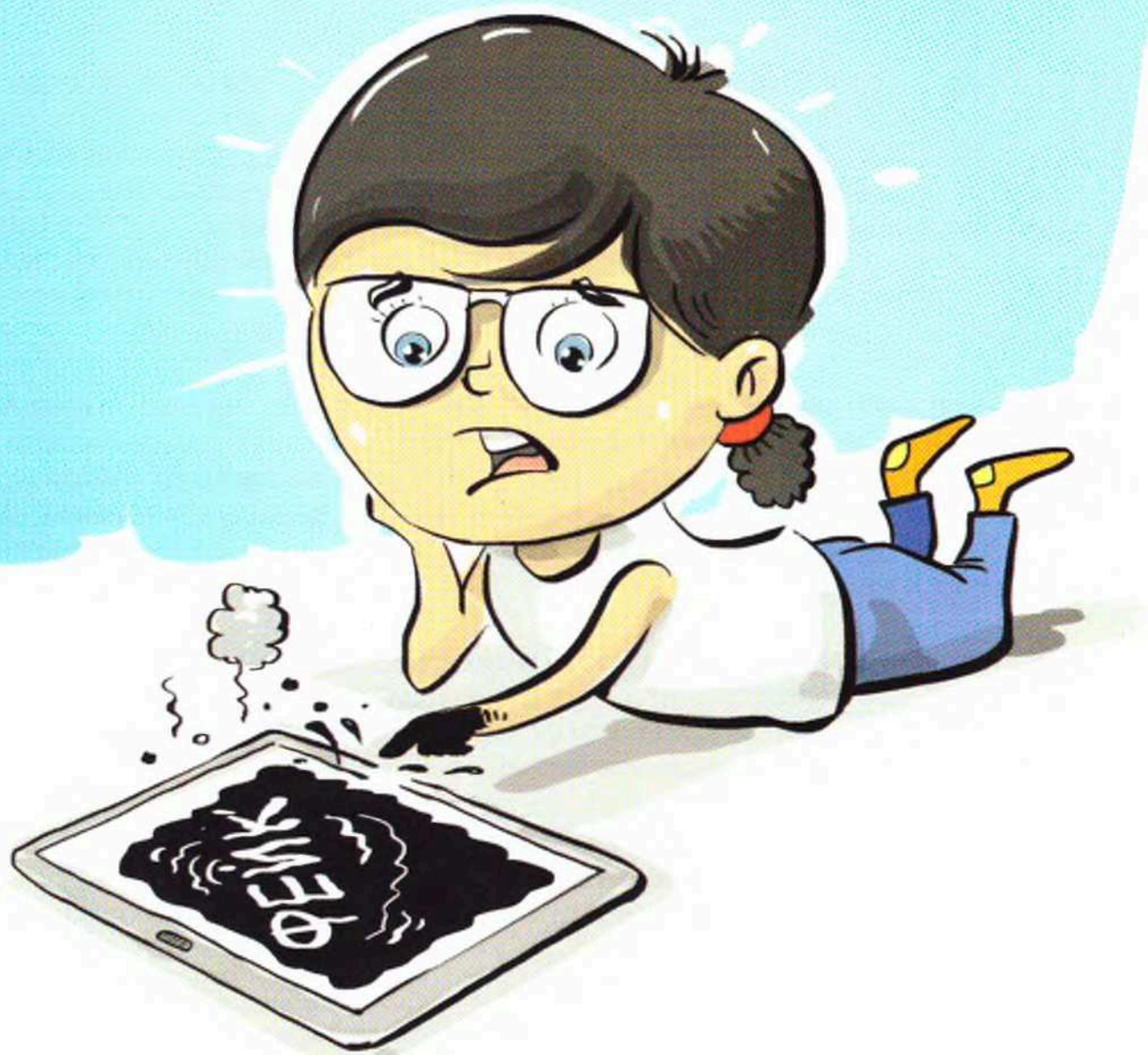
ФЕЙКИ В ИНТЕРНЕТЕ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт
ligainternet.ru

В Интернете есть много интересного, веселого и познавательного контента. Но необходимо подвергать сомнению все, что мы читаем и смотрим в Интернете.

> **ФЕЙК** – целенаправленно распространяемая ложная информация, которую специально создают, чтобы запутать, ввести в заблуждение или посеять панику среди людей.

Очень важно уметь проверять информацию, чтобы не попасться на провокацию и отличить фейк от настоящей новости. На что нужно обратить внимание:

1. **Оригинал всегда лучше любого пересказа.** Очень важно искать оригинальный источник новости, откуда она начала распространяться. Подумай, можешь ли ты доверять этому источнику? Если это «желтое СМИ» или сайт, специально собирающий громкие заголовки, то доверять такому источнику нельзя!

2. **Обрати внимание на текст.** У реальной новости всегда много свидетелей и участников, которые рассказывают о событиях своими словами. По этой причине СМИ напишут про одну и ту же новость по-разному. Фейки – наоборот, не отличаются разнообразием. Фейковые новости, даже опубликованные на разных сайтах, мало отличаются друг от друга, а иногда и вовсе могут быть написаны «под копирку». Фейк придуман одним источником, откуда его скопировали другие сайты.

3. **Настоящая новость никогда не пройдет мимо популярных, известных и авторитетных СМИ.** Крупные газеты, сайты и телеканалы беспокоятся о своей репутации, поэтому тщательно проверяют любую информацию. Фейки распространяют небольшие издания, которые могут не проверить информацию, а иногда и заведомо опубликовать ложные сведения.

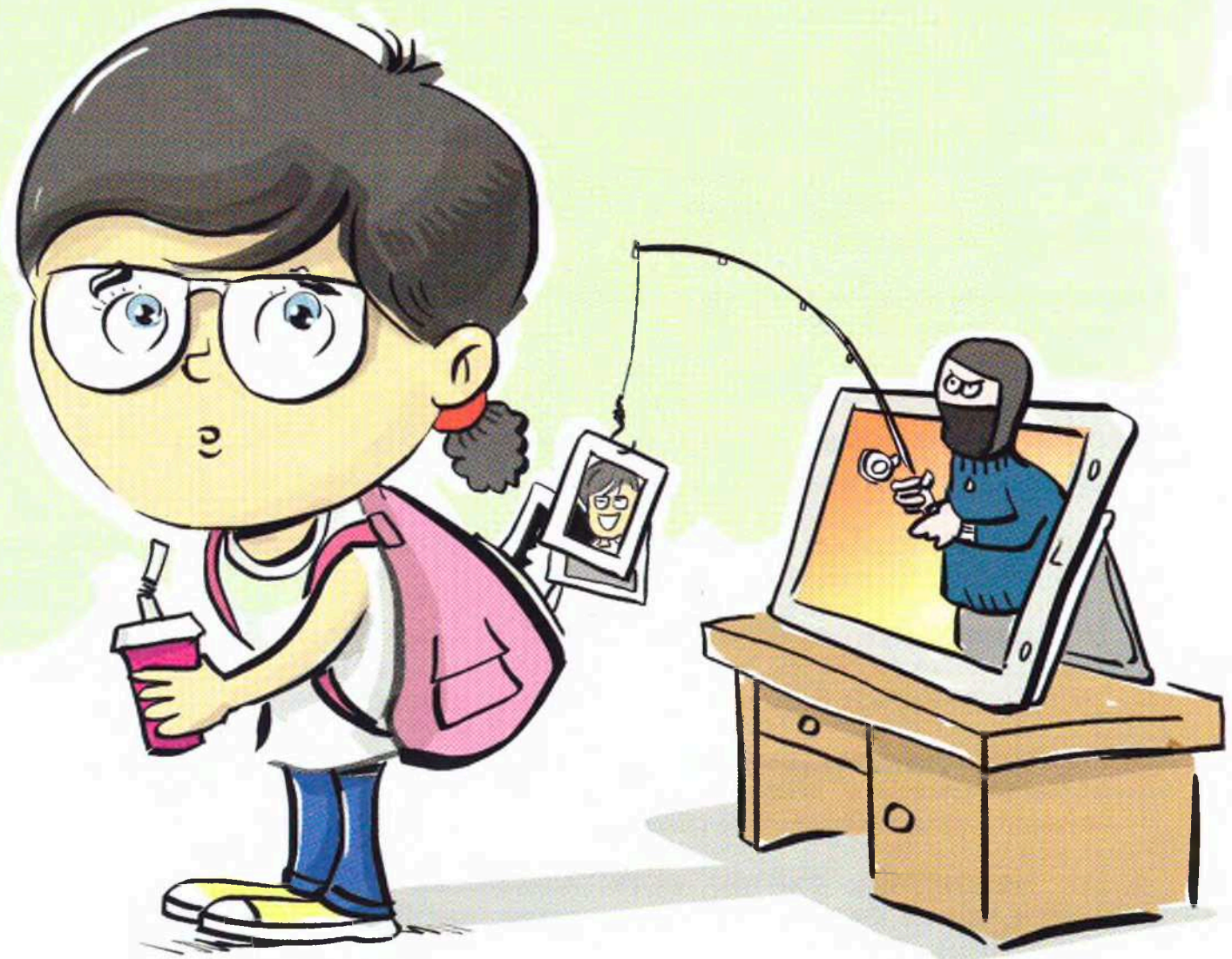
4. **Проверяй факты и цитаты из новости.** Не важно, кому принадлежит цитата, насколько это уважаемый и популярный человек. Недобросовестные СМИ могут подделать или вырвать из контекста любые слова для создания фейковой новости.

5. **Обращай внимание на основную суть новости**, а не на мелкие детали в ней. Обычно в фейках указывают очень много подробностей, которые создают иллюзию правдоподобности отвлекают внимание от основного смысла.

Полезный совет!

> Если ты нашел или получил недостоверную информацию, не пересылай ее друзьям и родным! Сначала дождись официального опровержения или подтверждения.

ЧТО ТАКОЕ ФИШИНГ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

ЧТО ТАКОЕ ФИШИНГ?

Фишинг с английского переводится как «рыбалка». Это самый распространенный вид мошенничества в Интернете. С помощью фишинга мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу какого-либо известного сайта: Интернет-магазина или соцсети.

Существует несколько подсказок, при помощи которых можно точно понять, настоящий это сайт или сайт-подделка:

1. **Проверяй адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают похожий на оригинал сайт. В адресной строке сайта может отличаться одна буква или символ.

2. **Обращай внимание на предупреждение браузера о небезопасном сайте.** Проверь, есть ли в адресной строке символ замка, если его нет, то это может быть признаком ненадежного сайта.

3. **Внимательно смотри на наполнение сайта.** Зачастую сайты мошенников, где продается товар, который ты ищешь, имеют ограниченный ассортимент товаров или вовсе могут быть одностраничными сайтами.

4. **Обращай внимание на правильность написания слов в текстах.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.

Базовые правила, которые помогут тебе уберечь себя от поддельных сайтов:

1. **Будь внимателен и тщательно обдумывай ситуацию.** Если у тебя возникают сомнения в надежности сайта – лучше им не пользоваться.

2. **Не игнорируй предупреждения!** Большинство браузеров имеют встроенные системы защиты, предупреждающие, что сайт, на который ты собираешься перейти, может быть небезопасен.

3. **Не вводи личные данные** (имя, фамилию, номер телефона, домашний адрес, номера и пароли банковских карт, свои фотографии и пр.) на незнакомых сайтах и не сообщай их посторонним.

4. **На некоторых сайтах есть возможность вместо регистрации зайти через свой профиль в социальной сети. Не пользуйся этой функцией.** Если преступники получат доступ к твоему профилю в соцсети, то они получат доступ и ко всем сайтам, куда ты через него заходил.

5. **Если ты стал жертвой мошенников, то следует незамедлительно обратиться за помощью к родителям.** Они помогут написать заявление в полицию. Чаще всего преступников удается поймать. Однако вернуть средства гораздо сложнее.

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.

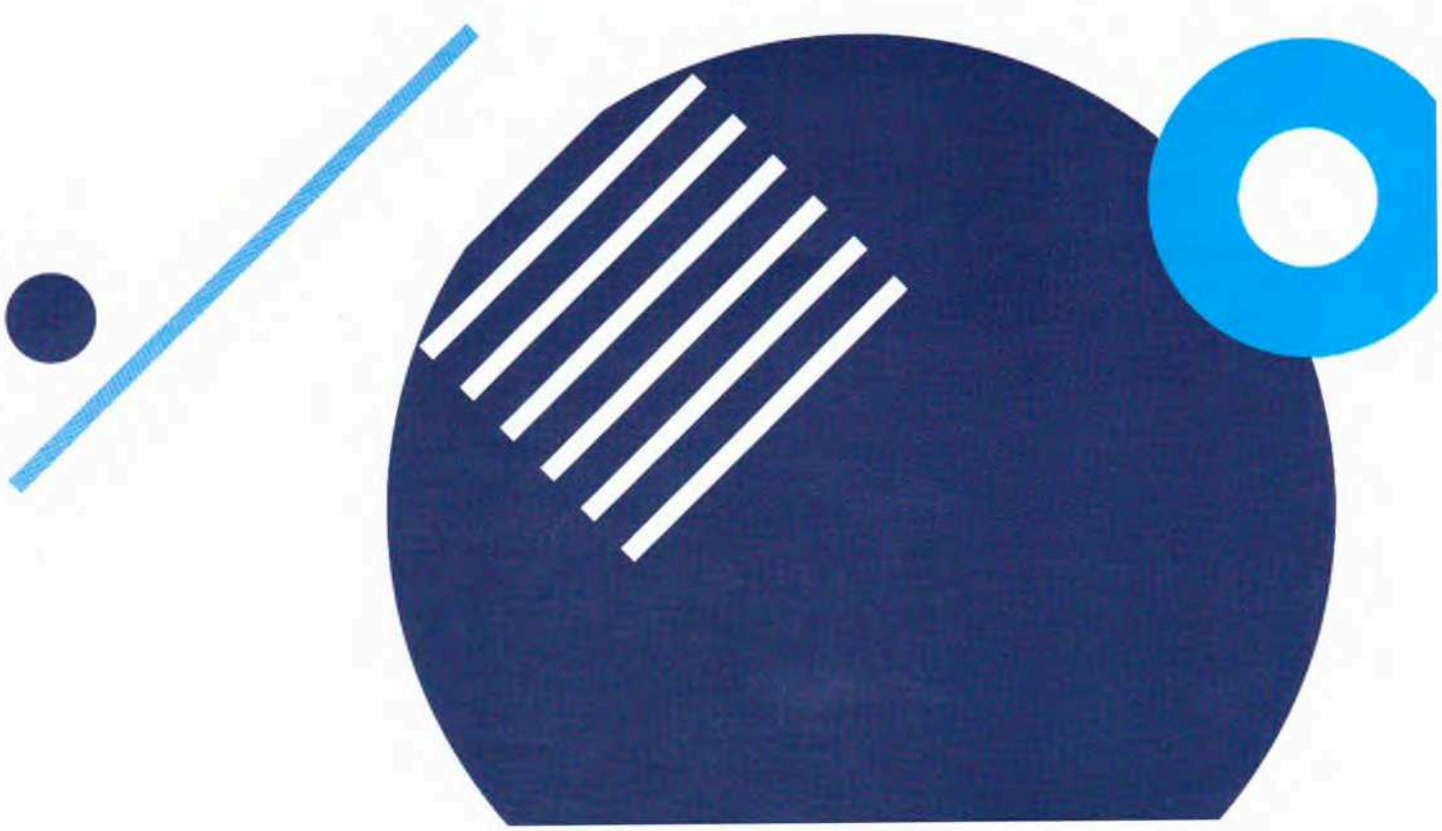
9. **Обращайте внимание на настроение и поведение ребенка.** Смена привычек может свидетельствовать о том, что он попал в неприятную ситуацию. Важно, чтобы ребенок знал, что в любой ситуации, ему следует довериться и рассказать об этом вам.

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



ОПАСНЫЕ СООБЩЕСТВА ЦИФРОВОГО МИРА: КАК ИЗБЕЖАТЬ СЕТЕВОЙ МАНИПУЛЯЦИИ

Деструктивные сообщества в сети – проблема реального мира

В Интернете существует большое количество опасных групп, сообществ, которые распространяют опасные для жизни, здоровья, нравственности человека идеологию, увлечения, движения, в том числе, вовлекают в экстремистскую деятельность и совершение иных преступлений. К таким группам относятся:

Суицидальные сообщества – группы, в которых публикуется контент, связанный, с тематикой самоубийств. Сообщества суицидальной направленности часто маскируются, тем не менее, их можно выявить по таким признакам: романтизация смерти и идей самоубийства; героизация людей, совершивших самоубийство и подражание им; практика «селфхарма» (причинения вреда самому себе); распространение деструктивно-суицидальной информации разного вида разнообразными способами. Например, часто пропагандируется такой контент через аниме, идеи анорексии идеологию ЛГБТ сообществ и др. 46% россиян убеждены, что Интернет значительно увеличил число самоубийств (по данным ВЦИОМ).

Аутодеструктивные сообщества – группы, распространяющие идею и практики причинения самому себе физического или психологического вреда. Например, группы «селфхарм». Часто бывают подготовительным этапом для вовлечения детей в суицидальные группы.

Сообщества школьных расстрелов (скулшутинг) – движение, ставшее популярным в США. Эти сообщества романтизируют и продвигают идею массовых убийств и, в особенности, массовых убийств среди детей и подростков в школах. К таким относится, например, движение «Колумбайн», признанное террористическим на основании решения Верховного суда Российской Федерации. По данным исследователей, скулшутинг пропагандируется даже через «кровавое аниме».

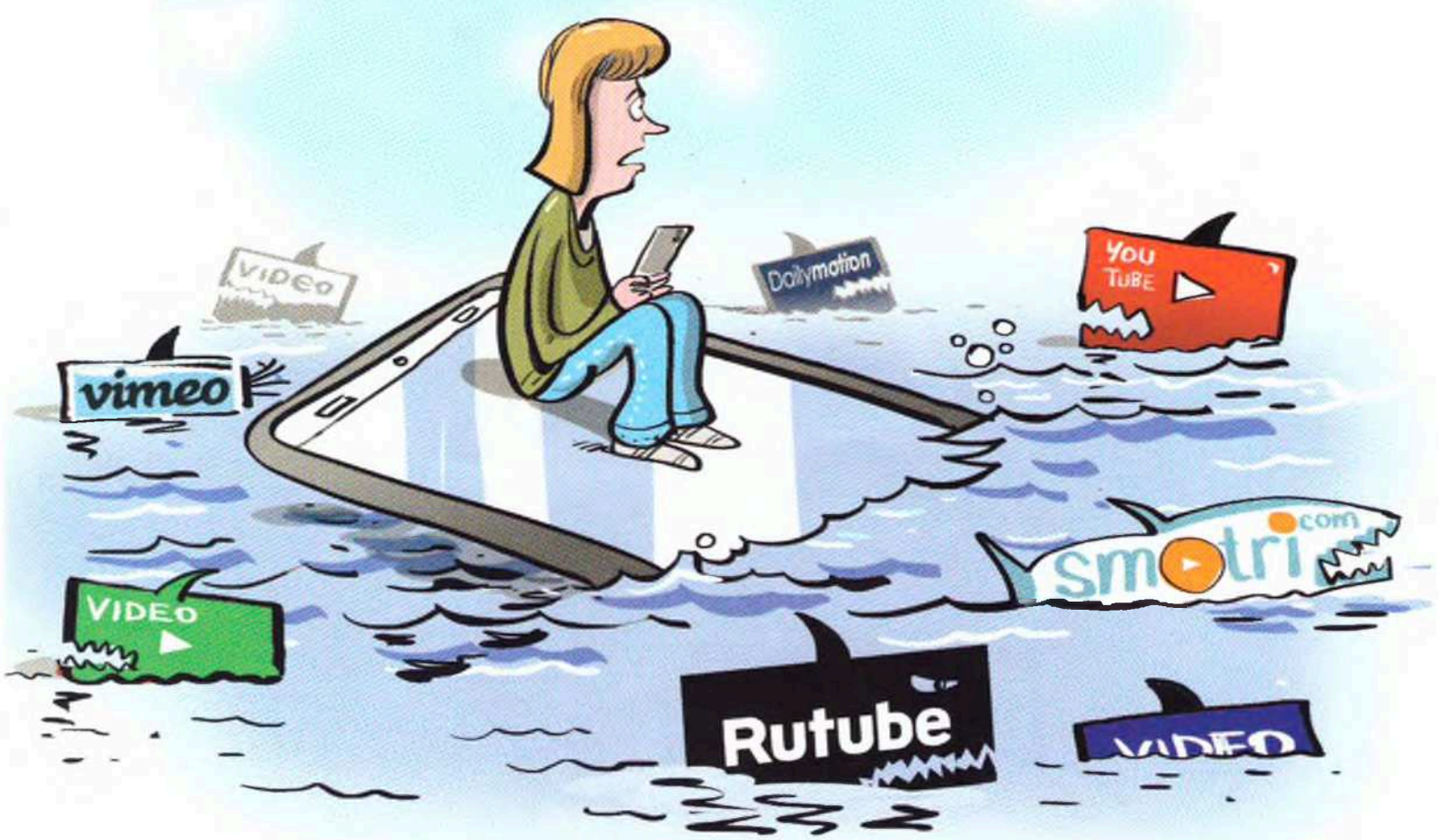
Сообщества по криминальной идеологии – продвигают идеалы из криминальной среды среди подростков. Наиболее известным примером является движение АУЕ (признано экстремистским и запрещено на территории Российской Федерации). В таких сообществах романтизируется не только криминальный, но и тюремный образ жизни и быт, а также криминальные герои книг, фильмов и сериалов.

Сообщества по пропаганде наркотиков – данные сообщества пропагандируют не только употребление наркотиков, романтизируя наркопотребление и образ жизни наркоманов, но и вовлекают своих членов в распространение наркотиков. Для этого пользователям массово рассылаются предложения о «подработке», где обещают высокую заработную плату. Бывают случаи и втягивания в эту деятельность детей и подростков. При этом несовершеннолетние, решившие подработать курьером, как правило, устанавливаются правоохранительными органами (в отличие от их работодателей-преступников) и получают реальные сроки лишения свободы.

Экстремистские сообщества – сообщества, занимающиеся публикацией и распространением экстремистского контента, пропагандирующие экстремистские идеи, а также привлекающие своих подписчиков к совершению преступлений на почве политики, расовой, национальной или религиозной ненависти.

Ключевой вопрос

Как помочь ребёнку не попасть в деструктивное сообщество?



Внимание!

На что обратить внимание...

- Наличие в сообществах, которые посещает ребенок, или в ленте новостей его аккау фотографий увечий: порезы, ссадины, кровь, травмы и т.п.
- Наличие фотографий в мрачных тонах, с депрессивным содержанием.
- Наличие в ленте цитат, обесценивающих жизнь или традиционные духовно-нравственные, в числе, семейные ценности; содержащих пренебрежительные/неуважительные высказыва по отношению к родителям, деторождению, служению Отечеству, исторической памяти нар России, ценности жизни человека, руководству страны и принимаемым решениям.
- Наличие в подписках у подростка или в ленте новостей его аккаунта сообществ, посвящен скулшутингу, а также лицам, которые совершали эти преступления.
- Интерес к «аниме» у ребенка или его друзей.
- Ребенок стал часто проводить время вне дома, скрывать информацию о том, где и с проводит время, при этом вы не знаете телефонов его друзей и их родителей, его успеваемо в школе упала.
- У ребенка появились денежные средства или дорогие вещи, происхождение которых вы знаете или он пользуется вещами, которые ему, якобы, дал временно поносить товарищ.

Последствия вовлечения в деструктивные движени

- **Снижение способности самостоятельно думать и принимать решения.**
- **Отказ от личной ответственности.**
- **Отрицание авторитетов, в том числе родителей, учителей и знакомых.**
- **Обесценивание норм морали и общечеловеческих ценностей.**
- **Выраженная симпатия к антигероям, антидвижениям.**
- **Выраженное стремление к разрушению и деструктиву.**
- **Снижение успеваемости в школе.**
- **Неуважение и травля учителей.**
- **Нарушение коммуникации и конфликты со сверстниками.**
- **Формирование школьных банд или радикальных группировок.**
- **Политизация детей и подростков.**
- **Рост преступлений среди детей и подростков.**
- **Рост наркомании среди подростков.**
- **Попытки самоубийства и причинения себе вреда.**

Как вовлекают в опасные сообщества?

Для вербовки и привлечения новых людей в движение вербовщ используют своеобразную «Воронку вовлечения».

Как это работает?

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

Это надо знать!

1. **Постоянные флешмобы могут быть опасны** – это регулярные задачи, например: облейся холодной водой, напиши пост и поставь правильный хештег, опубликуй свои фото в конкретных условиях и т.п. Такие активности «дрессируют» пользователей на бездумные массовые действия.
2. **Массовые тесты, квесты, задания** – псевдотесты на IQ, творческие способности, тип личности и т.п. Они не несут никакой пользы и не могут определить ничего из вышеперечисленного, но подталкивают пользователей к ненужной им активности.
3. **Общественные и явно политические задания** могут выражаться в требовании у ребенка поставить на аватар радужный (ЛГБТ) флаг, опубликовать пост с поддержкой или осуждением какого-либо внутриполитического или мирового инцидента, распространить фейковую новость, сдать деньги на поддержку какой-либо организации.
4. **Максимальный перепост** служит формированию среди пользователей привычки делать репосты каких-либо публикаций к себе в ленту. Таким образом публикации, в том числе и фейки, могут распространяться лавинообразно, каждый раз захватывая все больше и больше пользователей, которые занимаются их репостом и распространением.
5. **Метод наводнения** – формирование постоянного и плотного информационного поля вокруг какого-либо вопроса. В результате у пользователей складывается ложная уверенность, что какая-либо позиция поддерживается разными независимыми источниками и обсуждается на разных уровнях, а значит эта позиция важна и правдива.
6. **Метод «от вас скрывают, а я расскажу правду»** – придает максимальную правдоподобность сообщению и создает у пользователей чувство избранности, ведь с ними поделились какой-то правдой, которую от всех остальных скрывают.
7. **Виртуальные рейтинги и награды** – в соцсетях, сетевых сообществах и массовых играх используются награды и рейтинги, призванные подстегнуть интерес пользователей, заставить их участвовать в активности не «просто так», а за какую-либо награду, даже если эта награда – символическая позиция в виртуальном рейтинге.

Личный пример

> **Обращаем внимание на молодёжный сленг и изучаем его! Для этого бывает достаточно посмотреть значение разных слов в Интернете. Так, например, слова «самовыпил» и «выход» могут означать самоубийство. Пора бить тревогу по всем фронтам!**

Цифры:

58% **убеждены, что современные дети живут в более опасное время, чем они сами** *(по данным ВЦОМ).*

46% **опрошенных считают, что Интернет значительно увеличивает количество самоубийств** *(по данным ВЦОМ).*

60% **опрошенных взрослых уверены, что социальные сети и их контент оказывают вредное воздействие на детей** *(по данным ВЦОМ).*

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

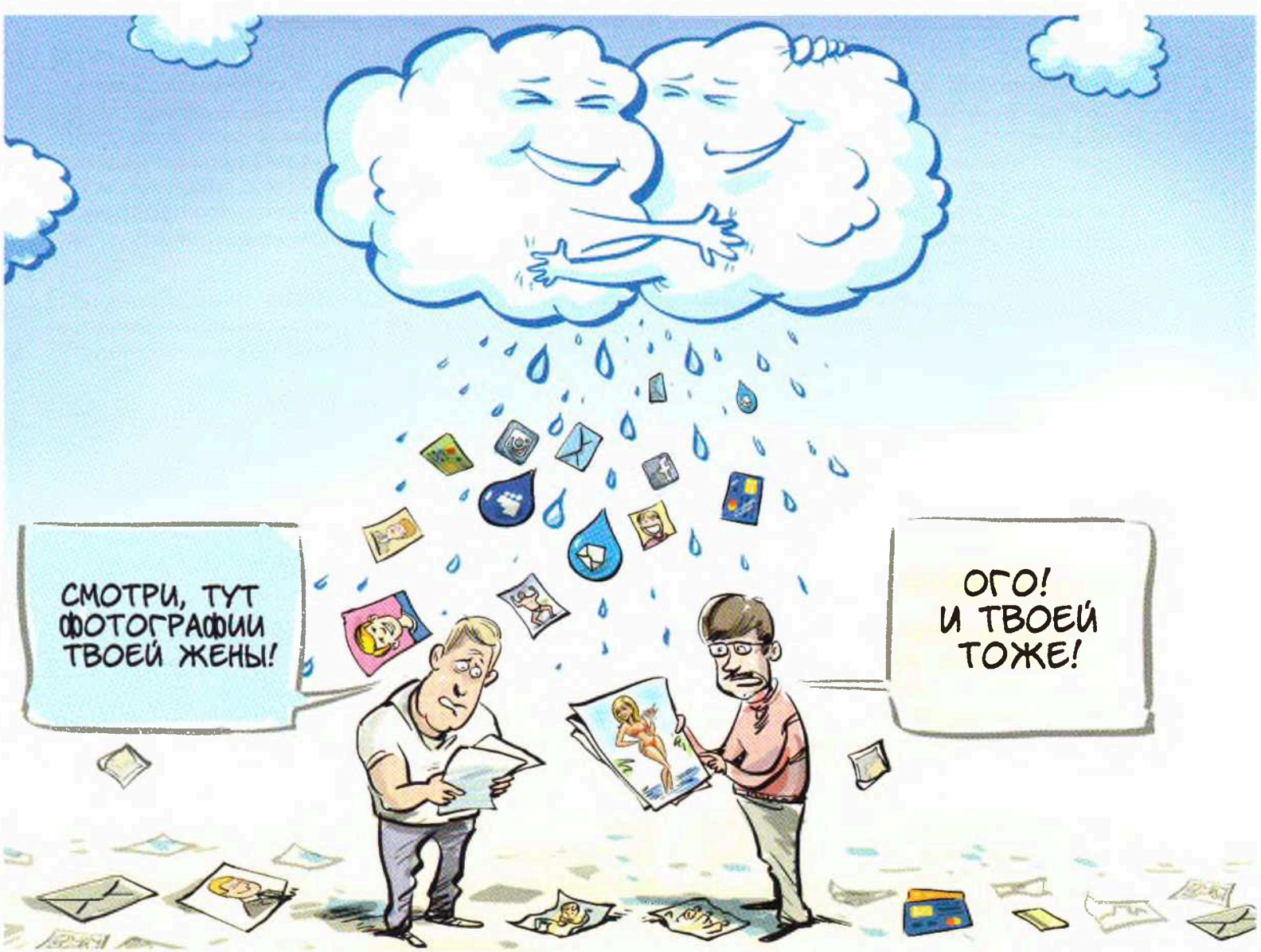
Сайт
ligainternet.ru

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

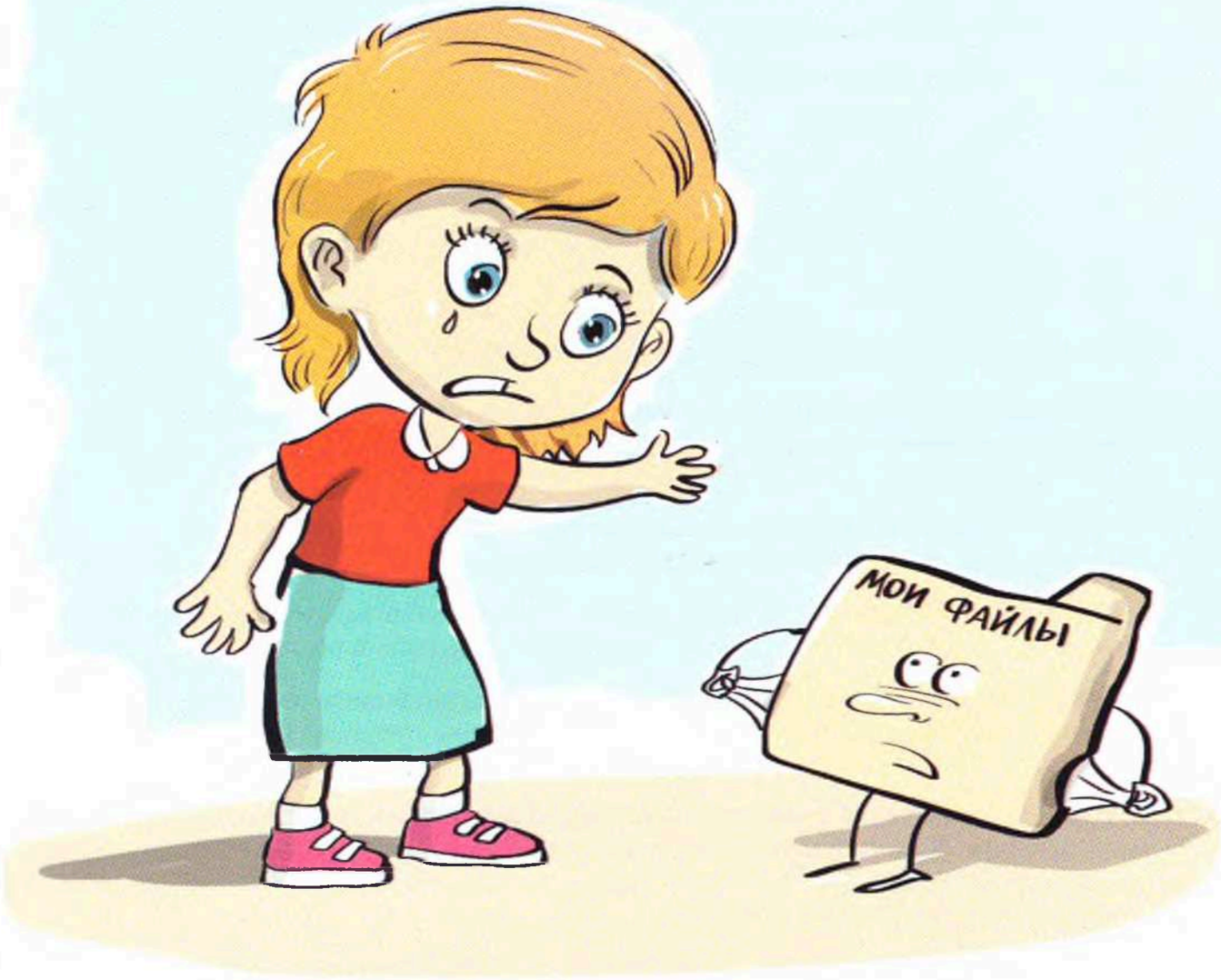
Не публикуйте в соцсетях лишнюю информацию о себе. Абсолютно вся информация, включая ваши фото, адреса, увлечения, имена домашних животных и многое другое, могут быть использованы мошенниками для установления личности, создания подробной картины о вас, как о пользователе, и подбора персональных мошеннических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

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

Персональные данные – это все ключевые и важные сведения о человеке. Их следует тщательно беречь и не раскрывать в Интернете без необходимости. Раскрытие персональных данных в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже аккаунтов, мошенническим действиям, вымогательству денег у тебя или твоих близких, угрозах совершения компрометирующих тебя действий, краже денег и документов. В некоторых случаях это даже может привести преступника на порог твоего дома.

Что относится к персональным данным?

1. **Фамилия, имя, отчество;**
2. **Все твои документы** (паспорт, свидетельство о рождении, аттестат и др.);
3. **Банковские данные** (номер счета, карты, пин-код, CVV-код);
4. **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
5. **Фотографии и видеозаписи с твоим изображением;**
6. **Данные о твоих родственниках;**
7. **Твои логины и пароли.**

Чаще всего пользователи сети сами выкладывают информацию о себе в Интернет. Мошенники охотятся за этими данными. Большинство информации о жертвах преступники находят в открытом доступе в соцсетях и в Интернете.

Как защитить свои персональные данные?

1. **Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов.** Пароль восстановить проще, чем вернуть украденные деньги.
2. **Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**
3. **Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.
4. **Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.
5. **Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.
6. **Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.

МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

Современные мошенники в Интернете действуют не так, как мы обычно привыкли. Сейчас злоумышленники не крадут у нас деньги напрямую. Вместо этого мы сами им их отдаем. Мошенники манипулируют нами, нашей доверчивостью, страхом или жадностью, а современные технические средства позволяют подделать все, в том числе, сайт или номер телефона.

КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

1. **Взлом аккаунтов в соцсетях и рассылка сообщений от друзей.** Мошенники придумывают разные ситуации и просят срочно перевести деньги.

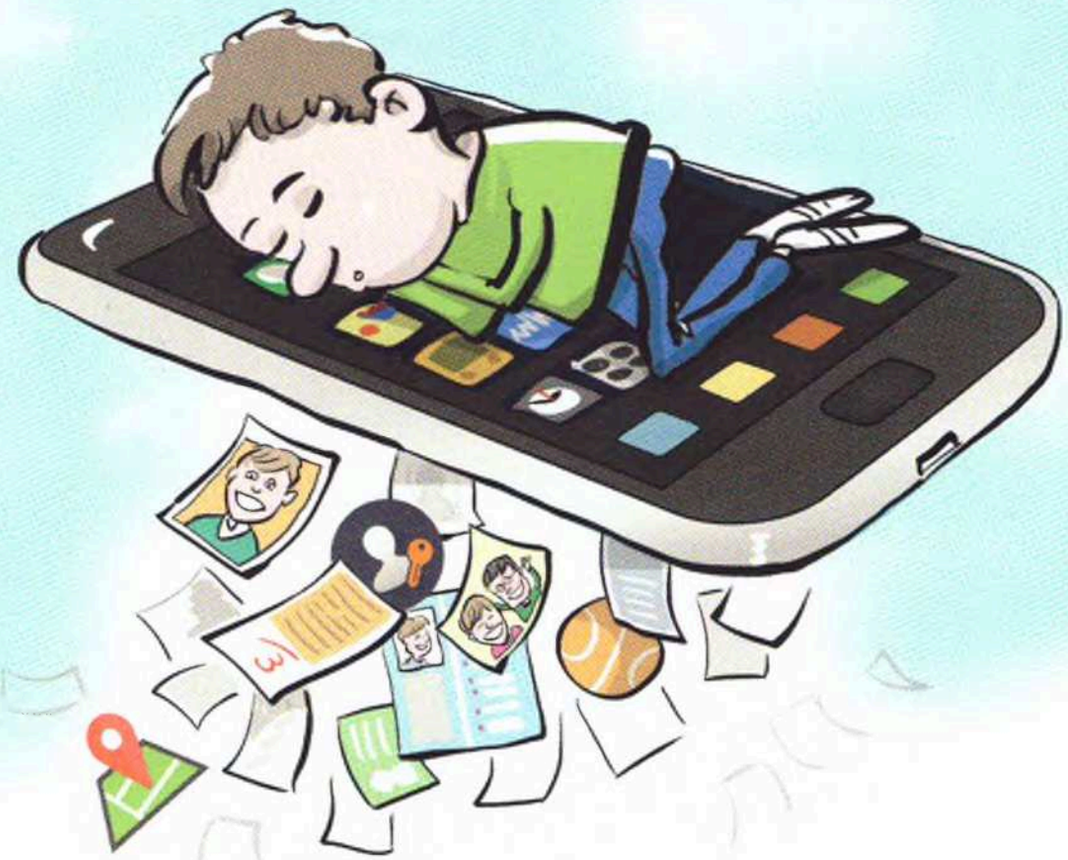
2. **Сайты-подделки.** Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-поделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.

3. **Рассылка писем по электронной почте и в соцсетях с выигрышем.** Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.

4. **Звонки с поддельных номеров.** Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.

5. **Шантаж.** Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях.

Современные технические средства позволяют мошенникам подделать любой номер телефона, любой сайт, взломать почту или личную страницу. Будьте бдительны и перепроверяйте информацию. Никогда не отправляйте свои интимные фотографии даже хорошо знакомым людям, которым вы доверяете. Знайте, что ваши откровенные фотографии, легкомысленно направленные кому-либо, могут быть украдены, в том числе, для рекламы разного рода неприличных или противоправных услуг. Вы можете узнать об этом только когда ваши близкие или знакомые увидят вас и составят о вас негативное мнение. Впоследствии подобные фотографии также могут быть существенным препятствием для зачисления в ряд ВУЗов или устройства на хорошую работу.



В своей работе мошенники активно используют социальную инженерию. Они сделают все, чтобы ты сам отдал свои деньги. Для этого они используют нашу невнимательность и доверчивость.

Знаешь ли ты, что никому нельзя сообщать свои пароли, пин-коды, коды из СМС и сообщений? В наше время это знают все, но мошенники могут обхитрить неосторожного пользователя. Они позвонят тебе и представятся сотрудником банка, расскажут о том, что прямо сейчас кто-то пытается украсть твои деньги со счета. А чтобы этого не случилось, ты должен сообщить им код из СМС, которая сейчас придет на твой номер. Естественно, никто твои деньги не крал. А вот если ты передашь мошенникам этот код, то они получат полный доступ к твоему счету, карте и всем деньгам, которые на ней лежат.

Мошенники не обязательно запугивают. Они могут сообщить о крупном выигрыше. Допустим, в 300 тысяч рублей. Но чтобы получить этот выигрыш, надо заплатить небольшую комиссию – всего лишь 300 рублей. Многие люди в такой ситуации теряют бдительность и думают, что 300 рублей – маленькая цена за такой большой выигрыш. Однако приз, естественно, они не получают, а лишаются своих денег.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ?

1. **Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию.** При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.

2. **Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили.** Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номеру и с какой целью.

3. **Проверяй адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.

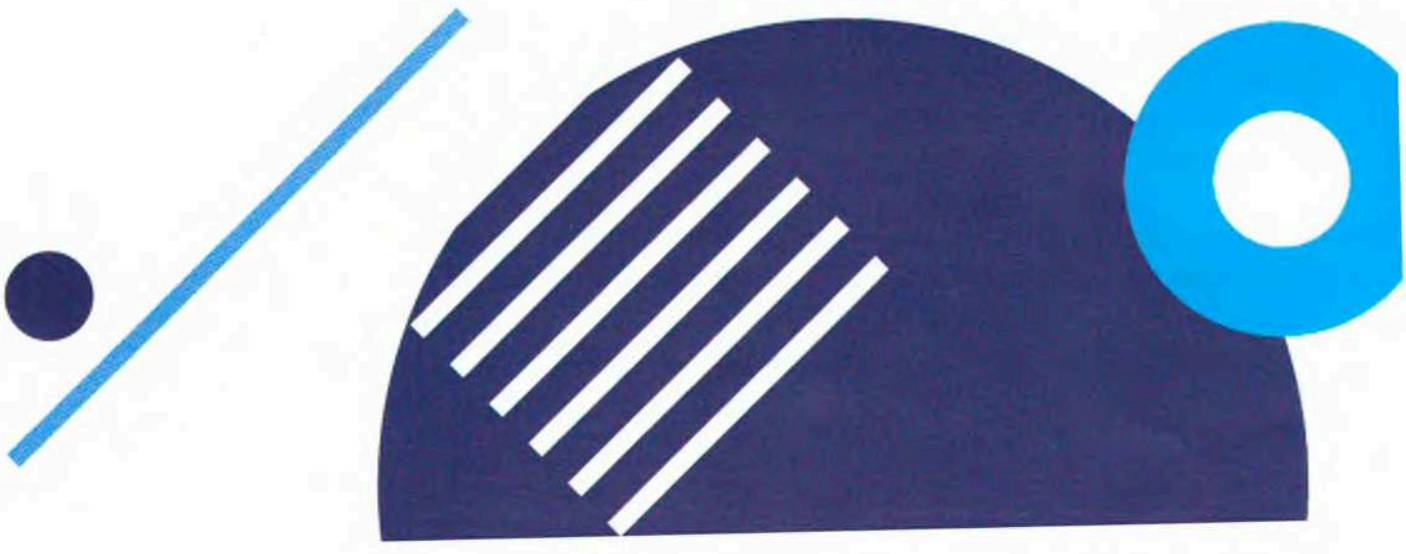
4. **Обращай внимание на наполнение сайта.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.

5. **Не переходи по незнакомым ссылкам.**

6. **Не открывай файлы из писем или сообщений, которые прислали незнакомые люди.**

7. **Если же ты стал жертвой мошенников, то следует сразу же сообщить об этом родителям.**

ЧТОБЫ НЕ ПОПАСТЬСЯ МОШЕННИКАМ – МЫСЛИ САМОСТОЯТЕЛЬНО!



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

10 СОВЕТОВ ДЛЯ ДЕТЕЙ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

1. **Для развлечения и общения с настоящими друзьями Интернет не нужен, нужна реальная жизнь**. Сокращай время пользования Интернетом! Отводи для общения в виртуальном мире не более 1 часа в день. Не позволяй социальным сетям отбирать у тебя здоровье и перспективы!

2. **Анонимность в сети - миф. Всё, что мы выкладываем в Интернете, остаётся там навсегда.**

3. **Проводи больше времени в реальной жизни:** общайся с друзьями, родителями, найди себе действительно интересное увлечение, читай, занимайся спортом, придумывай и реализуй полезные социальные проекты, помогай людям, включайся в общественную деятельность, смелее используй свои таланты.

4. **Будь бдителен! В Интернете много мошенников, которые охотятся за твоими деньгами и данными.** Есть и такие преступники, целью которых является испортить как можно больше детей или загубить их жизнь. Некоторые делают это за большие деньги, продавая снимаемые детьми видео и фотографии, а некоторые потому, что психически больны. Однако понять это, общаясь в Интернете, невозможно. Просто не подпускай к себе незнакомых людей и не позволяй им сделать из тебя свою жертву.

5. **Не выкладывай свои персональные данные в Интернет!** Помни, что отправлять их не стоит даже друзьям.

6. **Закрой свои страницы в соцсетях от посторонних!** Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и не продолжай общение.

7. **Не бойся рассказать родителям о своих проблемах!** Если кто-то решит тебя обижать, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.

8. **Помни, что из Интернета ничего не удаляется!** Если ты не хочешь, чтобы какие-то твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.

9. **Не верь всему, что написано в Интернете!** В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.

10. **Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни.** Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

НЕ СЛЕДУЙ МОДЕ!

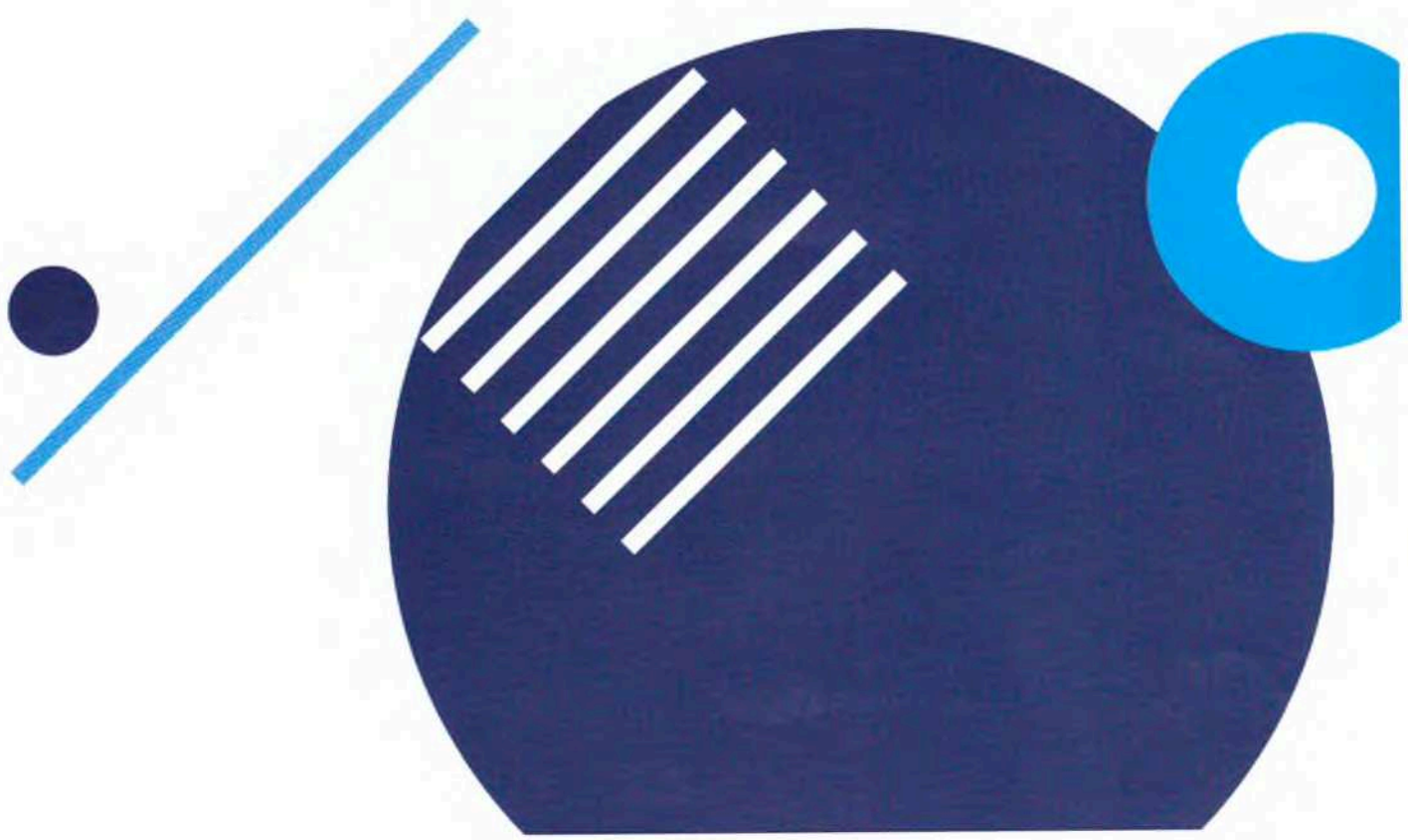
Социальные сети – самый верный способ «убить время». Сетевые развлечения поглощают его без остатка. Но с головой погружаясь в виртуальный мир, мы забываем про друзей, близких, учебу, работу, активный отдых и развитие.

Тебе может показаться, что не иметь профиля в социальной сети – это странно, но на самом деле все вовсе не так. Если у тебя нет профиля в соцсети – поздравляем! Ты уже победил! Ведь теперь у тебя будет гораздо больше времени на полезные вещи: учебу, спорт, настоящую, не сетевую дружбу!

Все больше россиян признаются, что соцсети приносят им больше негативных эмоций: печаль, обиду, зависть. Отказ от соцсетей поможет стать по-настоящему счастливым.

Современные соцсети созданы не для общения. Они созданы для рекламы, для продажи товаров и услуг, навязывания чужого мнения. А если у тебя нет соцсетей – ты мыслишь и думаешь самостоятельно!

НЕ ПОГРУЖАЙСЯ В ИНТЕРНЕТ С ГОЛОВОЙ! ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!



ТРАВЛЯ В ИНТЕРНЕТЕ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

ТРАВЛЯ В ИНТЕРНЕТЕ

Травля в Интернете является большой проблемой для всех пользователей. Травлю в сети еще называют кибербуллингом. Она включает в себя издевательства, оскорбления, унижения, преследование человека.

Некоторым кажется, что травля – это всего лишь безобидные шутки. На самом деле это не так. **Травля может привести к проблемам со здоровьем, к психическим травмам и другим проблемам.** Иногда обижая других, обидчик стремится самоутвердиться за чужой счет. Очень часто обидчик сам является глубоко несчастным, нереализованным и затравленным человеком, который таким деструктивным способом пытается отомстить окружающим за свои проблемы. А, находясь под мнимой защитой Интернета, позволяющей сохранять определенную анонимность, обидчик смело оскорбляет других. Как правило, в реальной жизни обидчик не сможет в открытую сказать тебе ни одного обидного слова.

Однако защищённость обидчика в Интернете на самом деле имеет мнимый характер. Обидчик думает, что его никто не сможет найти, и последствий за его действия не будет. На самом деле это не так. Найти обидчика в сети для специалистов сегодня не составляет никаких проблем.

КАК ВЫГЛЯДИТ ТРАВЛЯ В ИНТЕРНЕТЕ?

1. **Оскорбительные и угрожающие сообщения, изображения или видео;**
2. **Передразнивание, бойкоты или унизительные комментарии в сети, в которых упоминается личность человека;**
3. **Распространение неприятных слухов и обсуждение человека за его спиной;**
4. **Создание поддельных аккаунтов от имени конкретного человека с целью обмануть или унизить его;**
5. **Специально смонтированные фото или видео с изображением человека.**

ЧТО ДЕЛАТЬ, ЕСЛИ ТЫ СТОЛКНУЛСЯ С ТРАВЛЕЙ В ИНТЕРНЕТЕ?

1. **Поговори с родителями или учителями об этой ситуации.** Они не оставят тебя одного в неприятном состоянии и помогут наилучшим способом разрешить любую ситуацию. Расскажи им, что ты воспринимаешь эту ситуацию серьезно и объясни какие чувства ты испытываешь.

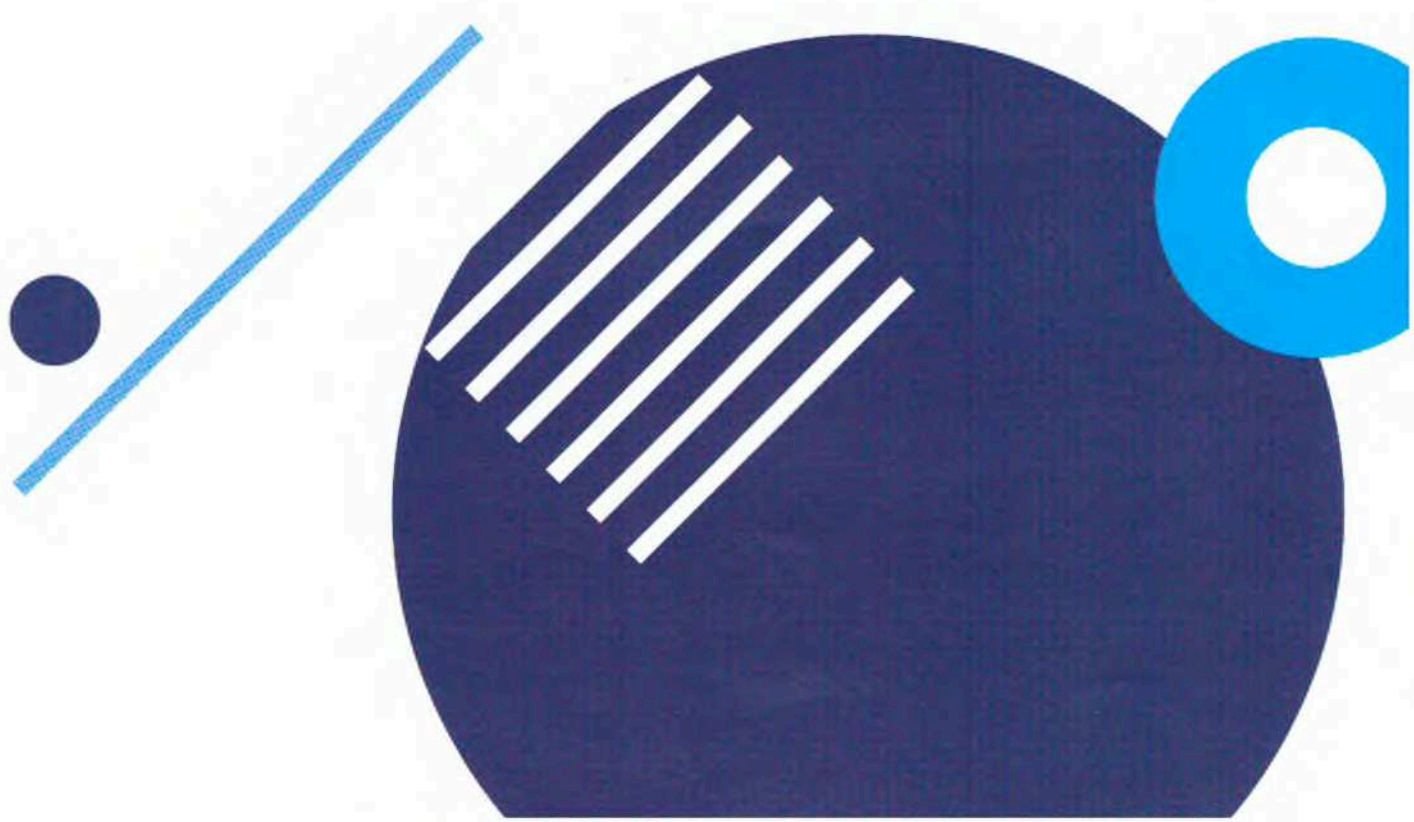
2. **Постарайся сохранять спокойствие и не отвечать обидчику.** Как правило, его цель – вывести тебя на эмоции. Помни, что твой обидчик распускает о тебе слухи, оскорбляет тебя не потому, что на самом деле считает тебя таким, а потому, что у него самого серьезные проблемы (возможно даже с психикой).

3. **Вместе с родителями собери доказательства:** сделай скриншоты переписки, скопируй ссылки на аккаунты обидчика, тебе это может пригодиться в случае обращения в полицию.

4. **Заблокируй обидчика и внеси его в черный список,** чтобы у него больше не было возможности оскорбить тебя или задеть ложными и неприятными высказываниями.

5. **Никогда не оставайся сторонним наблюдателем, если травле подвергнулся кто-то другой.** Собери в группе (в чате), в которой вы общаетесь команду единомышленников, обговори с ними стратегию действий против обидчика. Вам необходимо выступать единым фронтом против любых оскорбляющих действий и требовать прекращения недопустимого поведения. Как правило, обидчики не осмеливаются идти против большой группы людей, действующих заодно, у них не хватает на это смелости. Если действия обидчика не прекратятся и в этом случае, следует всей команде единомышленников демонстративно выйти из группы (чата), это окажет психологическое воздействие на остальных участников, а также будет поддержкой для жертвы травли. Попробуй выйти на личное общение с жертвой травли и поддержать ее. Если жертвой травли стал твой знакомый, расскажи об этом учителю или его родителю. Тем самым ты можешь помочь человеку, который самостоятельно не видит выхода из сложившейся ситуации и страдает.

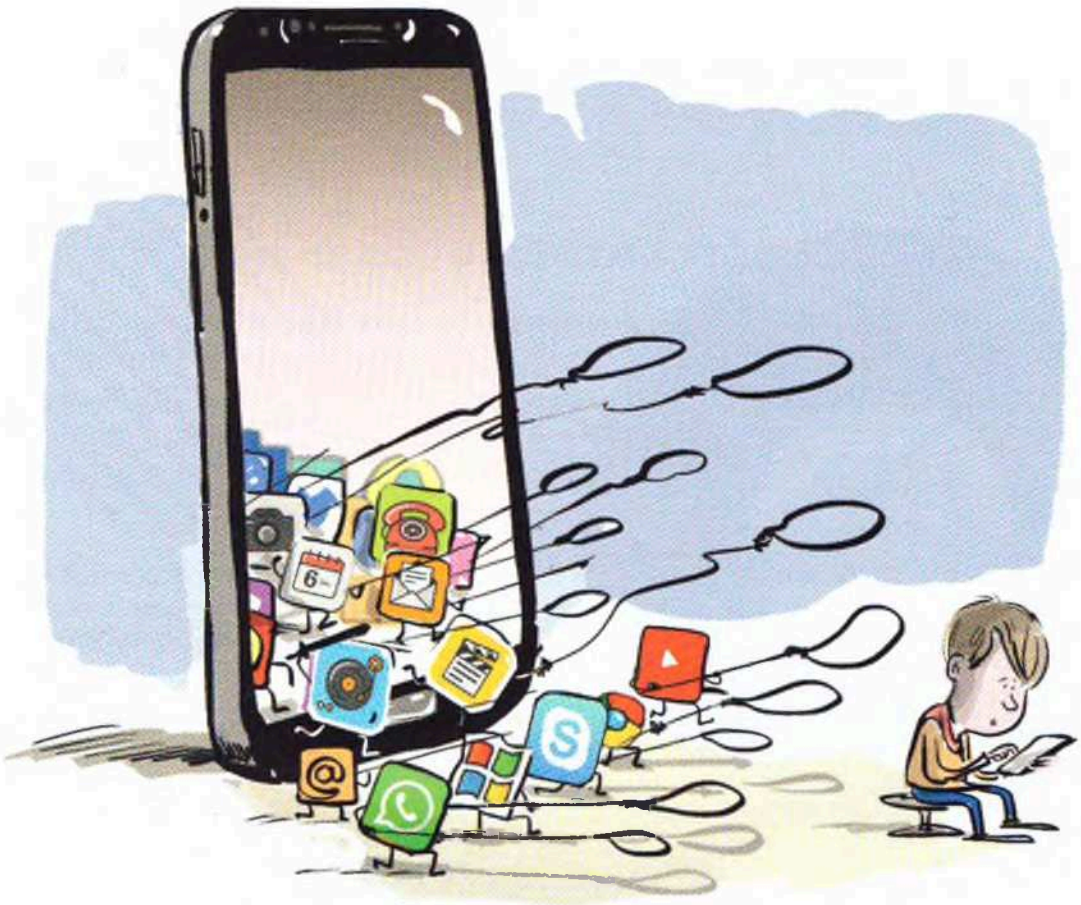
ПРОВОДИ БОЛЬШЕ ВРЕМЕНИ В РЕАЛЬНОЙ ЖИЗНИ!



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

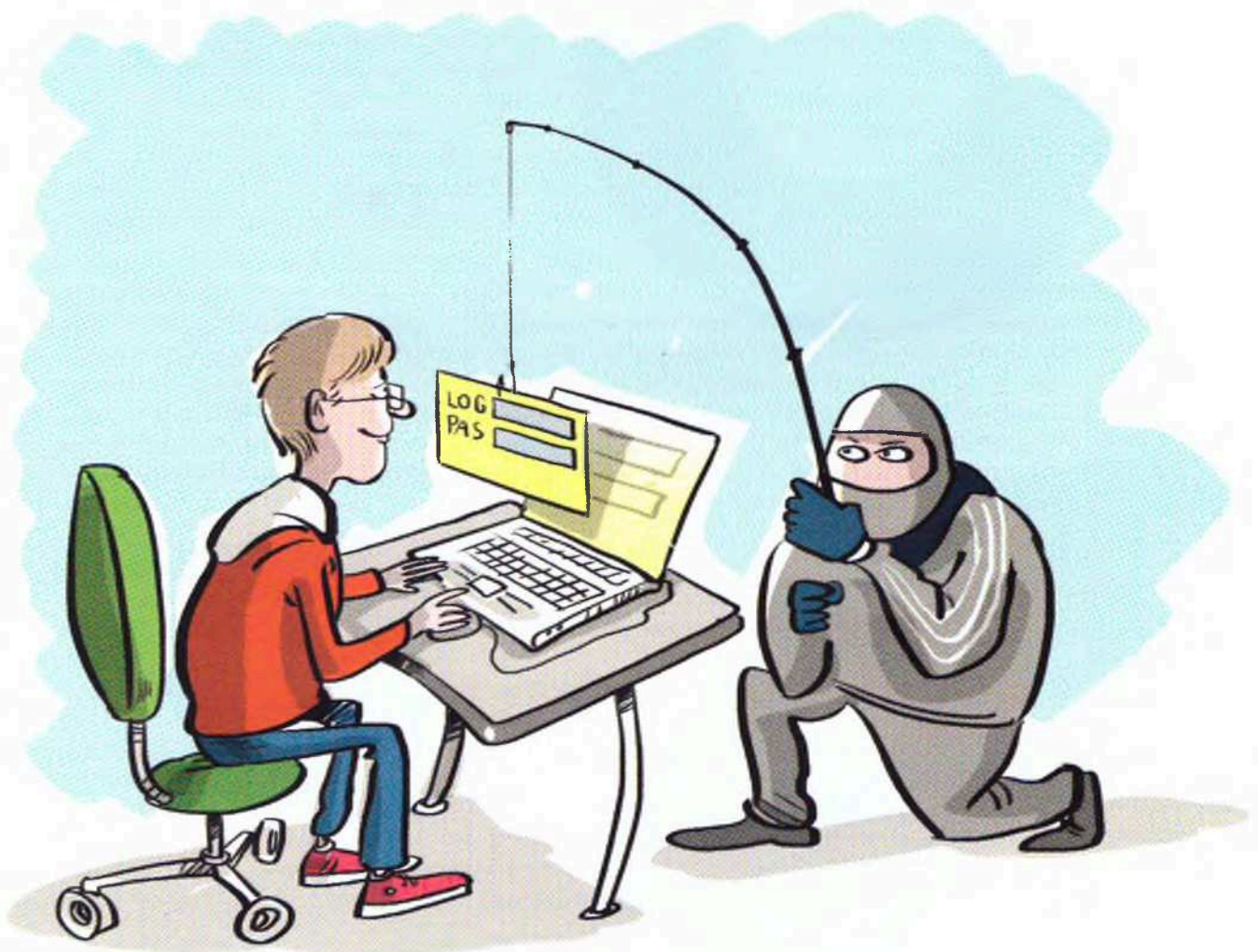
МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: необходимые средства защиты

Процветающий бизнес на каждом из нас

Современные технические средства очень сильно изменили виды мошенничества, которые используются злоумышленниками. Они могут, например, подделывать сайты, создать страницу абсолютно идентичную странице Интернет-магазина с нужным вам товаром, но при оплате деньги отправятся напрямую к мошенникам.

Самым распространенным способом мошенничества в Интернете является «фишинг». С его помощью мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу, например, известной соцсети. При попытке войти в свой профиль на таком сайте мошенники получат полный доступ к вашему аккаунту.

Они с лёгкостью подделывают любой номер телефона и не только его цифры, но даже могут сделать так, что при звонке ребёнок увидит надпись, например, «полиция», «мама», «брат» и т.п. Более половины россиян регулярно получают звонки от мошенников (по данным ВЦИОМ). Страшно? Есть способы остановить злоумышленников!



Ключевой вопрос

Как противостоять преступным действиям мошенников?

Внимание!

Современные мошенники активно используют социальную инженерию – психологические приемы, вынуждающие жертву сделать именно то, что нужно мошеннику, например перейти по ссылке, скачать вредоносный файл или сообщить код из СМС. По данным ВЦИОМ, 9% россиян теряли деньги в результате действий Интернет-мошенников, а 6% заявляли о краже крупных сумм.

За чем же охотятся цифровые мошенники?

- **Деньги;**
- **Персональные данные;**
- **Логины и пароли.**

Надо запомнить!

1. Для современных мошенников персональные данные являются не менее ценными, чем денежные средства, а иногда они даже полезнее. Именно с помощью персональных данных преступники отнимают у жертвы денежные средства, входя к ней в доверие. Кроме того, персональные данные сами по себе имеют ценность, ведь мошенники могут продавать их другим преступникам.
2. Кроме онлайн-мошенников существует другая, не менее опасная группа – телефонные мошенники. Они могут представиться кем угодно: сотрудником банка, полиции, прислать СМС от имени родственника. Они также используют социальную инженерию, пытаясь украсть данные. Иногда мошенники специально охотятся за голосом человека, например, задавая навязчивые вопросы. Их интересует то, как абонент назовет свои ФИО, а также скажет: «Да». В дальнейшем мошенники могут использовать записи голоса для входа в банковский аккаунт жертвы, голосом подтверждая банковские операции.
3. Еще одна опасность в Интернете – скрытые платные подписки. Многие мошенники или недобросовестные организации провоцируют пользователей на оформление подписок таким образом, что пользователь узнает об этом только тогда, когда обнаружит регулярное списание денег со своего счета. Такую скрытую подписку можно случайно оформить при переходе на сайт с пиратским контентом, при скачивании файла или приложения или при оплате какой-либо услуги в Интернете. Так, например, однократно купив что-либо или пожертвовав деньги, можно не заметить галочку, которая подтверждает ваше согласие на подписку. Иногда создатели сайта специально делают эту галочку едва различимой или даже вовсе скрытой с экрана. Будьте бдительны!

Полезные советы

Как защитить ребенка от мошенничества в Интернете?

1. В первую очередь следует научить ребенка перепроверять информацию. В случае с сайтами следует обращать внимание на адресную строку – нет ли в адресе сайта каких-либо изменений или неточностей. Если адрес отличается от настоящего даже на один символ – это явный признак подделки. Если входящий звонок поступает от представителя банка или другой структуры, следует самостоятельно перезвонить в эту организацию и задать им вопрос, есть ли у них такой сотрудник и мог ли он вам сейчас звонить. Чаще всего банки не осуществляют операции по звонкам. Однако следует учитывать, что мошенники могут целиком скопировать даже настоящий номер и представиться настоящим именем сотрудника.
2. Объясните ребенку, что не следует принимать поспешных решений. Мошенники могут требовать от жертвы принять решение в текущий момент. Они рассчитывают на то, что в спешке, панике или страхе человек утратит бдительность и охотнее согласится на перевод денег. В таком случае можно ответить: «Сейчас я все проверю и перезвоню вам», или «перезвоните мне через 5-10 минут, мне нужно время, чтобы подумать». Обычно этого времени хватает человеку, чтобы распознать мошенников, проверить информацию и не допустить ошибки.

3. Ребенка следует приучить беречь свои персональные данные с раннего возраста. Ребенок должен знать, что именно относится к персональным данным и что их нельзя размещать в Интернете без необходимости. Опасность представляют как сами данные, так и фотографии документов. Даже простое размещение номера телефона в социальной сети может привести к нежелательным звонкам, спаму, угрозам или шантажу.
4. Если у ребенка уже есть банковская карта, не следует хранить на ней много денег. Лучше всего класть деньги на карту тогда, когда он собирается что-то потратить или хранить на ней небольшое количество денег, которое не страшно будет потерять.
5. Не привязывайте телефон ребенка к банковским картам, счетам, платежным системам. Все платежи за ребенка лучше проводить самостоятельно.
6. Ограничивайте установку приложений на телефон ребенка. Наличие на телефоне антивируса и родительского контроля позволит защитить телефон от спама и вредоносных программ.
7. Установите ограничения и контроль на мобильном счете ребенка. Лимит расходов, можно установить в личном кабинете мобильного оператора. Там же можно отключить возможность оформления платных подписок и изменения тарифа.
8. Научите ребенка опасаться звонков с незнакомых номеров и не перезванивать на них. К любому звонку с неизвестного номера следует относиться с осторожностью. Если перезвонить на такой номер, вас могут перевести на линию, где за каждую минуту разговора с вашего счета будут списываться огромные деньги.
9. Объясните ребенку, что нельзя переходить по ссылкам из СМС и загружать файлы, которые пришли с неизвестного номера. Такой файл или ссылка могут установить на устройство вирус или отправить все данные владельца телефона прямо в руки к мошенникам.
10. Подключите ребенку защиту от нежелательных звонков. Такая функция есть у смартфонов на системах Android и iOS. Она позволит отфильтровать спам, звонки с опасных и нежелательных номеров.
11. Если ребенок уже стал жертвой мошенников, следует немедленно обратиться в полицию. Не забудьте сохранить все доказательства мошеннической деятельности – скриншоты сайтов, переписок, квитанции онлайн-платежей.

Личный пример

Установите на смартфоне ребенка надежный пароль, который он должен знать наизусть и ни с кем не делиться. Это обезопасит устройство при попадании в руки чужих людей, в том числе других детей.

ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

Интернет – это возможность общаться с друзьями на расстоянии, не терять связь на летних каникулах и обсуждать интересные темы. Но также в Интернете есть много незнакомых пользователей, которые не просто так хотят добавить тебя в друзья и начать общение. Незнакомцы в Интернете могут оказаться не теми, за кого себя выдают. Среди них могут оказаться мошенники или иные преступники, у которых дети вызывают особый интерес, и чтобы добиться возможности стать твоим другом, они могут соврать про свой возраст (представиться твоим ровесником) и поставить на аватарку чужую фотографию. Если человек, который предлагает тебе дружбу в Интернете, активно интересуется информацией о тебе или твоей семье, если он ведет себя агрессивно и грубо, если он предлагает неприятные или неприличные темы для общения, то лучше не добавлять его в друзья, а если добавил, то не стесняться заблокировать. То же самое следует сделать, если ты сомневаешься, правду ли про себя рассказывает новый знакомый из Интернета. Ведь под аккаунтом твоего сверстника может скрываться самый настоящий преступник. Самым безопасным вариантом будет никогда не добавлять в друзья человека, с которым ты не встречались в реальной жизни.

ТЕБЕ СЛЕДУЕТ ОСТЕРЕГАТЬСЯ НЕЗНАКОМЦЕВ В ИНТЕРНЕТЕ, КОТОРЫЕ:

1. Задают много вопросов о семье и личной жизни;
2. Просят об одолжениях в обмен на что-либо;
3. Убедительно просят никому о них не рассказывать и держать дружбу в тайне;
4. Задают вопросы о том, кто еще имеет доступ к твоему телефону, компьютеру или аккаунту;
5. Настаивают на личной встрече;
6. Заставляют тебя чувствовать себя виноватым, шантажируют или даже угрожают;
7. Ведут с тобой такие разговоры, после которых ты ощущаешь печаль, тревогу, грусть, стыд, страх, одиночество, свою ненужность близким, разочарование в жизни или людях, безысходность, злость, ненависть, желание причинить кому-то боль (знай, что все это не твои чувства, а лишь умелая манипуляция твоим сознанием).

ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

1. **Страницы в социальных сетях лучше закрыть от посторонних.** Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои личные данные от попадания в руки преступников. Как правило, информацию о себе, своих увлечениях, хобби, фото с друзьями и многое другое мы публикуем в соцсетях. Очень часто информацию о нас злоумышленники берут в открытом доступе.

2. **Будь осторожен, когда добавляешь незнакомого человека в друзья, особенно того, кого ты не знаешь в реальной жизни.** Если же новый знакомый задает тебе много вопросов о семье или о том, где ты живешь и учишься, то никогда не рассказывай ему эту информацию. Сразу же сообщай о подозрительном незнакомце своим родителям.

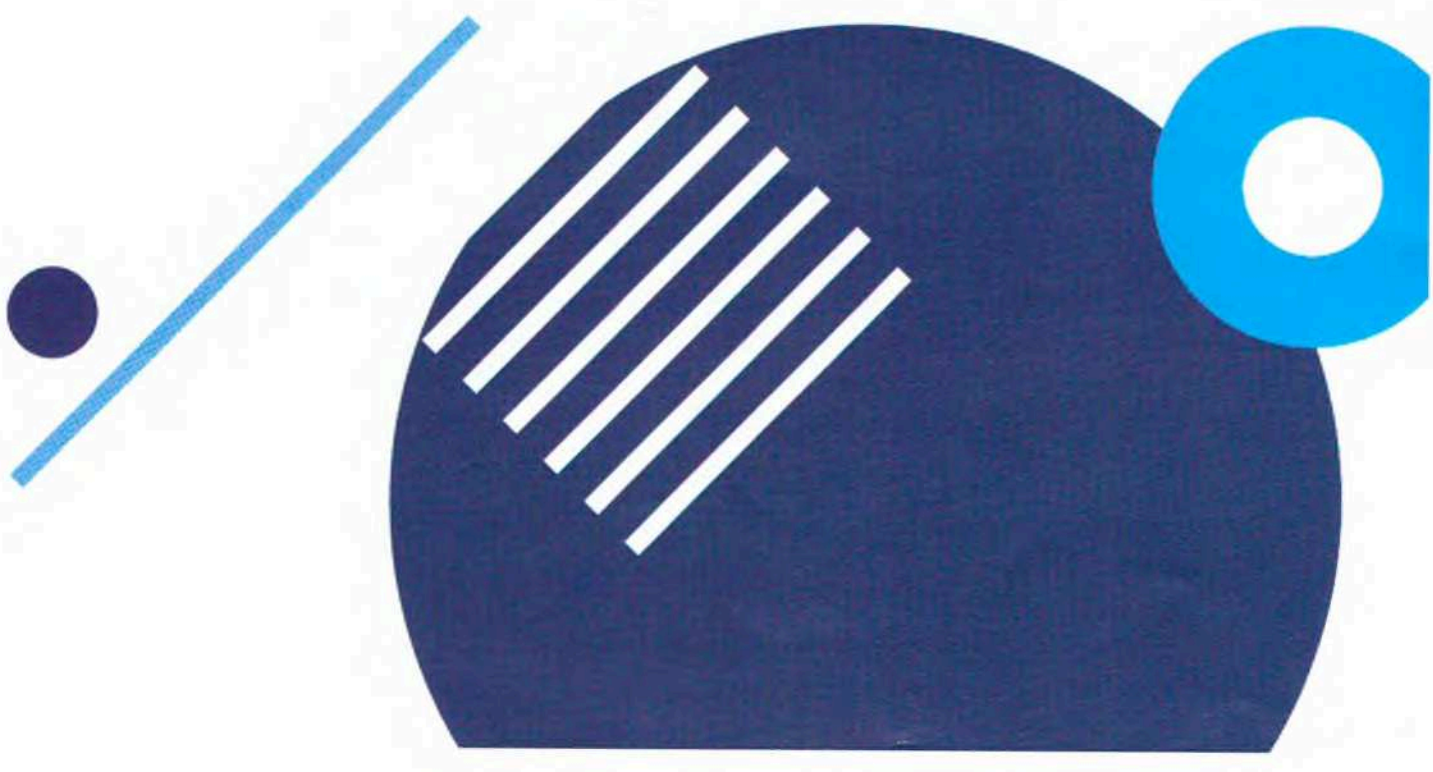
3. **Будь внимателен, если в переписке тебя призывают к действию и пытаются подловить.** Об этом свидетельствуют такие фразы, как: «А ты сможешь или тебе слабо?» «Все мои знакомые уже это делали, в этом нет ничего такого» и аналогичные. Такие фразы должны тебя насторожить. Рекомендуем сразу блокировать подобные аккаунты.

4. **Не соглашайся на встречу с людьми из Интернета.** Под профилем твоего ровесника могут сидеть далеко не девочки и мальчики, а самые настоящие преступники. Всегда сообщай своим родителям о своих друзьях из Интернета, а также о том, куда ты направляешься, с кем собираешься встретиться во избежание опасности.

5. **Если человек, с которым ты общаешься в Интернете заставляет тебя испытывать негативные чувства и эмоции, о которых было написано ранее, поделись об этом с родителями или другими взрослыми людьми, которым ты доверяешь.** Не стесняйся признаться в этом. Такие эмоции может испытывать любой человек, но только взрослый в состоянии помочь избавиться от них и защитить тебя от их воздействия.

Помни, что любую ситуацию ты можешь обсудить со своими родителями, не бойся обращаться за помощью. От этого зависит твоя безопасность, а возможно, даже жизнь.

БУДЬ ОСТОРОЖЕН, ДОБАВЛЯЯ «ДРУЗЕЙ» ДЛЯ ОБЩЕНИЯ В СЕТИ!



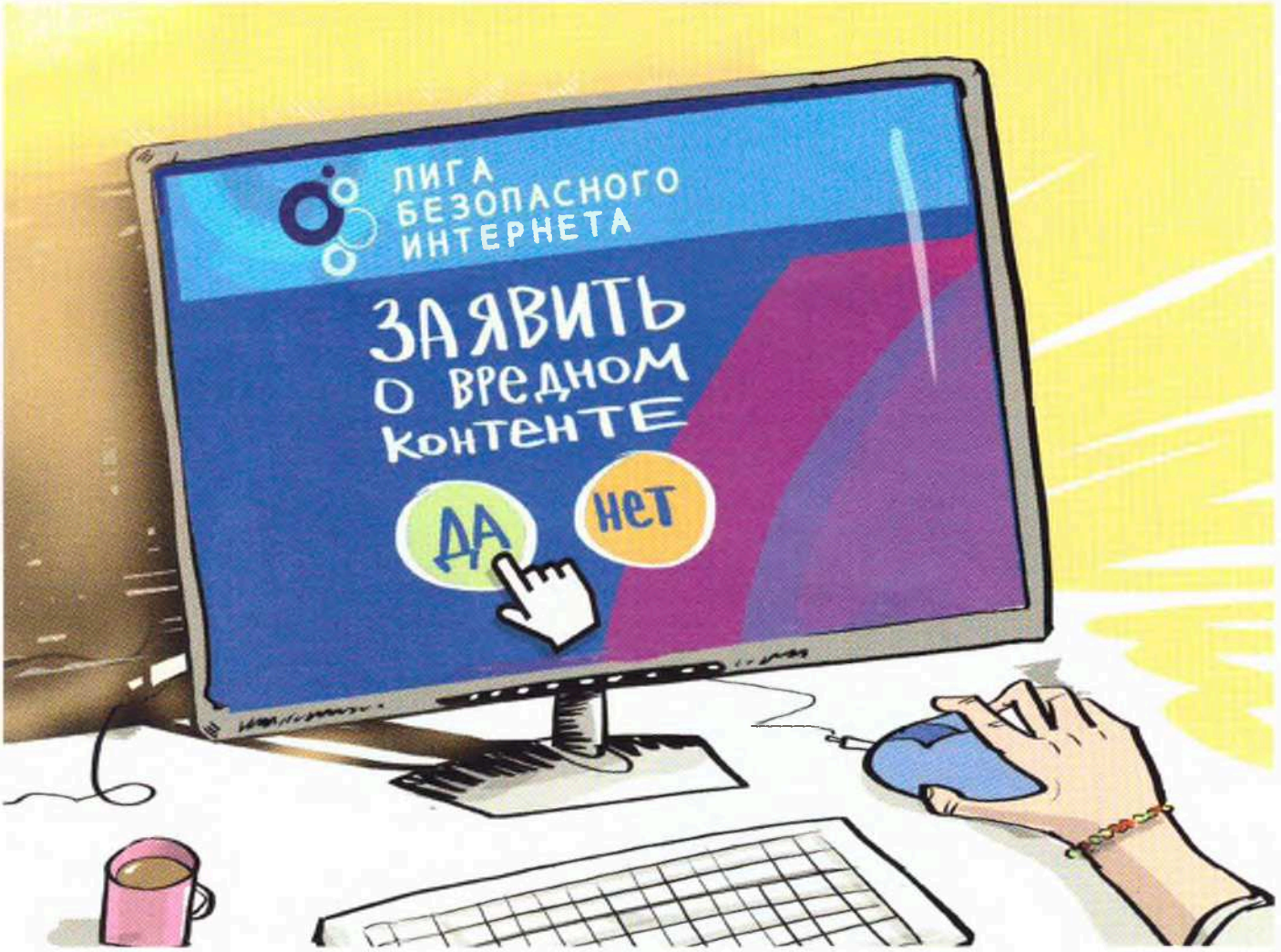
ОПАСНЫЕ ПУБЛИКАЦИИ В СОЦИАЛЬНОЙ СЕТИ: ПОЧЕМУ НЕЛЬЗЯ ПРОМОЛЧАТЬ!

Ваше право повлиять на Интернет

Многие из вас сталкиваются с опасным контентом в соцсетях. Такой контент может принимать самые разные формы. В опросе, проведенном ВЦИОМ, 32% опрошенных заявили о вреде, который Интернет приносит обществу, 35% согласились, что контент в Интернете может нести угрозу семейным ценностям, а 46% отметили, что Интернет значительно увеличивает число самоубийств.

> Здесь дана подробная инструкция по обращению в органы власти в связи с распространением деструктивного контента. Инструкция универсальна и применима ко всем социальным сетям. Направление обращений в органы власти — это ваше право по закону. **Никто не может вас в этом ограничить.**

В обращении указывается конкретная ссылка на аккаунт, группу, сообщество, чат или список таких ссылок. Желательно также прикладывать скриншоты самих публикаций, так как часто они бывают удалены/заблокированы/скрыты к моменту рассмотрения письма.



Ключевой вопрос:

Куда и к кому обращаться по поводу опасной информации в сети?

Внимание!

Вы установили факты распространения детской порнографии, призывов к суициду, рекламы азартных игр (онлайн-казино), склонения несовершеннолетних к противоправным действиям. По всем этим темам нужно обращаться в Роскомнадзор.

Сделать это можно двумя способами:

- **Первый:** если у вас есть аккаунт на госуслугах, то проще направить через приложение Роскомнадзора. Вы можете скачать его в магазине приложений как для Android, так и для Apple:

https://play.google.com/store/apps/details?id=org.rkn.ermp
https://apps.apple.com/us/app/ркн/id1511970611

В приложении необходимо приложить ссылку и скриншот опасной публикации. Здесь очень быстро можно отследить результат обращения, проверить был ли заблокирован тот или иной ресурс.

- **Второй:** если нет учетной записи на госуслугах, то можно направить через форму на официальном сайте Единого реестра запрещённых сайтов:

https://eais.rkn.gov.ru/feedback/

Здесь необходимо выбрать тему обращения, прикрепить ссылку и скриншот опасной публикации.

Надо знать!

Наркотики, экстремизм:

Если кто-то в видео или публикации пропагандирует наркотики, говорит об эффектах от их употребления или демонстрирует употребление, то нужно обращаться в Министерство внутренних дел Российской Федерации. Для этого на сайте МВД России необходимо выбрать Главное управление по контролю за оборотом наркотиков.

Также в МВД России необходимо обращаться, если вы столкнулись с информацией экстремистского характера, в том числе с контентом, посвященным скулшутингу (массовые расстрелы в школах). Для этого на сайте МВД России необходимо выбрать Главное управление по противодействию экстремизму.

Чаще всего это довольно агрессивные публикации с использованием нецензурной брани, где содержатся призывы убивать, громить, крушить, истреблять, использовать оружие, физическую силу, выходить на улицы для применения насилия, нападать на группы людей или социальные учреждения.

Форму для подачи заявления вы можете найти на официальном сайте МВД России:

https://мвд.рф/request_main

На сайте необходимо заполнить данные и вставить текст письма. В тексте необходимо добавить ссылку на публикацию и указать название соцсети и прикрепить скриншот.

ЛГБТ-пропаганда, видеоролики с насилием, жестокостью, истязанием людей или животных, пропаганда проституции и аморального образа жизни, информация, вызывающая у детей страх, ужас или панику, видео ненасильственных смертей и катастроф:

Подача заявления по такому контенту осуществляется на официальном сайте Генеральной Прокуратуры Российской Федерации:

https://epp.genproc.gov.ru/web/gprf/internet-reception

Введите текст обращения и прикрепите скриншот опасной публикации. Необходимо также добавить ссылку на публикацию и указать название социальной сети.

Также, обращения о фактах нарушения Российского законодательства в Интернете можно присылать Лиги безопасного Интернета: info@ligainternet.ru или передавать по горячей линии: 8 (800) 700-56-76. Лига безопасного Интернета перенаправляет все входящие обращения в соответствующее ведомство.

Не опускайте руки!

ВОПРОС: «Я направил/а обращение и получил/а ответ, в котором содержится отказ в рассмотрении или опасная информация не была обнаружена».

ОТВЕТ: Любой ответ, содержащий отказ в рассмотрении обращения, либо отказ в удалении противоправной информации, вы можете обжаловать в прокуратуре. Инструкция по обращению в прокуратуру дана выше. К письму необходимо приложить сканы/копии ответов с отказом.

Также вы можете такие ответы присылать нам, в Лигу безопасного интернета. В дальнейшем мы перенаправим их в Роскомнадзор, МВД или Генеральную прокуратуру и будем добиваться удаления информации.

Ответы вы можете присылать на почту info@ligainternet.ru с пометкой «Отказ». Если вы хотите публиковать ответы в комментариях, то не забывайте закрывать на скриншотах ваши персональные (личные) данные!

Личный пример

Чем больше обращений будет подано, тем быстрее социальные сети будут очищены от противоправного контента.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

МАНИПУЛЯЦИИ В ИНТЕРНЕТЕ: ФЕЙКИ, ЛОЖЬ, НЕДОСТОВЕРНАЯ ИНФОРМАЦИЯ

Что такое «фейк»?

Проблема верифицированных источников информации сейчас стоит очень остро не только в России, но и во всем мире. Фейк – целенаправленно распространяемая ложная информация под видом достоверной. Может выражаться в самых разных формах, таких как: текстовые материалы, новостные статьи, аудио- и видеозаписи, передачи, а иногда и целые фильмы, снятые в документальном или псевдодокументальном жанре.

Ключевой вопрос:
Жизнь в век дезинформации.
Фейки и ложь в сети

Основным местом концентрации фейков является Интернет. Подобные материалы чаще всего распространяются через интернет-мессенджеры, а уже оттуда попадают в социальные сети или «желтые» средства массовой информации.

Фейки могут распространяться с самыми разными целями:

1. Ради шутки или создания повышенного внимания какому-либо событию.
2. Для увеличения посещаемости сайта («накручивания счетчика просмотров»). Создаются «громкие» заголовки-приманки, кликнув на который пользователи переходят на сайт и таким образом увеличивают трафик этого сайта.
3. С целью дезинформации читателей о реальной ситуации: изменения настроения в обществе, отношения людей к какому-либо вопросу, создания паники или волнения среди людей.

Внимание!

Самый распространенный формат фейков, с которым сталкивался практически каждый – **фейковые новости.** Миллионы людей, подвергаясь регулярному воздействию фейков, начинают верить ложной информации, что в перспективе приводит к негативным последствиям. Лишь 49% россиян, согласно опросу, проведенному ВЦИОМ, уверены, что смогут отличить фейк от настоящей новости.

С фейками в интернете сталкиваются не только взрослые, но и дети. Ребенок может увидеть заголовок на сайте, содержащий ложную информацию. Фейки могут целенаправленно рассылаться пользователям в мессенджерах или соцсетях. Кроме того, иногда происходят взломы официальных сайтов или страниц известных организаций. В таком случае злоумышленники могут рассылать ложную информацию от их лица.

Как правило, в информационном пространстве **фейки живут относительно недолго – 3-4 дня.** Для искусственного поддержания интереса к подобному материалу совершаются «вбросы» – ложная информация поступает в Интернет через специальные каналы, откуда распространяется в настоящие СМИ, либо же расходится по пользователям и распространяется с помощью пересылки друг другу.

Кроме фейков существуют и самые настоящие «ментальные вирусы». Ментальные вирусы – это какие-либо тексты, статьи или новости, а иногда аудио- или видеозаписи, содержащие в себе определенную идею. Как и настоящие вирусы, они способны заражать сознание людей и целого общества, внедряя вредную, опасную и разрушительную идею.

Источники опасности:

- **У каждого фейка есть конкретная цель** – могут провоцировать людей на совершение опрометчивых поступков.
- **С учетом специфики Интернета - очень большой охват аудитории, скорость распространения.**
- **Могут представлять угрозу жизни и здоровью людей.**
- **Инструмент манипуляции.** Создатели фейка могут управлять подвергнувшимся воздействию как организованной структурой.

Как распознать фейк?

1. Сообщение быстро распространяется в соцсетях или мессенджерах.
2. Сообщение очень эмоциональное, вместе с тем не содержит факты, которые возможно перепроверить.
3. Передаются сведения об угрозе жизни и здоровья большого числа людей, а также о наличии многочисленных жертв.
4. Присутствует указание на то, что власти скрывают информацию во избежание паники или волнений. Именно поэтому вы не найдете ничего в СМИ. Подчеркивается, что значимая для общества информация специально утаивается.
5. Присутствует просьба о максимальном распространении информации, либо о сокрытии (ведь автор сообщил ее вам «по секрету»).
6. Присутствует указание на лицо, сообщившее новость (врач больницы, водитель скорой, учитель школы, знакомый знакомого), либо информация о месте, где что-то произошло (номер больницы, название города, адрес школы).
7. Источник информации сложно установить.

При проверке информации есть ряд маркеров, на которые очень важно обратить внимание:

1. **Оригинал всегда лучше любого пересказа,** поэтому всегда важно искать оригинальный источник информации и задумываться на сколько этому источнику информации можно доверять. Не является ли, например, источником новости желтое СМИ или какая-то из «тизерных» сеток, которые занимаются привлечением трафика пользователей с помощью «кликбейтных», то есть громких заголовков.
2. **При работе с оригинальными источниками важно смотреть взаимосвязь между этими источниками информации.** Если информация опубликована в разных источниках, то как они сами между собой связаны. Не является ли это партнерской сетью ресурсов или единой сетью распространения информации.
3. **Чаще всего разнообразие фейковых сообщений очень низкое,** постоянно публикуется фактически одно и то же сообщение. Практически все фейки являются перепостами.
4. **При сравнении оригинальной настоящей новости и фейка, у настоящей новости всегда очень много свидетелей,** очень много участников, они по-разному рассказывают своими словами о том, что произошло. Настоящая новость имеет очень много серьезных верифицированных источников информации. Сейчас ни одна заслуживающая внимания новость не проходит мимо ведущих средств массовой информации.
5. **Очень важно обратить внимание на контекст новости** и проверять полную суть любой цитаты, которая используется в том или ином сообщении. Не стоит доверять ссылкам на громкие и авторитетные имена. Проверять нужно как цитаты, так и факты, кому бы они не принадлежали, какая бы известная фамилия ни была озвучена.
6. **Очень важно обращать внимание на суть, смысл самого материала,** а не на мелкие детали, которых очень много в фейках. Они, таким образом, отвлекают внимание от содержания, придавая некую достоверность материалу.
7. **В новой информационной реальности важно научиться доверять серьезным средствам массовой информации, официальным источникам,** которые дорожат своей репутацией и ответственно относятся к распространению новых сведений и данных.

Полезные советы

Если вы получили или обнаружили недостоверную информацию, есть простые шаги, с помощью которых можно защитить себя, своих друзей и родственников от массового распространения этого сообщения:

1. **Стоит дождаться официального подтверждения или опровержения** громкой новости, прежде чем пересылать что-то друзьям и знакомым.
2. **Обратитесь в службу поддержки** и направьте туда все имеющиеся у вас ссылки, скриншоты и т.д.
3. **Обратитесь в полицию, Роскомнадзор** и прикрепите ссылки и скриншоты страниц, содержащих недостоверную информацию.
4. **Если вы считаете, что сообщение или публикация является общественно опасной, вы можете прислать скриншот и ссылку в Лигу безопасного Интернета по адресу: info@ligainternet.ru или в сообщениях VK: vk.com/liga.**

Внимание!

В случае обнаружения фейковой информации не стесняйтесь и пользуйтесь кнопкой «Пожаловаться» (в случае с социальными сетями или мессенджерами). Мессенджеры и соцсети должны оперативно блокировать такие сообщения и публикации.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ЦИФРОВАЯ ЗАВИСИМОСТЬ ДЕТЕЙ

Дети – цифровые аборигены

Наши дети в современном мире много времени проводят в Интернет. Все, что они смотрят, пишут и размещают в сети сохраняется навсегда, поисковики найдут сказанное или выложенное ими через годы. По прошествии лет ребенок станет совсем другим человеком, у него будут новые друзья, знакомые, новая работа и, возможно другие взгляды. И ему может стать неудобно, стыдно или невыгодно иметь такие цитаты, такие фотографии и такие связи. Сетевое поведение может аукнуться ребенку при поступлении в ВУЗ или на работу, при получении в визы или при интересных знакомствах.

Поисковики помнят всё. Кнопки «Удалить» из Интернета не существует.

Но помнит он только то, что мы сами ему о себе сообщили.

Ключевой вопрос:

Сколько времени, для чего и с кем наши дети в сети?

Внимание!

Не только дети, но и взрослые могут проводить в Интернете целый день. Видео, соцсети, игры - на это можно тратить очень много времени. Как показали независимые исследования в 76% случаев дети используют Интернет для игр, в 70% для просмотра видео, в 67% для общения с друзьями и в 53% для подготовки к урокам. 80% опрошенных школьников не могут обойтись без смартфона*. Среднее время, которое подростки проводят в Интернете, составило почти 6 часов в день*. Эта пугающая тенденция приводит к подмене реальных ценностей виртуальными.

Ключевые фигуры IT-отрасли, которые сами занимались разработкой устройств и программ, такие как Билл Гейтс или Стив Джобс, строго ограничивали время использования Интернета и гаджетов в своей семье. До определенного возраста они вообще не разрешали детям пользоваться смартфонами.

Признаки «беды»

1. Ребенок теряет интерес к нахождению на улице, встречам с друзьями или спортивным играм.
2. Ребенок плохо учится в школе, постоянно даже там «сидит» в смартфоне.
3. Ребенок утомляется, плохо спит, жалуется на головные боли и зрительное утомление.
4. У ребенка меняются привычки в еде.
5. Ребенок начинает плохо следить за личной гигиеной.
6. Ребенок зацикливается на конкретном сайте или игре.
7. Ребенок крайне агрессивно реагирует на просьбы отвлечься от его виртуальных занятий.
8. Находясь не за компьютером, ребенок ведет себя нервно или раздражительно.
9. Ребенок отдаляется от родителей, перестает разговаривать с ними на личные, волнующие его темы.
10. Ребенок отдаляется от одноклассников и друзей в реальном мире, отдавая предпочтение «виртуальному общению, находит себе лучшего друга «родную душу» в социальных сетях.
11. Ребенок проводит ночное время или часть времени, предназначенного для сна, в социальных сетях или за компьютерными играми.
12. Ребенок резко меняет свое отношение к вопросам, касающимся традиционных духовно-нравственных основ жизни, в частности: патриотизма, милосердия, сострадания, начинает защищать права на нетрадиционные сексуальные отношения, смену пола, гендерную идентичность, идеологию феминизма, чайлдфри и пр.
13. Ребенок проявляет беспричинную агрессию, замкнутость, депрессию, частую смену настроения.
14. На теле ребенка регулярно появляются ссадины, порезы или иные повреждения.

Полезные советы

1. Установите ограничения на то, когда и сколько времени может проводить ваш ребенок в Интернете во внеучебное время.
2. Введите запрет на использование ребенком телефонов, компьютеров и планшетов в ночное время. Общение ребенка через социальные сети и личную переписку в ночное время часто используется преступниками как методика доведения их до самоубийства, вовлечения в опасные квесты, нанесения вреда собственному телу, склонения к разговорам на сексуальные темы и иные виды деструктивного поведения.

* Всероссийский центр изучения общественного мнения

3. Используйте доступные вам технологии – функции родительского контроля! Инструменты для отслеживания времени, проведенного в сети, помогут вам установить рамки допустимого пользования электронными устройствами или Интернетом. Будьте честны с ребёнком и объясните, ради чего вы собираетесь использовать эти технологии. Родитель должен знать, чем ребенок занимается в сети! Более подробную пошаговую инструкцию о том, как настроить родительский контроль на разных устройствах можно найти на портале Лиги безопасного Интернета https://ligainternet.ru/

4. Отключите уведомления в приложениях социальных сетей, чтобы свести к минимуму отвлекающие факторы.

5. В зависимости от возраста вашего ребенка вы можете составить ежедневный распорядок использования гаджетов для всей семьи, в котором определено время на реальный мир (общение с друзьями и в семье без гаджетов), и время на виртуальный мир. Не противопоставляйте эти два мира, чтобы живое общение не было наказанием! Пусть расписание будет естественно чередовать различные полезные виды деятельности.

6. Не используйте смартфон как средство для освобождения ребенка от вас. Если ребенок слишком рано выйдет в Интернет, это может привести к «цифровой наркомании» и проблемам со здоровьем.

7. Разнообразьте список ваших домашних дел «оффлайновыми» занятиями – например совместными физическими упражнениями, чтением книг или настольными играми.

8. Обсудите возможность запрета использования электронных устройств во время занятий с классным руководителем вашего ребенка, вынесите данный вопрос на рассмотрение родительского собрания для распространения ограничения на всех учеников класса.

Личный пример

Вы можете подать хороший пример независимого поведения ребёнку и сами, сократив свой досуг перед экраном ноутбука или смартфона.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru