стать агрессивными, поддаться суицидальным мыслям, оказаться завербованными в экстремистские организации или попасть под «зомбирование западной пропаганды».

Что должны сделать родители, чтобы обезопасить своего ребенка?

- **Будьте в курсе**, на кого подписан ваш ребенок в видеохостингах.
- **Знайте, какую информацию содержат видео**, которыми ваш ребенок обменивается со своими сверстниками.
- **Проверяйте любимые видео вашего ребенка** и каналы, на которые он подписан. Так вы сможете понять, какие видео ваш ребенок смотрит на портале.
- **Проверяйте, можно ли на этом видеохостинге отправлять жалобы** на неуместный, оскорбительный и опасный контент.
- **Узнайте, как работает раздел комментариев** на этом сервисе. Так вы сможете понять, можно ли ограничить комментарии – проверять их перед публикацией или вовсе отключить.

Что родители должны обсудить со своими детьми?

- **Обязательно объясните ребенку,** какую информацию ему можно, а какую нельзя рассказывать и показывать в своих видео. Объясните, почему некоторые вещи нельзя публиковать на всеобщее обозрение.
- **Расскажите ребенку о необходимости настройки** и защиты конфиденциальности его аккаунта. Личные видео, не предназначенные для чужих глаз, лучше вовсе не публиковать.
- **Расскажите ребенку, что абсолютно всё,** что он публикует, в том числе и видео, так или иначе **попадает в публичный доступ,** где его могут увидеть не только друзья, но и вся школа, все родственники, друзья родственников, и даже родители одноклассников. Если ребенок сомневается, хочет ли он, чтобы все эти люди увидели его видео, то лучше его не публиковать.
- **Покажите и объясните ребенку, как на данном видеохостинге отправить жалобу в службу поддержки** на неприемлемые видео и оскорбительные комментарии.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

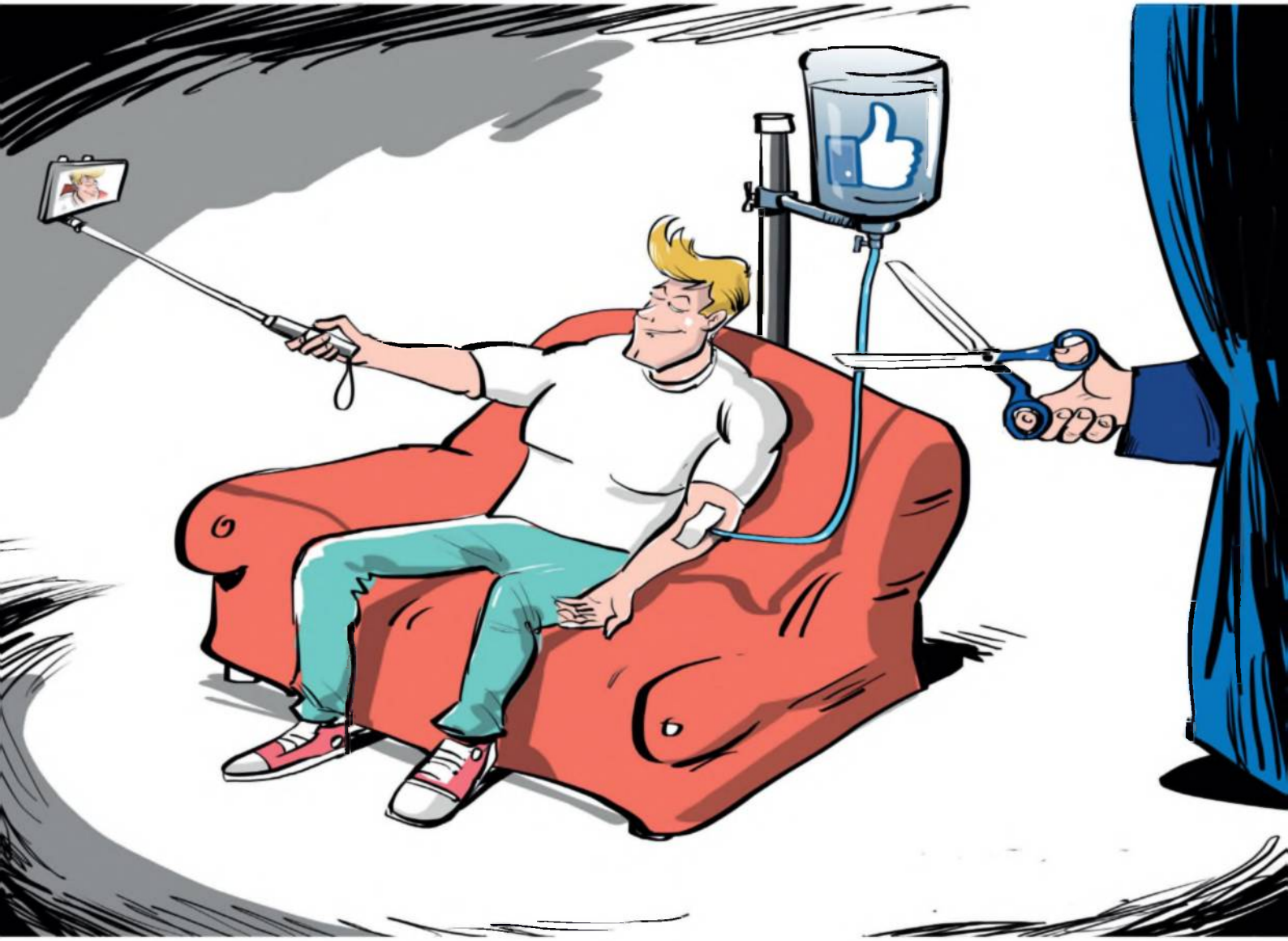
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ВОЗДЕЙСТВИЕ ВИРТУАЛЬНОЙ ЖИЗНИ: ИЛЛЮЗИИ СОЦСЕТЕЙ

«Мультиреальность» как ценность и проблема

Современные дети и взрослые существуют одновременно в двух реальностях – реальной и виртуальной. Перенос частной жизни в виртуальное пространство приводит к тому, что цифровой мир не просто дополняет реальную жизнь, а становится ее полноценной частью. Это называют «мультиреальностью».



Ключевой вопрос

Какие существуют проблемы в «мультиреальности», как их минимизировать?

Внимание!

Виртуальная жизнь может целиком заменить реальную, люди пытаются переносить шаблоны и модели подведения из виртуального мира в реальный.

Признаки чрезмерного погружения человека в виртуальный мир:

- Если во время разговора или дискуссии в реальной жизни человек не может отстоять свою точку зрения, он попытается «забанить» (заблокировать) собеседника так, как сделал бы это в соцсети – уйти от разговора, перестать отвечать, игнорировать собеседника.

- Многие дети сегодня учатся пользоваться смартфонами и Интернетом еще до того, как научатся писать и читать. С самого раннего возраста они начинают поглощать огромное количество не самого качественного развлекательного контента. Каждый четвертый ребенок в возрасте от 0 до 12 месяцев использует Интернет. Более половины детей в возрасте до 3 лет используют Интернет каждый день. Это приводит к изменению умственного развития, ухудшению памяти и социальных навыков.

- Происходящее в социальных сетях представляет для детей больший интерес, чем собственные впечатлений в реальной жизни. Всё интересное, что происходит в жизни, необходимо фотографировать и выкладывать в соцсети. Например, достопримечательность на отдыхе необходимо сфотографировать и «запостить» в соцсети. Публикация для пользователя гораздо важнее, чем сама достопримечательность.

Преодолевайте иллюзии! Соцсети постоянно создают иллюзии, которым подвержено большинство пользователей. Эти иллюзии часто переносятся и в реальный мир:

Иллюзия недолговечности – большинство пользователей уверено, что все, что они выложили в сеть, будет жить несколько часов или дней. Но старые публикации никуда не пропадают, даже если их удалить. Они хранятся и формируют обширный цифровой след об авторе, их можно восстановить и использовать для шантажа или компромата. По данным Лаборатории Касперского, 22% детей выкладывали в Интернет информацию, о размещении которой в последствии жалели.

Иллюзия доброжелательности – авторы публикаций в социальных сетях ожидают видеть похвалу и одобрение в свой адрес. Несогласных или возмущенных людей можно просто «забанить», так они не смогут комментировать и даже просматривать публикации пользователя. Чем больше пользователь находится в плену этой иллюзии, тем меньше он готов к нападениям недоброжелателей и «троллей» в соцсети и тем сильнее будет травмирован в случае травли или агрессии. 30% детей, по данным Лаборатории Касперского, близко знакомы с травлей в социальных сетях – они либо сами были ей подвержены, либо становились очевидцами подобного.

Иллюзия ценности – многие пользователи уверены, что все, что они пишут и публикуют – нужно и полезно для остальных пользователей. В какой-то степени, это действительно так. Только вся эта информация нужна и полезна не для других пользователей, а для самой соцсети и ее разработчиков. Ведь чем больше информации о себе вы опубликуете, тем более точный портрет смогут собрать о вас алгоритмы соцсетей и тем более дорогую рекламу смогут вам показывать.

Полезные советы:

- **Не переносите поведение из социальных сетей в реальный мир!** Общение с собеседником лично совершенно не похоже на общение в чате.
- **Внимательно относитесь к тому, что публикуете!** Если вы не готовы столкнуться с критикой – лучше не публиковать. В Интернете много недоброжелателей.
- **Помните,** что любая информация в Интернете, фото, видео или сообщения могут быть восстановлены даже спустя много лет после удаления.
- **Общайтесь с людьми в реальности,** а не в социальных сетях. Чем меньше вы пользуетесь смартфоном, тем лучше!

Личный пример

Отключайте смартфон хотя бы на несколько часов в день. Цените время, которое вы проводите вместе с семьей, не тратьте его на социальные сети и приложения.

По данным исследования ВЦИОМ *(Всероссийский центр изучения общественного мнения)* **почти каждый третий (29%) пользователь соцсетей и мессенджеров в России тратит на них более 3 часов в день, а среди молодежи 18-24 лет эта цифра достигает 72%.**

По данным Лаборатории Касперского:

22% детей жалели
о том, что выкладывали в Интернет.

30% детей сталкивались с травлей в соцсетях –
подвергались ей либо видели травлю в отношении других.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

КАК ГАРАНТИРОВАТЬ СВОЮ БЕЗОПАСНОСТЬ В СЕТИ

Сложное слово, простые правила

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Ваш цифровой след хорошо виден! О каждом пользователе Интернета ежедневно собирается и хранится огромное количество информации. В основном ее собирают социальные сети и мессенджеры. Делается это для того, чтобы как можно точнее идентифицировать каждого пользователя и показывать ему наиболее актуальную рекламу. Чем точнее реклама попадает в интересы и увлечения пользователя, тем больше шансов, что он поддастся на нее, купит товар или приобретет услугу. Однако вся эта информация может попасть в руки к мошенникам. По данным ВЦИОМ, 57% получают звонки от телефонных мошенников, 19% получают от них сообщения, а 9% россиян потеряли деньги в результате действий мошенников.

Ключевой вопрос: Как обеспечить кибербезопасность?

Внимание!

Мошенники могут испо льзовать ваши данные самыми разными способами:

- Продать их другим мошенникам;
- Втереться в доверие и использовать для вымогательства денег;
- Использовать для шантажа;
- Использовать для травли.

Полезные советы

1. **Следите за галочками** (разрешениями), которые ставите (даёте сайтам и приложениям). Иногда кнопка «Ок», появившаяся на экране, означает полный доступ к вашему микрофону, камере или телефонной книге. Таким же образом, вы можете неосторожно оформить подписку на ненужную вам услугу или установить ненужные, а иногда и опасные программы на компьютер. Будьте бдительны!
2. **Старайтесь не пользоваться бесплатными сервисами.** Большинство бесплатных сервисов и приложений, включая мессенджеры и VPN-плагины, могут предоставлять свои услуги на бесплатной основе. Если программа доступна бесплатно, следует задуматься, чем же зарабатывают ее разработчики. Как правило – это персональные данные пользователей программы, которые она ежедневно записывает и передает разработчикам. Те же, в свою очередь, продают их сторонним организациям.
3. **Помните,** что все ваши публикации в Интернете не только публичны, но и хранятся вечно. Помните! Любая приватность может быть нарушена, публикации могут стать доступны в случае утечки.
4. **Не публикуйте и не отправляйте материалы интимного характера.** Любая информация, которую вы выкладываете в Интернет, может стать поводом для шантажа, провокации, а в будущем может даже принести проблемы в карьере. Материалы интимного характера, даже в переписках, не удаляются из Интернета и могут быть использованы преступниками для изготовления порнографических материалов с целью последующей продажи или фальсификации компромата. Никогда не отправляйте фото и видео интимного характера даже самым близким людям, поскольку всегда существует вероятность утечки информации из-за неосторожности, взлома почты или аккаунта.
5. **На незнакомые сайты лучше даже не заходить.** Некоторые сайты способны самостоятельно устанавливать вредоносные программы и вирусы. Для этого даже не нужно ничего скачивать, достаточно просто зайти на сайт. То же относится к письмам и сообщениям, которые приходят из незнакомых источников.
6. **Ненадежные и сомнительные письма лучше не открывать** и уж тем более нельзя скачивать файлы, пришедшие от неизвестного отправителя в письмах или мессенджерах. Это относится даже к текстовым файлам. Например, файлы формата .pdf, в котором распространяется большинство документов, вполне способны распространять вирусы среди скачавших пользователей.

Личный пример

Не публикуйте в соцсетях лишнюю информацию о себе. Абсолютно вся информация, включая ваши фото, адреса, увлечения, имена домашних животных и многое другое, могут быть использованы мошенниками для установления личности, создания подробной картины о вас, как о пользователе, и подбора персональных мошеннических схем.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ НАЙТИРЕБЕНКА.РФ

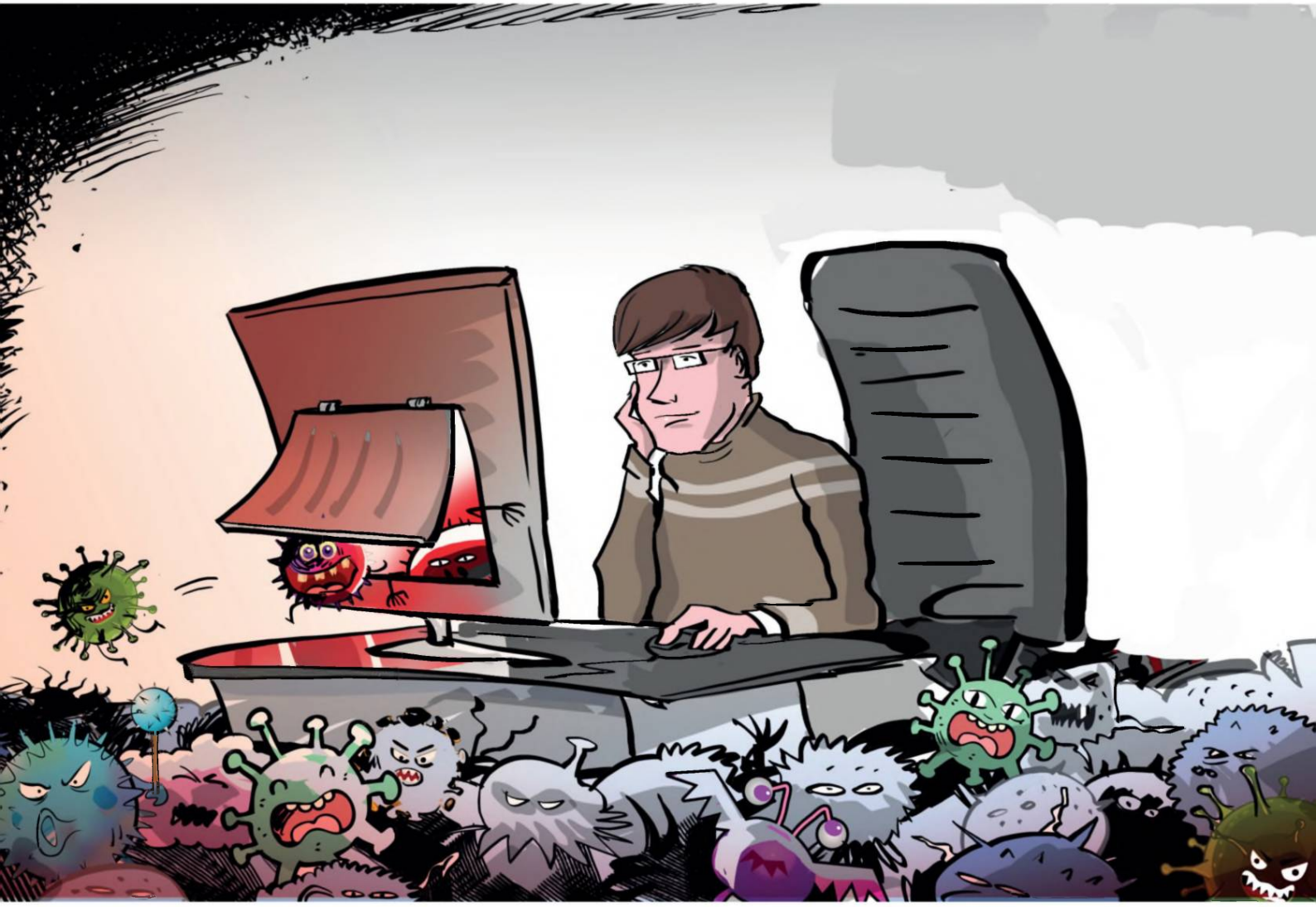
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

КИБЕРУГРОЗЫ: ЗНАНИЕ О ФАКТОРАХ ОПАСНОСТИ – ВАША БЕЗОПАСНОСТЬ!

Ключ в виртуальный мир

Современный смартфон – полноценный персональный компьютер. Он обладает всеми теми же функциями, что и домашний компьютер или ноутбук, а в чем-то даже их превосходит. В отличие от домашнего компьютера смартфон имеет постоянный доступ в Интернет, он работает 24 часа в сутки, имеет продвинутую камеру и микрофон, а также датчики движений, что позволяет ему круглосуточно записывать всю информацию о своем пользователе. Так, смартфон является нашим ключом в виртуальную реальность.



Ключевой вопрос

Как сделать свой смартфон безопасным?

Источники проблемы

- **Огромное количество навязчивой рекламы** – сайты, приложения, соцсети и игры – все это содержит огромное количество рекламы, на которой зарабатывают их разработчики. По данным Всероссийского центра изучения общественного мнения 29% россиян получают спам ежедневно.
- **Информационный шум** – в цифровом мире множество неконтролируемых уведомлений, которые приходят на телефон практически ежеминутно. Большинство пользователей не хотят тратить время на их отключение и удаление. А они содержат часто совсем ненужные рекламные предложения, приманки и являются способом вымогательства денег пользователя.
- **Установка нежелательного и вредоносного программного обеспечения** – при переходе по новой ссылке, скачивании файлов, установке приложений (даже из проверенных источников!) существует вероятность установки вирусов, шпионских или рекламных программ. Опасность могут представлять даже приложения, скачанные из официальных магазинов смартфонов. По данным ВЦИОМ, лишь 16% родителей устанавливают на устройство их ребенка антивирус.
- **Утечка персональных данных владельца** – все, что содержится в смартфоне, начиная от логинов и паролей, заканчивая фотографиями, банковскими реквизитами и даже перепиской, может не только попасть в руки к мошенникам, но и стать достоянием общественности.

Внимание!

Чем активнее используется устройство, тем больше данных о своем владельце оно накапливает. К таким данным относятся не только ваши фото, видео, переписки, но и такие данные, как:

- история установки и использования приложений;
- история энергопотребления, то есть циклов и времени зарядки, интенсивности работы;
- история уведомлений и действий;
- история магазина приложений;
- история браузера;
- история перемещений по городу и многое другое.

Надо знать!

Вредоносные приложения на смартфонах пытаются заработать на пользователе – вытянуть деньги, внимание пользователя, показывая ему рекламу или перенаправляя на сайты, украсть персональные данные или профиль пользователя, передать мошенникам доступ к самому устройству.

Вредоносные приложения бывают разными:

- **Фальшивые приложения** – копия настоящих приложений, как правило, банковских или приложений мобильных операторов. Их задача – полностью замаскировавшись под настоящее приложение, украсть у пользователя данные от личного кабинета и получить доступ к мобильному или банковскому счету.
- **Приложения-вымогатели** – блокируют устройство и требуют перечисление денег за разблокировку.
- **Денежные «пиявки»** – программы со скрытой подпиской. Однажды купив подобную программу или совершив покупку с её помощью, можно обнаружить, что она оформила «полноценную» подписку и деньги теперь списываются регулярно. Как правило, всегда можно отказаться от «денежной пиявки» и отменить такую подписку. Следите за своими расходами в сети.

Информация к размышлению

Вредоносные программы можно разделить на две большие категории:

- **Вирусы** – вредоносные программы, которые напрямую вредят устройству, установленным программам. Распространяются по Интернету и заражают устройства.
- **Трояны** – маскируются под настоящие программы, а иногда даже могут выполнять некоторые полезные функции. Похищают данные пользователя, рассылают спам, создают трафик на сайты.

Как вирусы попадают на устройство?

- **Из зараженного электронного письма** или файла, приложенного к письму – нельзя открывать письма, пришедшие из неизвестных источников, а особенно скачивать и запускать файлы, прикрепленные к этим письмам. Вирусы могут распространяться даже через текстовые файлы, например в формате .pdf.
- **Через зараженный сайт** – многие сайты способны самостоятельно устанавливать на компьютеры вирусы. Для этого бывает достаточно просто открыть страницу. Это особенно актуально для нелегальных сайтов, например, с пиратским контентом.
- **Через установку неизвестных приложений** с неизвестного сайта – если вы скачиваете что-либо из Интернета, убедитесь, что источник надежен. Программы лучше скачивать с официальных сайтов разработчиков этих программ.

Как защитить себя от киберугроз:

- **Не открывайте письма и сообщения от незнакомых отправителей;**
- **Не скачивайте пиратский контент;**
- **Внимательно проверяйте адреса веб-сайтов**, которые вы посещаете;
- **Не устанавливайте на телефон или компьютер, приложение из непроверенного источника;**
- **Не давайте приложениям разрешения, которые не нужны им для работы** – приложению «калькулятор» не нужен доступ к микрофону смартфона;
- **Следите за своими расходами в сети** и за тем, какие подписки оформляют приложения;
- **В настройках телефона отключите уведомления** от приложений, которые вы не хотите получать;
- **Установите на компьютер и телефон антивирус;**
- **Храните на телефоне как можно меньше информации о себе.** Так вы защититесь от утечки данных;
- **Подключите на телефоне функцию защиты от спама**. На некоторых устройствах она доступна в настройках или ее можно подключить у мобильного оператора.

Личный пример

Не открывайте MMS и сообщения, присланные с незнакомых номеров!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

КЛИПОВОЕ МЫШЛЕНИЕ: ЦЕНА ДЛЯ ЛИЧНОСТИ

Небезопасные клипы

Клиповое мышление – тип мышления, заключающийся во фрагментарном восприятии информации. Люди с преобладающим клиповым мышлением склонны к восприятию информации отрывочно и порционно, небольшими кусками, при этом значительно страдает глубина понимания материала, а также критический подход к информации.

У современных подростков такой тип мышления преобладает. Его формированию активно способствует формат подачи информации в соцсетях, особенно короткие видео (в TikTok, YouTube).

Особенности клипового мышления:

- Фрагментарность;
- Яркость;
- Кратковременность;
- Нелогичность;
- Отрывочность;
- Разрозненность;
- Поддержание общения одновременно с несколькими собеседниками.

Ключевой вопрос: Как бороться с клиповым мышлением?

Внимание!

Основной причиной развития клипового мышления у детей и подростков является особенность преподнесения информации в Интернете. Информация в сети подается отрывочно, в виде коротких статей или видео. Ярким примером является чтение новостей «по заголовкам». В таком случае человек менее склонен сомневаться в информации и перепроверять ее.

Считается, что клиповое мышление преобладает у тех, кто большую часть свободного времени проводит в Интернете ввиду специфики подачи информации. В среднем, современные подростки в возрасте от 12 до 17 лет тратят на Интернет почти 6 часов в день (по данным Mediascope).

У современной молодежи по данным экспертов зафиксированы проблемы, связанные с чтением. При попытке прочитать и усвоить сложный текст, (например, инструкцию), многие подростки начинают испытывать резь в глазах и головную боль.

Что способствует формированию клипового мышления:

- Музыкальные клипы;
- Реклама на ТВ;
- Электронные СМИ;
- Мобильные средства связи;
- Социальные сети и мессенджеры, такие как TikTok, YouTube.

Развитие клипового мышления проводит к следующим проблемам:

- Внушаемость;
- Плохая обучаемость;
- Гиперактивность;
- Дефицит внимания;
- Предпочтение визуальных символов логике и углублению в текст;
- Неспособность к восприятию однородной информации (в т.ч. книжного текста);
- Снижение уровня грамотности у подростков и студентов;
- Вместо логических связей выстраиваются эмоциональные;
- Ослабляется или нивелируется чувство сопереживания, а также ответственности.

Полезные советы

- Контролируйте экранное время ребенка.
- Воспользуйтесь приложениями для тренировки памяти и внимания.

Личный пример

Организуйте «время без гаджетов» - по вечерам или по выходным дням, когда не только ребенок, но и вся семья сможет максимально отвлечься от телефонов, компьютера и Интернета.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru