Внимание!!! Информацию о выявленных интернет – сайтах, социальных сетях, распространяющих запретный контент, Вы можете направить на сайт <http://rkn.gov.ru/> в раздел «Единый реестр запрещенной информации» (<http://eais.rkn.gov.ru/feedback/>)

Интернет риски для детей

В интернете есть много полезного и интересного, но вместе с тем в онлайне дети рискуют столкнуться с неприятностями. От некоторых угроз их может оградить ненавязчивый «родительский контроль», но обучение цифровой грамотности – насущная необходимость.

**НЕБЕЗОПАСНЫЙ ГЕЙМИНГ**

Под видом фальшивых приложений и на ненастоящих или «серых» игровых сайтах ребенка (и взрослого) поджидают «традиционные» киберугрозы в виде вредоносных программ и онлайн-мошенничества. 

По данным «Лаборатории Касперского», число атак на мобильных пользователей, когда злоумышленники мимикрировали под популярную игру, в частности Brawl Stars, в первом полугодии 2022 года увеличилось в 1,5 раза по сравнению с аналогичным периодом в 2021 году, а под Roblox – почти в четыре раза.

Ребенок должен понимать, что, скачивая различные подозрительные файлы с просторов Сети, он может столкнуться с вредоносными или нежелательными программами. И тогда как минимум будет нанесен вред устройству, а как максимум – украдены [конфиденциальные данные](https://rskrf.ru/tips/eksperty-obyasnyayut/personalnye-dannye-kak-novaya-valyuta/)– имя, адрес, платежная информация и т. д.

Решение:

Расскажите ребенку, что игры нужно скачивать только из официальных источников и что не стоит кликать на все подряд. Нередки случаи, когда подростки в игровом чате видят предложения перейти по «волшебной» ссылке, чтобы бесплатно получить внутриигровые предметы или усиление аккаунта, а ссылка на самом деле ведет на [фишинговый сайт](https://rskrf.ru/tips/eksperty-obyasnyayut/fishing/" \o "https://rskrf.ru/tips/eksperty-obyasnyayut/fishing/).

**ДОКСИНГ**

Сегодня набирает обороты такое явление, как доксинг , когда недоброжелатели намеренно ищут и публикуют личную информацию о человеке со злым умыслом. Для этого доксеры собирают личные данные, в том числе и те, что люди сами размещают на страницах соцсетей.

Согласно опросу, проведенному «Лабораторией Касперского», 13% школьников выкладывают фотографии, на которых видно обстановку квартиры, 12% указывают в соцсетях имена родственников и родителей, а 10% публикуют номер телефона. К сожалению, такая информация может оказаться привлекательной для злоумышленников.

Решение:

Вместе с ребенком зайдите в настройки профиля, чтобы выставить максимальные настройки приватности, а также объясните ему, какую информацию и фотографии не стоит размещать в соцсетях.

Важно осознать самим, что излишняя откровенность в Сети еще никому не приносила пользы. Расскажите ребенку, что любая личная информация о нем и его семье на руку только злоумышленникам. Неважно, будет ли это номер телефона или школы, большое количество фотографий или геометки, – чрезмерная открытость чревата последствиями.

**КИБЕРБУЛЛИНГ**



Обидные сообщения или угрозы, распространение ложной информации о человеке – все это примеры онлайн-травли. Дети могут столкнуться с ней в социальных сетях, мессенджерах, на игровых платформах и не только. Последствия кибербуллинга могут быть тяжелыми – от негативных эмоций и вплоть до депрессии.

Опасно и то, что во многих случаях кибербуллинг возникает и продолжается не только в виртуальной реальности, но может переходить в офлайн, в том числе в формат личного общения между подростками.

Ситуация осложняется тем, что дети зачастую не хотят делиться с родителями аспектами своей цифровой жизни и скрывают, что происходит с ними в Сети.

Решение:

Важно договориться с ребенком, чтобы он обязательно поделился с вами, если в Сети кто-то стал ему угрожать, шантажировать его, что-то вымогать или вести себя оскорбительно. Для этого необходимо выстраивать доверительные отношения в семье и интересоваться онлайн-жизнью ребенка. Его важно предупредить о том, что с интернет-травлей может столкнуться любой, вне зависимости от возраста, интересов или внешности, – в этом случае следует сразу прекратить всякое общение с обидчиками. Также ребенку нужно знать, что часто злоумышленники в интернете могут выдавать себя за тех людей, которыми они не являются.  
Признаком того, что ребенок подвергается кибербуллингу, может стать внезапное удаление своей страницы в соцсетях и явные изменения в поведении, эмоциональном и физическом состоянии, ухудшение успеваемости в школе.

**ОПАСНЫЙ И НЕ ПОДХОДЯЩИЙ ДЛЯ ДЕТЕЙ КОНТЕНТ**

Сцены насилия, употребления алкоголя и наркотиков, нецензурная лексика – все это не для детских глаз и ушей, однако вместе с позитивным и полезным интернет изобилует и подобным видом контента. Не зря на фильмах, роликах и компьютерных играх ставится отметка «18+». Родителям стоит обращать на нее внимание, а еще лучше – быть в курсе, во что играют и что смотрят их дети. Хотя бы в общих чертах.

Решение:

Запрещать ребенку проводить время онлайн или излишне ограничивать его – не выход. Поговорите с ребенком, проведите аналогии с реальной жизнью. Например, многие знают, что нельзя никуда уходить с посторонними или переходить дорогу на красный свет. Такие же правила действуют и в цифровом мире. Не отвечать незнакомцам, не переходить по подозрительным ссылкам, критически относиться к крайне щедрым или пугающим

сообщениям.

**ОПАСНЫЕ НЕЗНАКОМЦЫ**



Социальные сети – важный элемент социализации детей. Там, так же как и в жизни, встречаются разные люди, и не всегда у них благие намерения. Сегодня актуальна угроза онлайн-груминга – когда взрослый человек пытается установить доверительные отношения с ребенком и встретиться в реальной жизни или получить приватные фотографии или видео, в том числе для дальнейшего шантажа.

По данным проведенного «Лабораторией Касперского» опроса, 79% детей получают заявки в друзья от незнакомых людей. В 23% случаев это заявки от взрослых. В группе риска дети 7–10 лет.

Решение:

Проверьте, что на странице вашего ребенка в социальных сетях нет номера школы, где он учится, номера телефона, информации о родителях, а сам профиль закрыт для посторонних. Интересуйтесь у ребенка, с кем и о чем он общается онлайн, при этом важно соблюдать баланс и не запугивать его или излишне контролировать.

**РЕКОМЕНДАЦИИ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ**

* когда ребенок только начинает осваивать цифровое пространство, стоит воспользоваться программами родительского контроля, но прежде рассказать юному пользователю об этом – для чего родители ставят такую программу;
* используйте надежные защитные решения на всех устройствах (в том числе на смартфонах);
* обратите внимание на настройки приватности в социальных сетях: не публикуйте слишком много личной информации – и детей научите тому же;
* проверьте, что на странице вашего ребенка в социальных сетях нет номера школы, где он учится, номера телефона, информации о родителях, а сам профиль закрыт для посторонних;
* используйте надежные пароли: минимум 12 символов с буквами в разном регистре, цифрами и спецсимволами;
* настройте двухфакторную аутентификацию в тех сервисах, которые это позволяют;
* не открывайте вложения из подозрительных писем или сообщений в мессенджерах и соцсетях и не переходите по ссылкам из них;
* скачивайте приложения только из официальных ресурсов;
* проверяйте адрес сайта перед тем, как вводить на нем личные или платежные данные;
* если столкнулись с кибербуллингом, не вступайте в диалог с обидчиком, заблокируйте его, сообщите о травле администраторам площадки.