

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.

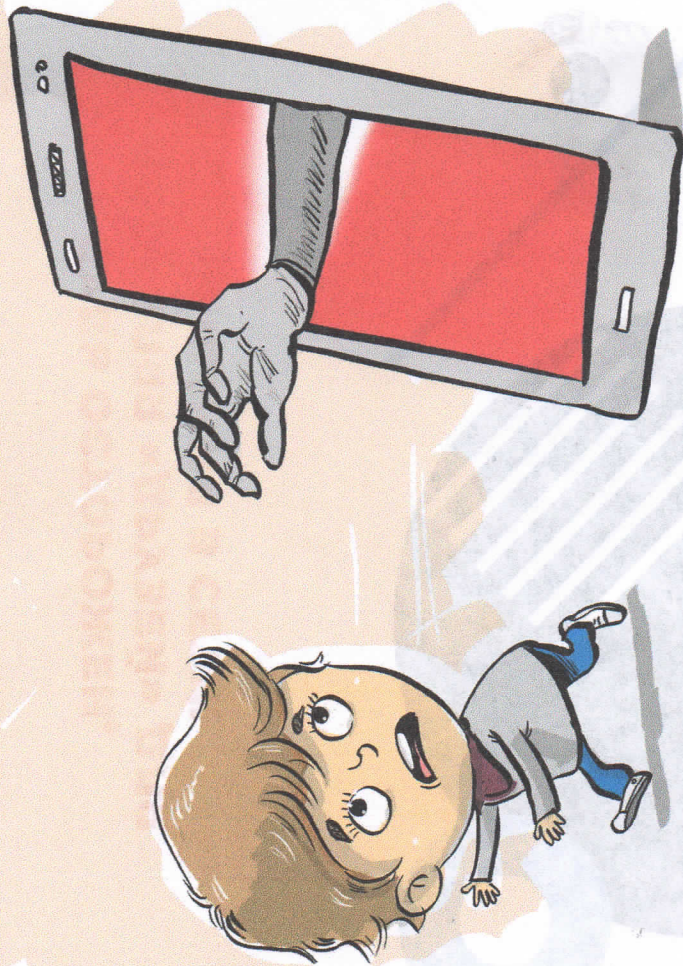
Существует несколько подсказок, при помощи которых можно точно понять, настоящий это сайт или сайт-подделка:

- 1. Проверь 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 односторонними 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 получают доступ к твоему профилю в соцсети, то они получают 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 удастся поймать. Однако вернуть средства гораздо сложнее.

ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ



ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

Интернет – это возможность общаться с друзьями на расстоянии, не теряя 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 предложить 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 встречался 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:

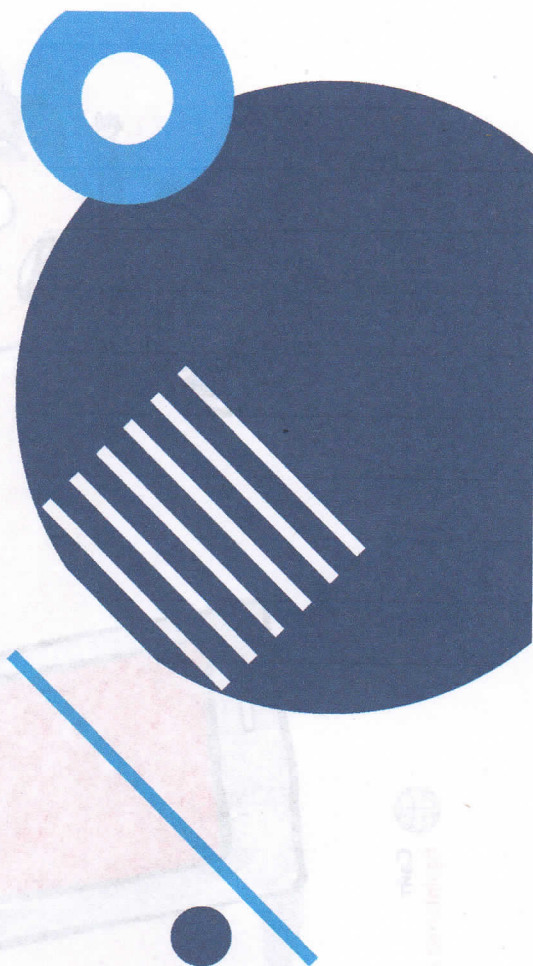
1. Страницы в социальных сетях лучше закрыть от посторонних. Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои личные данные от попадания в руки преступников. Как правило, информацию о себе, своих увлечениях, хобби, фото с друзьями и многое другое мы публикуем в соцсетях.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



ЦИФРОВОЙ СЛЕД



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ



лига
безопасного
интернета



Сайт
ligainternet.ru

Внимательно посмотри на свой телефон. Ты знаешь, что современные смартфоны – те же самые компьютеры? Они обладают такими же функциями, а в чем-то даже превосходят компьютеры или ноутбук. Наши телефоны включены круглосуточно. И все это время они собирают о нас информацию. Больше всех информацию собирают приложения соцсетей и мессенджеров. Фото, видео, история переписок, хобби и увлечения, даже места, в которых ты бываешь – все это приложения собирают и хранят. А все, что однажды попало в Интернет, остается там навсегда и удалить это невозможно.

ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ ВСЯ ЭТА ИНФОРМАЦИЯ?

1. **Соцсети, поисковые сайты, Интернет-магазины и прочие крупные Интернет-ресурсы собирают данные для того, чтобы потом показывать своим пользователям рекламу.** Чем точнее реклама попадает в интересы и увлечения каждого конкретного пользователя, тем она качественнее и дороже.
2. **За этими данными охотятся злоумышленники.** Они могут использовать их для того, чтобы как можно больше узнать о жертве, выяснить, где человек работает, в каком банке у него открыт счет, как его зовут и так далее.
3. **Соцсети собирают информацию буквально о каждой твоей активности.** Под какими постами ты ставишь лайки, сколько времени ты читаешь новость, какие заголовки тебе нравятся больше, с какими людьми ты дружишь и общаешься, какую музыку ты слушаешь, какие видео тебе нравятся. У соцсетей есть информация даже о том, что ты ешь и какие фото отправляешь друзьям.

Вся эта информация называется цифровым следом, который каждый из нас оставляет в сети. Невозможно пользоваться Интернетом и не оставлять след. Даже если ты решишь ничего не публиковать, ничего никому не писать, в любом случае прочитанные и просмотренные посты будут формировать длинную историю твоей активности. Этот след уникален для каждого человека, двух одинаковых быть не может. О каждом из нас в Интернете настолько много информации, что можно создать настоящего цифрового двойника.

В Интернете, как и в реальной жизни, нужно быть очень внимательным со своими словами и действиями. Особенно осторожно следует относиться к публикуемым и пересылаемым личным фотографиям. Ни в коем случае никому не отправляй фотографии интимного характера! Из Интернета, как мы помним, ничего не удаляется. Всегда помни: чем меньше мы используем гаджеты – тем лучше!

ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!

ПОКУПКИ И ПЛАТЕЖИ В ИНТЕРНЕТЕ: основные правила безопасности

Уже много лет пользователи во всем мире пользуются онлайн-платежами. Это удобно: можно не тратить время на поход в магазин, долгий поиск товаров на полках. На сайтах или в приложениях интернет-магазинов вам доступен весь ассортимент товаров с простым механизмом поиска и возможностью заказать их прямо на дом.

Однако, онлайн-услуги удобны не только для покупателей, но и для преступников!



Внимание!

- **Мошенники создают «зеркальные» сайты** – копии реально существующих магазинов, которые практически идентичны настоящим, предоставляющим возможности приобретения качественных товаров. Мошенники, используя всего лишь одну лишнюю цифру или букву, иные символы, похищают деньги или данные невнимательных пользователей.
- **Участились случаи, когда на разных торговых площадках мошенники регистрируются в качестве продавца**, предлагают товары, получают заказы на них. После того, как покупатель оплачивает товар, мошенник сообщает, что товар закончился. Покупателю возвращается уплаченная сумма, а взамен приходит ссылка на сторонний сайт, где этот товар можно приобрести по скидке. Если купить что-то на таком сайте, то вместо желаемого товара могут прислать бракованный или просто пустые коробки.

Ни одна компания не будет продавать свои товары по невыгодным ценам. Мошенники используют скидки и распродажи, чтобы заманить доверчивых пользователей на свои сайты.

Правила безопасности

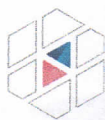
- **При любой покупке в Интернете будьте бдительными**, подробно и внимательно изучите сайт, его название и указанный адрес, сравните его с официальным названием той организации, где желаете купить товары и услуги.
- **Не переходите ни по каким случайным ссылкам.**
- **Не оставляйте данные** своей банковской карты на подозрительных сайтах.
- **Приобретайте билеты на самолет или поезд только на официальных сайтах** авиакомпании или железнодорожной компании.
- **Изучайте отзывы** о продавце, внимательно смотрите, когда он был зарегистрирован на сайте, торговой площадке, проверяйте даты отзывов о нем. Например, если он зарегистрирован сегодня, а отзывы написаны в этот же день или спустя непродолжительное время, то явно отзывы написаны им самим, а не реальными покупателями.
- **Общаясь с продавцом, расспросите**, как будет доставлен товар, в какой упаковке, уточните полное описание товара, что также поможет узнать о его качестве.
- **Сохраняйте всю переписку** и контакты продавца, запишите название сайта. Указанные сведения помогут правоохранительным органам поймать мошенников, если вы попадете в их ловушку.

Нет никаких гарантий, что при онлайн покупке заказанный товар окажется качественным. Внимательно проверяйте отзывы о таких «магазинах» в сети!

Мошеннические схемы в социальных сетях

- **Мошенники, взломав страницы ваших близких, друзей, знакомых, от их имени рассылают сообщения о том, что оказались в трудной ситуации, и просят занять денег.** Любые деньги, которые вы отправите, поступают на банковские счета мошенников. Лучшим решением в данном случае будет звонок вашим друзьям, близким, чтобы выяснить, какие у них проблемы и нужна ли им реальная помощь. Они ведь могут даже не знать, что мошенники используют их страницу для сбора денежных средств.
- **Многие из «онлайн продавцов» не имеют юридического лица или законных оснований для ведения торговли.** Они, чаще всего, просят пользователя перевести денежные средства на личную банковскую карту – в результате пользователь остается без желанной покупки и без денег.
- **Используя сайты, будьте внимательны, не оправляйте и не публикуйте свои фото или видео, которыми потом можно вас шантажировать.** Знакомясь с кем-либо в Интернете, помните, что вы не видите собеседника, им может быть совершенно не тот человек, который изображен на опубликованных им фото. Зачастую мошенники входят в доверие, начинают просить деньги на лечение или билеты.

Будьте бдительны при общении в социальных сетях!



**НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ**
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ



**лига
безопасного
интернета**



Сайт
ligainternet.ru



**СЛЕДСТВЕННЫЙ ДЕПАРТАМЕНТ
МВД РОССИИ**

СЛУЖИМ РОССИИ, СЛУЖИМ ЗАКОНУ!

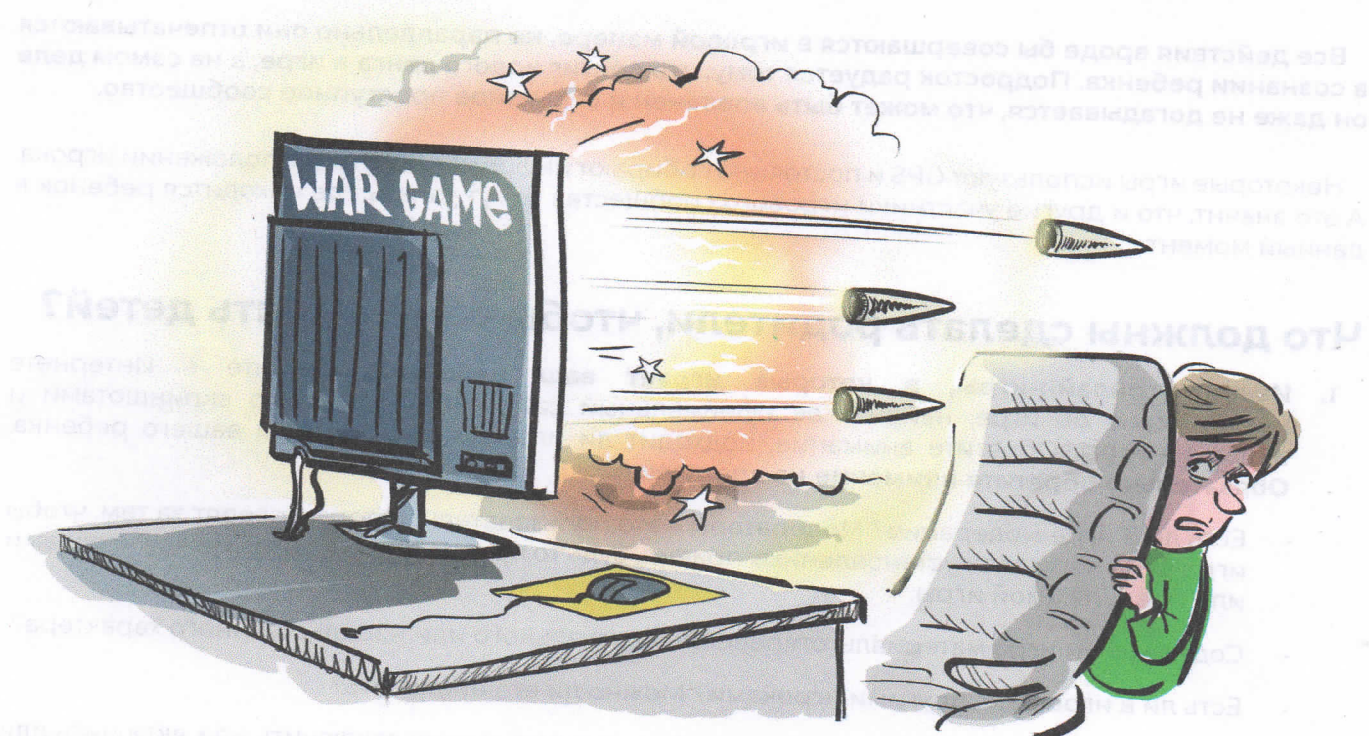


ОНЛАЙН-ИГРЫ

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.



**НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ**
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ



**лига
безопасного
интернета**



Сайт
ligainternet.ru

