# 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.**

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

# ЧТО ТАКОЕ «НЕЛЬЗЯ»: ОБМЕН ИНТИМНЫМИ ФОТОГРАФИЯМИ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

## Незнакомцы в сети – всегда источник опасности

Наибольшую опасность для ребенка в Интернете представляют незнакомцы, которые могут начать общение с целью обмена интимными фотографиями или сексуального насилия.

Часто в сети несовершеннолетних обманом или уговорами заставляют совершать действия сексуального характера на веб-камеру или посылать интимные изображения. Они просят ребенка сохранять их отношения в тайне и стремятся физически и эмоционально разлучить его с близкими и друзьями.

**Ранее Лигой безопасного Интернета был проведен эксперимент. В социальной сети был зарегистрирован аккаунт ребенка. В течение суток после регистрации аккаунта начали приходить сообщения и запросы на дружбу от незнакомых взрослых.**

**Ключевой вопрос**

Как предостеречь ребёнка от общения с незнакомцами в цифровой среде?

# Внимание!

**Излишне доверительное общение с незнакомцами в Интернете и рассылка своих фотографий или видео может привести к очень неприятным последствиям:**

- **Травля** – фотографии и видео могут использовать тролли или агрессоры с целью травли жертвы, ее унижения и высмеивания;
- **Шантаж** – фото и видео интимного характера могут использовать для шантажа жертвы, вымогая деньги или склоняя к каким-либо действиям, в том числе интимного характера.
- **Вовлечение детей в изготовление детской порнографии и занятие проституцией -** фотографии и видео могут использовать преступники, с помощью шантажа или за плату вымогая фотографии ребёнка, либо принуждая его к занятию проституцией.

# Каким образом незнакомцы входят в доверие к ребенку?

- Регулярно посещают популярные среди детей сайты, соцсети и сообщества, некоторые выдают себя за детей, чтобы обманом втянуть в разговоры и общение;
- Используют собранные о ребенке сведения, чтобы завязать с ним доверительные отношения, в ходе которых ребенок станет легче делиться с ними новой информацией о себе;
- Распространяют сексуально откровенные материалы и могут уговаривать ребенка делиться с ними его интимными фотографиями. Впоследствии преступники могут использовать фотографии ребенка для шантажа и угроз, чтобы встретиться лично или заставить ребенка присылать еще больше своих фотографий и видео;
- Фото и видео интимного характера у ребенка могут попросить и знакомые ему и его родителям люди.

# Полезные советы

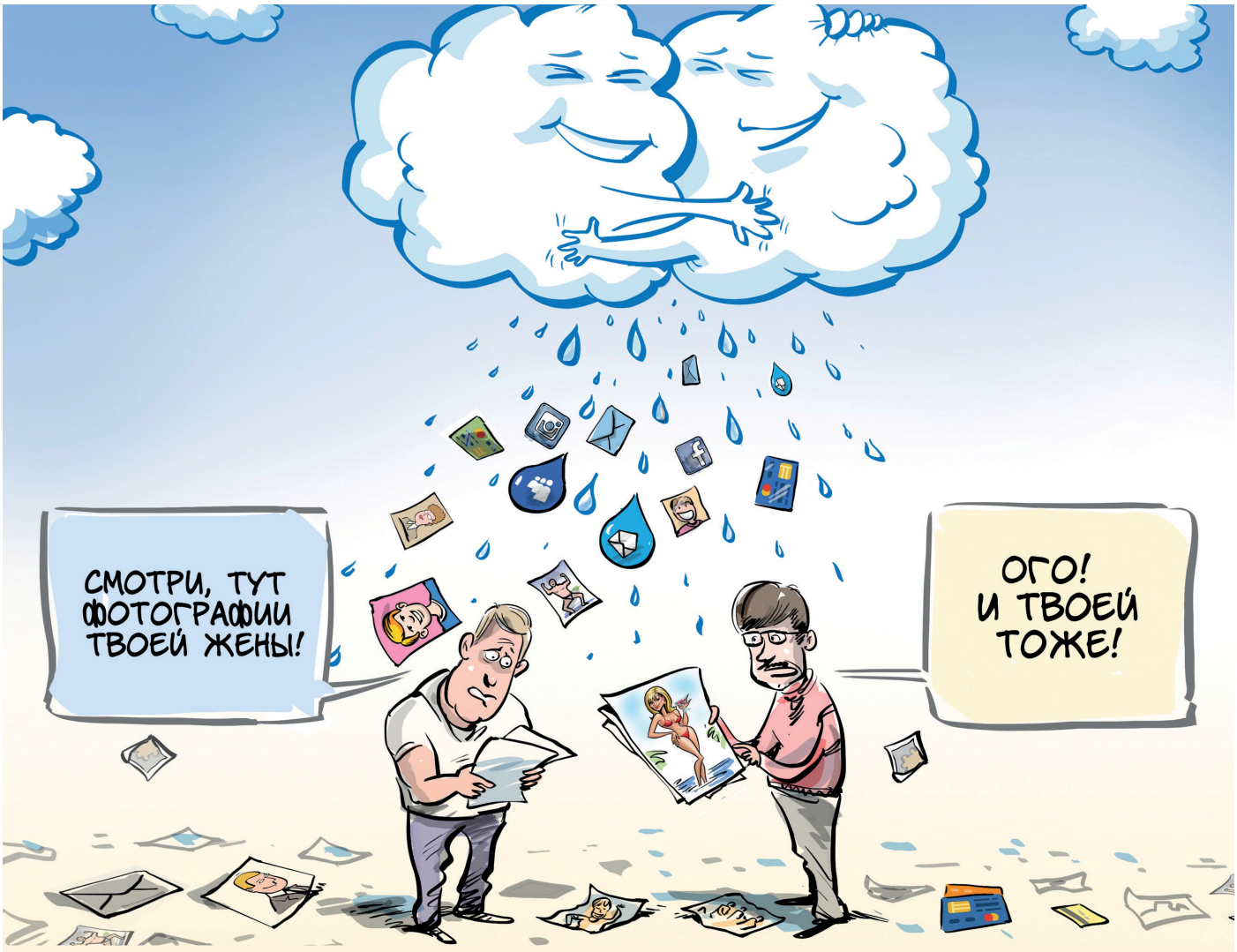
**Если вы обнаружили, что кто-то начинает с вашим ребенком опасное общение, то вы можете предпринять следующие шаги:**

1. Помогите ребенку сделать страницы в соцсетях закрытыми и изменить настройки конфиденциальности. В случае с детьми помладше сделайте это самостоятельно.
2. Договоритесь с ребенком о том, какие публикации разрешено делать на своей странице.
3. Посоветуйте ребенку удалить из друзей и подписчиков тех, с кем он лично не знаком. Если ребенок не уверен в том, стоит ли добавлять того или иного пользователя в друзья, то лучше этого не делать.
4. Разговаривайте с ребенком о том, что в случае неприятной или неловкой ситуации он всегда может к вам обратиться, и вы вместе разрешите ситуацию. Особенно важно, чтобы ребенку было комфортно говорить о неудобных вещах, которые вызывают у него сожаление или стыд.
5. Объясните ребенку, что непристойные сообщения или просьбы от незнакомцев необходимо блокировать и направлять жалобы на них в администрацию сайта или сервиса, а также сообщать родителям.
6. В случае обнаружения нежелательных контактов в соцсетях ребенка и склонения к действиям сексуального характера необходимо сообщить в полицию, прикладывая все имеющиеся доказательства: ссылки на аккаунты незнакомцев, скриншоты переписки и т.д.

**ЗА РАСПРОСТРАНЕНИЕ ДЕТСКОЙ ПОРНОГРАФИИ, А ТАКЖЕ ЗА ДЕЙСТВИЯ СЕКСУАЛЬНОГО ХАРАКТЕРА В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ, ПРЕДУСМОТРЕНА УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ.**

# Личный пример

**Объясните ребенку, что личными данными, а также некоторыми фото и видео изображениями не стоит делиться и со знакомыми людьми, и даже с друзьями. Расскажите о возможных последствиях таких действий. Любые подобные фото и видео изображения могут быть размещены в публичном доступе и нанести психический и эмоциональный вред ребенку. Поясните, что все, что попадает в Интернет, остается там навсегда.**




НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

# ОБЩЕНИЕ С НЕЗНАКОМЦАМИ ОНЛАЙН: ПОЧЕМУ ЭТО ОПАСНО

## Агрессоры в цифровом мире

**Одна из самых больших опасностей в сети – люди, которые по разным причинам могут представлять угрозу для здоровья или психики ребенка. Такие люди зачастую угрожают не только детям, но и взрослым.**

## Кто представляет в Интернете наибольшую угрозу

- **Тролли и агрессоры.** Интернет-травля иногда носит организованный характер, когда группа обидчиков координирует свои действия и может даже иметь единый «центр управления».
- **Шантажисты.** Если информация или материалы личного характера попадают в руки к злоумышленникам, они могут использовать их для шантажа своей жертвы.
- **Вербовщики.** Эти люди ищут среди пользователей сети тех, кого смогут приобщить к каким-то определенным идеям, группам или движениям, зачастую носящим криминальный или экстремистский характер.
- **Манипуляторы.** Воздействуют на эмоции и психику широкой группы пользователей с целью вызвать у них агрессивное поведение или спровоцировать на какие-то действия.
- **Мошенники.** Стремятся похитить у пользователя его персональные данные или финансовые средства. С этой целью используют методы социальной инженерии, манипулируют эмоциями жертвы, а также прибегают к техническим средствам, подделывая сайты, профили и даже номера телефонов.
- **Педофилы.** Входят в доверие к ребенку, иногда маскируясь в Интернете под другого ребенка. Обманом навязывают ему встречу или заставляют его присылать материалы интимного характера.

# Ключевой вопрос

Что такое «Нежелательный контакт»?

## Внимание!

**Нежелательным контактом называется любое общение в Интернете, беспокоящее вашего ребенка, создающее конфликтную ситуацию или обстоятельства, при которых ему может быть причинен вред. Также в сети ребенок может столкнуться с опасными или неуместными материалами, способными расстроить, напугать или обидеть его. 82% детей получают запросы на дружбу в социальных сетях от незнакомых людей, а 29% - от незнакомых взрослых (по данным Лаборатории Касперского)**

## Ребенку следует остерегаться незнакомцев в Интернете, которые:

- Задают много вопросов о его личной жизни.
- Просят об одолжениях в обмен на что-либо.
- Просят никому о них не рассказывать.
- Пытаются контактировать с ребенком множеством различных способов – смс, соцсети, онлайн-чаты и т.п.
- Задают ребенку вопросы о том, кто еще имеет доступ к его телефону, компьютеру или аккаунту.
- Лестно отзываются о внешнем виде ребенка.
- Задают вопросы или делают комментарии личного или интимного характера. 10% детей отмечали, что им приходили странные сообщения от взрослых пользователей.
- Настаивают на личной встрече. 37% детей встречаются с теми, с кем познакомились онлайн.
- Заставляют ребенка чувствовать себя виноватым или угрожают ему.

## Полезные советы

- Расскажите детям, что делать, если им пишет кто-то, с кем они не хотят общаться.
- Уберите учетные записи детей из публичного доступа.
- Настоятельно посоветуйте ребенку удалить контакты людей, с которыми он не знаком лично.
- Договоритесь с детьми, какие данные они могут публиковать в Интернете, а какие нет. Например, фотографии, место жительства, учебы и т.д.
- Ребенку постарше предложите сделать страницы в соцсетях закрытыми для посторонних и подробно изучить настройки конфиденциальности, чтобы он мог контролировать, кто именно будет видеть его фотографии и записи.
- Лучший способ избежать опасного общения в сети – заблокировать человека, который пытается контактировать с ребенком и пожаловаться на его аккаунт администрации соцсети.
- Если вы поймете, что преследование ребенка со стороны незнакомых лиц, его травля или вовлечение в депрессивно-суицидальный контент не прекращаются, а все возможные меры помощи исчерпаны, следует сменить аккаунт ребенка, мобильное устройство и номер его телефона. Желательно на какое-то время полностью исключить ребенка из Интернета, например, пойти в поход с ребенком на несколько дней куда-нибудь, где не будет зоны покрытия сети.

## Это надо знать!

**Очень важно объяснить ребенку, что «виртуальные друзья» должны оставаться виртуальными, но если ребенок хочет встретиться с кем-либо из них, то вы хотели бы, чтобы он делал это с вашего разрешения. Безопаснее всего встречаться днем, в общественном месте и в сопровождении родителей или кого-либо из взрослых, кому ребенок доверяет.**

**Объясните ребенку, что он должен как минимум ставить кого-нибудь из родителей в известность о том, куда он направляется и с кем собирается встретиться.**

## Что делать, если ребенок попал в опасную ситуацию?

- Сохраняйте спокойствие и заверьте ребенка, что его никто не собирается ругать.
- Объясните ему, что даже взрослых иногда обманом заставляют делать то, о чем они потом жалеют.
- Дайте ребенку понять, что он всегда сможет обсудить с вами любой вопрос, не боясь наказания или критики.
- Не лишайте ребенка доступа в Интернет. Это может быть воспринято как наказание, и в дальнейшем ребенок не захочет рассказывать вам о своих проблемах.
- **Если вы считаете, что жизни или здоровью ребенка угрожают, сообщите об этом в полицию по номеру 102.**
- Прежде чем блокировать кого-либо или удалять записи, обязательно заснимите и сохраните доказательства – фото или скриншоты переписок, даты и время записей, ссылки на публикации или аккаунты.
- **Если эти материалы включают в себя интимные изображения детей младше 18 лет, имейте в виду, что хранение и распространение таких изображений является преступлением. Обязательно обратитесь в полицию.**

## Личный пример

**Обсудите с детьми, как они могут реагировать на различные раздражающие ситуации. Они должны понять, что в любой момент могут поговорить с вами, довериться, получить помощь!**

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

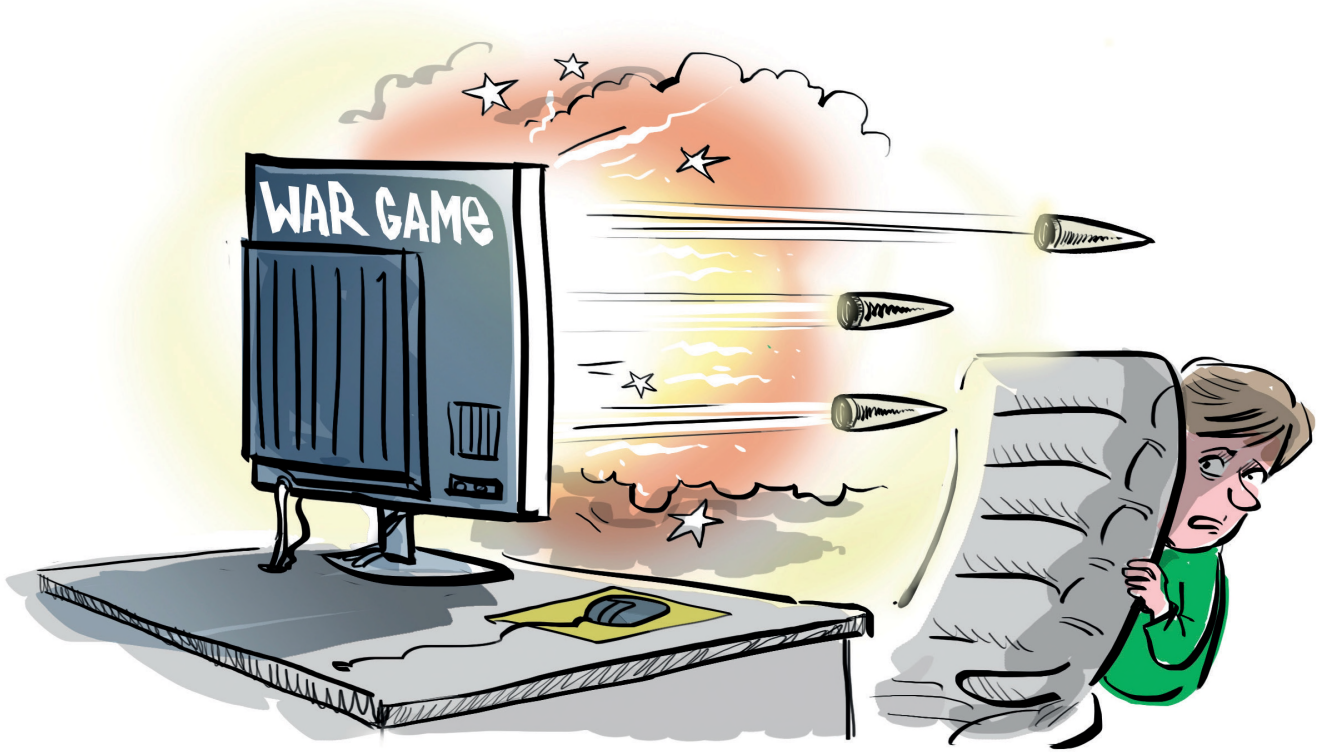
Сайт ligainternet.ru

# ОНЛАЙН-ИГРЫ

**Онлайн-игра – компьютерная игра, главной особенностью которой является необходимость постоянного подключения к сети Интернет. Число игроков в самых популярных онлайн-играх может достигать сотен тысяч пользователей.**

**Для достижения высокого результата в игре пользователям необходимо взаимодействовать между собой. Для этого используются: внутриигровой форум, чат, голосовое общение. Эта особенность онлайн-игр делает их очень популярными среди детей и подростков, но далеко не каждая игра может подойти ребенку по возрасту.**

Многие родители не задумываются в какие игры играют их дети, и не контролируют соблюдение возрастных ограничений, не проверяют с кем они общаются в играх, сутками проводя время за компьютером.




## Какие опасности есть в онлайн-играх?

Жестокие сюжеты – некоторые компьютерные игры, особенно в жанре «стрелялки от первого лица», пропагандируют жестокость и насилие. Видеоигры указанного жанра, изначально разработанные для тренировки сотрудников служб специального назначения для выработки оптимального поведения в экстремальной ситуации, вызывают повышенный интерес у детей и нередко случается, что ребенок хочет повторить сценарий такой игры в реальности. Многие эксперты отмечают, что подростки, планировавшие вооруженные нападения на образовательные учреждения, почти все свое свободное время проводили в онлайн-играх подобного жанра.

**Дети и подростки во внутриигровых чатах, в специализированных приложениях, а также в чатах стриминговых платформ, где обсуждаются онлайн игры (таких как Twitch, Discord) общаются с совершенно незнакомыми людьми и могут стать жертвой агрессии, травли и неприемлемого общения со стороны незнакомых взрослых игроков.**

Во внутриигровых чатах незнакомые взрослые могут отправить ребенку ссылки на мошеннические ресурсы, частные сервера или закрытые группы в соцсетях.

Общение в игровых чатах практически невозможно отследить и контролировать. Этим пользуются провокаторы и преступники, которые ищут в игровых сообществах детей и подростков, поддающихся внушению, и заманивают их в свои преступные схемы.

Многие современные онлайн-игры позволяют создать свой собственный «сервер», в котором можно реализовать любую идею: воссоздать любую точку на земном шаре, либо создать симуляцию боевых действий, причем такой хостинг может находиться в любой точки земного шара. Управляется такой сервер только администратором (модератором), доступ предоставляется исключительно по рассылаемым пользователям ссылкам-приглашениям (инвайтам).

**Администратор такой закрытой платформы, обладая полными правами, распределяет роли, придумывает названия и символику, вводит систему рангов. Для достижения нового ранга может устанавливать условия в виде специальных квестов: «убить определенное количество персонажей другой фракции, похитить их ценности на определенную сумму и т.д.». При выборе названий, с учетом закрытости платформы, администратор может использовать в качестве названий наименования запрещенных в Российской Федерации террористических группировок: «ИГИЛ», «Аль-Каида», «Боко Храм» и другие.**

**Все действия вроде бы совершаются в игровой манере, но параллельно они отпечатываются в сознании ребенка. Подросток радуется тому, что достиг нового ранга в игре, а на самом деле он даже не догадывается, что может быть вовлечен в серьезное преступное сообщество.**

Некоторые игры используют GPS и постоянно собирают информацию о местоположении игрока. А это значит, что и другие участники игрового сообщества могут узнать, где находится ребенок в данный момент.

## Что должны сделать родители, чтобы обезопасить детей?

1. **Изучите онлайн-игры, в которые играет ваш ребенок.** Поищите в Интернете информацию об игре, найдите ее официальный сайт, ознакомьтесь со скриншотами и видео из игры. Обратите внимание, подходит ли игра по возрасту для вашего ребенка. **Обязательно обратите внимание на следующее:**
   - Есть ли в игре модерация? Модераторы – это пользователи, которые следят за тем, чтобы игроки не нарушали установленных правил, будь то правил для общения между игроками или правил самой игры.
   - Содержит ли игра материалы откровенно сексуального или насильственного характера?
   - Есть ли в игре чат с другими игроками? Можно ли его отключить?
   - Существуют ли дополнительные настройки, которые можно отключить или включить для большей безопасности ребенка в игре?
2. **Ознакомьтесь с правилами поведения в игре, а также внутриигровых чатов.** Можете ли вы сообщить о каких-либо неуместных действиях, пожаловаться на оскорбительное поведение других игроков?
3. **Помогите ребенку создать логин и пароль.** Родителям следует внимательно следить и контролировать действия детей в сети.

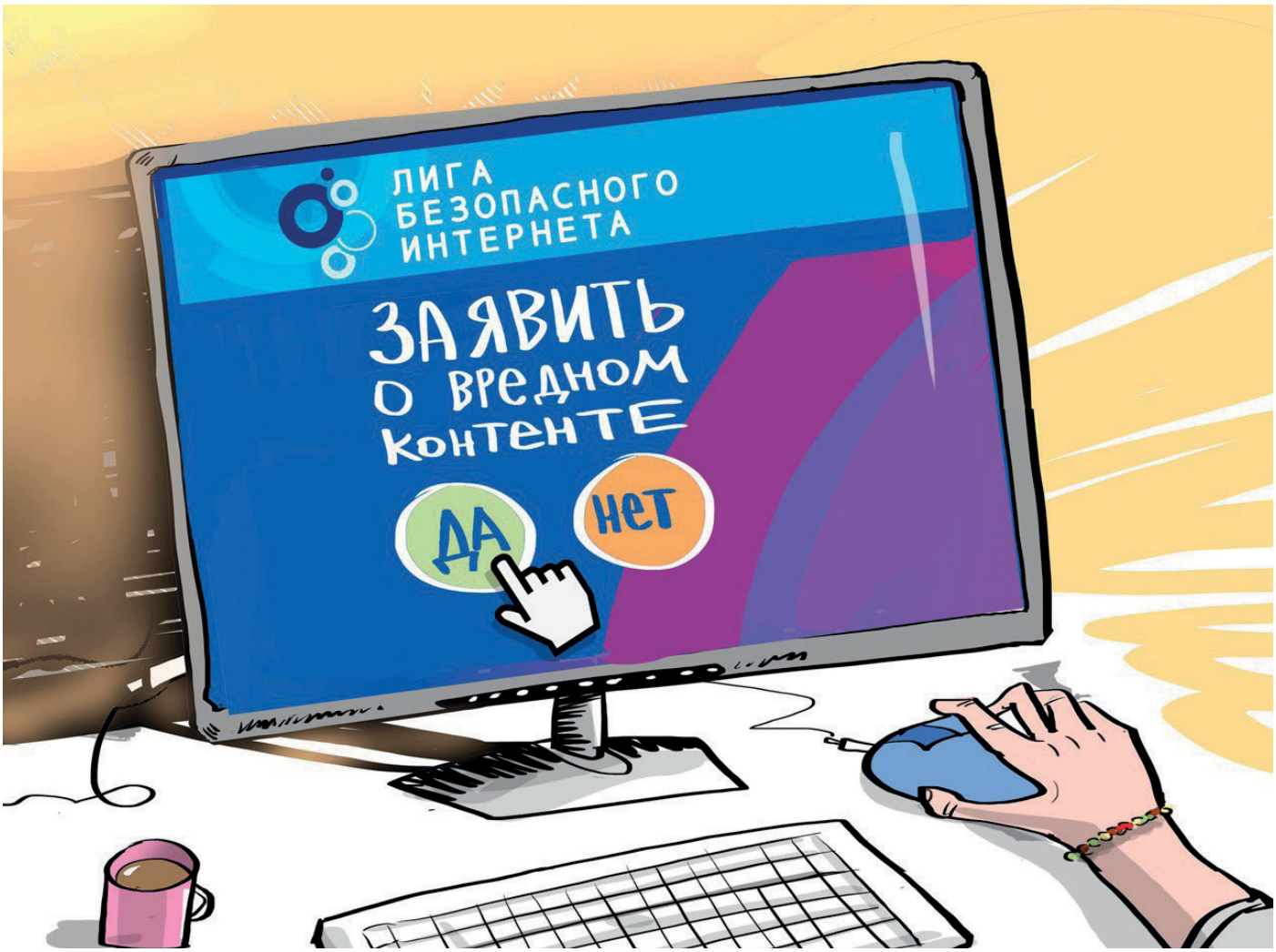
# ОПАСНЫЕ ПУБЛИКАЦИИ В СОЦИАЛЬНОЙ СЕТИ: ПОЧЕМУ НЕЛЬЗЯ ПРОМОЛЧАТЬ!

## 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

# 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».

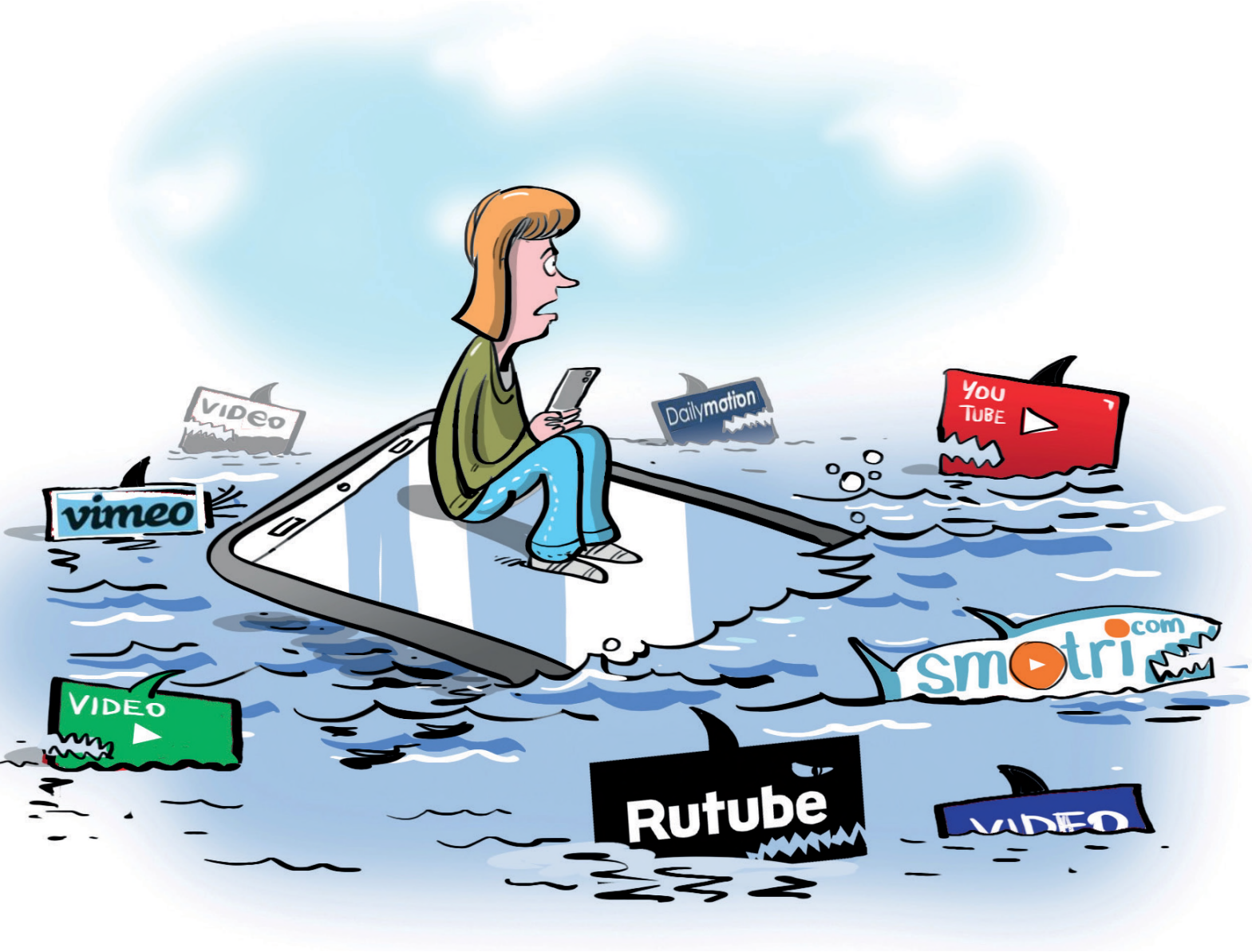
**Сообщества по криминальной идеологии** – продвигают идеалы из криминальной среды среди подростков. Наиболее известным примером является движение АУЕ (признано экстремистским и запрещено на территории Российской Федерации). В таких сообществах романтизируется не только криминальный, но и тюремный образ 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 аккаунта, 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 том числе, семейные ценности; содержащих пренебрежительные/неуважительные высказывания по отношению к родителям, деторождению, служению Отечеству, исторической памяти народа России, ценности жизни человека, руководству страны и принимаемым решениям.
- Наличие в подписках у подростка или в ленте новостей его аккаунта сообществ, посвященных 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 кем проводит время, при этом вы не знаете телефонов его друзей и их родителей, его успеваемость в школе упала.
- У ребенка появились денежные средства или дорогие вещи, происхождение которых вы не знаете или он пользуется вещами, которые ему, якобы, дал временно поносить товарищ.

# Последствия вовлечения в деструктивные движения

- **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 вербовщики используют своеобразную «Воронку вовлечения».**

# Как это работает?

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.

## 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

# ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЦЕНИМ И УМЕЕМ СОХРАНЯТЬ!

## Что надо знать о персональных данных

**Персональные данные – все данные о человеке, своего рода «паспорт его личности». Их следует тщательно беречь и не раскрывать в Интернете без необходимости. В противном случае это может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям. Безопасность – это наша непререкаемая ценность для детей и взрослых!**

## Что относится к персональным данным?

1. Фамилия, имя, отчество;
2. Номера и реквизиты всех документов (паспорт, СНИЛС, ИНН, свидетельство о рождении, аттестат об образовании, медицинский полис и т.п.);
3. Банковские данные (номер счета, карты, пин-код, CVV-код и т.п.);
4. Ваша контактная информация (номера телефонов, адреса электронной почты, адреса жительства, работы или учебы);
5. Фотографии и видеозаписи с вашим изображением;
6. Данные о ваших родственниках;
7. Ваши логины и пароли.

## Ключевой вопрос:

Насколько реально и как сохранить персональные данные вашей семьи?

## Внимание!

**Более трети россиян (37%) не знают, для чего и как могут быть использованы персональные данные (по данным ВЦИОМ)!**

Соцсети, мессенджеры и видеохостинги ежедневно собирают о нас огромное количество данных. Делается это, в первую очередь, для заработка денег. Большинство крупных платформ – бесплатны, ведь их владельцы зарабатывают на своих пользователях. Точнее – на их персональных данных, при перепродаже или использовании в рекламе. Соцсети и мессенджеры берут эти данные не только из профиля пользователя, но и из его переписки. Обратите внимание: вся переписка постоянно хранится на серверах социальной сети или мессенджера, поэтому в результате утечки, кражи или хакерской атаки ваша частная жизнь может стать достоянием общественности.

## Источники беды

Не стоит надеяться на «приватные» публикации, просматривать которые может только ограниченный круг лиц, которых настраивает сам пользователь. Ведь утечка может произойти через любого из этих людей. Иногда происходят крупные утечки, в результате чего данные тысяч пользователей попадают в открытый доступ. Но чаще всего пользователи сами выкладывают информацию о себе в Интернет. Защитите себя и свою семью! 80% информации о жертвах преступники находят в социальных сетях (по данным Роскомнадзора).

Кроме персональных данных о каждом человеке собираются также его фото- и видеоизображения. Современного человека ежедневно снимают сотни видеокамер, расположенных в публичных местах. Эта информация собирается, в первую очередь, государственными органами с целью обеспечения безопасности, раскрытия преступлений и т.п. Однако следует помнить, что такие видеозаписи могут попасть и в руки к шантажистам или иным злоумышленникам. Будьте осторожны! Не помогайте мошенникам, добровольно передавая им персональные данные.

В текущей ситуации большинство порталов органов власти и коммерческих компаний становятся объектами хакерских атак в ежедневном режиме.

**Так, за последнее время в публичный доступ утекли базы данных пользователей компании «Яндекс.Еда» и клиентов медицинской лаборатории «Гемотест». Все это происходит из-за того, что в России до сих пор нет существенной административной и уголовной ответственности для операторов подобных баз. Так, «Яндекс.Еда» «отделалась» штрафом всего лишь в 60 тысяч рублей.**

**Важно помнить, что из-за халатности или экономии компании на хранении данных, которые мы оставляем, оформляя карточку в магазине, на заправке или любом другом месте могут стать достоянием общественности.**

## Надо помнить!

Активный пользователь Интернета оставляет цифровой след – иногда свой полный портрет: состояние здоровья, внешность и физические данные, привычки, места пребывания, уровень дохода, данные о личной и интимной жизни и многое другое. Приложения на телефоне могут получить доступ микрофону, камере, акселерометру (используется для измерения движений устройства) и следить за своим пользователем круглосуточно. Всё это может представлять интерес для преступников! Мошенничество, шантаж, травля – вот неполный список того, для чего злоумышленники могут использовать информацию о пользователях. Следите за культурой поведения в сети, сохраняйте свою частную жизнь и конфиденциальность!

**В соответствии с действующим законодательством любой гражданин вправе отказаться от предоставления своих персональных данных. Согласие на обработку персональных данных может быть отозвано гражданином у организации в любой момент.**

**Если вас принуждают к подписанию согласия на обработку персональных данных и отказывают в предоставлении услуги, смело обращайтесь в прокуратуру.**

# Полезные советы

1. Посоветуйте своему ребенку при регистрации в социальных сетях использовать только имя или псевдоним (никнейм).
2. Следите за тем, чтобы ребенок не размещал в интернете лишнюю информацию: где он живет, где учится, какой дорогой ходит на уроки и т.п.
3. В настройках камеры на телефоне следует отключить геотеги (геолокацию, место съемки). Эта функция показывает, где именно делалась фотография. В таком случае любой желающий по фото может отследить пользователя.
4. Полезно будет настроить приватность в аккаунте своего ребенка. Таким образом его профиль смогут смотреть только его друзья.
5. Объясните ребенку, что нельзя выкладывать в Интернет фото или скан-копии его документов или банковских карт.
6. Расскажите ребёнку, что персональными данными стоит делиться только с ограниченным кругом лиц – самыми близкими. Не стоит передавать такие данные друзьям, а особенно незнакомым людям из соцсетей.
7. Ребёнку надо знать, что злоумышленники могут пытаться выведать информацию и персональные данные через личные сообщения в социальных сетях. Особенно внимательно стоит реагировать на ссылки, которые незнакомцы присылают ребёнку в личных сообщениях. Лучше по ним не переходить, а неизвестные файлы – не открывать.
8. Расскажите ребенку, что нельзя подключаться к первому попавшемуся бесплатному Wi-Fi в публичном месте. Через такую бесплатную сеть злоумышленники могут получать доступ к персональным данным пользователей.

# Личный пример

**Тщательно отбирайте фото и видео, которые вы сами выкладываете в Интернет!**

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru