

ТОП угроз в сети Интернет

В Интернете есть много полезного и интересного, но вместе с тем в онлайн пространстве любой может столкнуться с неприятностями. От некоторых угроз их оградить ненавязчивый «родительский контроль» или антивирусы, но обучение цифровой грамотности сегодня – насущная необходимость. Какие именно опасности подстерегают в Интернете и как их избежать, вы можете ознакомиться ниже.

НЕБЕЗОПАСНЫЙ ГЕЙМИНГ

Под видом фальшивых приложений и на поддельных игровых сайтах поджидают «традиционные» киберугрозы в виде вредоносных программ и онлайн-мошенничества. Важно понимать, что, скачивая различные подозрительные файлы с просторов Сети, мы можем столкнуться с вредоносными и мошенническими программами. И тогда, как минимум, будет нанесен вред устройству, а как максимум – украдены конфиденциальные данные – имя, адрес, платежная информация и т. д.



Решение:

Игры и приложения необходимо скачивать только из официальных источников и не стоит кликать на все подряд на экране, чтобы не запустить вредоносные ссылки. Нередки случаи, когда в игровом чате появляются заманчивые предложения перейти по «волшебной» ссылке, чтобы бесплатно получить внутриигровые предметы или усиление аккаунта, а ссылка на самом деле ведет на фишинговый сайт.

КИБЕРБУЛЛИНГ

Обидные сообщения или угрозы, распространение ложной информации о человеке – все это примеры онлайн-травли. Столкнуться с ней можно в социальных сетях, мессенджерах и даже на игровых платформах. 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 формате личного общения между людьми. Ситуация осложняется тем, что подростки зачастую не хотят делиться с родителями аспектами своей цифровой жизни и скрывают, что происходит с ними в Сети, а родители не придают значения жалобам ребенка на травлю в виртуальном пространстве.

Решение:

Важно чтобы ребенок не боялся поделиться с взрослыми, если в сети кто-то стал ему угрожать, шантажировать его, что-то вымогать или вести себя оскорбительно. С интернет-травлей может столкнуться любой, вне зависимости от возраста, интересов или внешности, – в этом случае следует сразу прекратить всякое общение с обидчиками, сохранить все переписки. Возможно, потребуется обращение в правоохранительные органы.

ТОП угроз в сети Интернет

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 своих страницах соцсетей.

Решение:

Зайдите в настройки своих профилей в социальных сетях и мессенджерах, чтобы выставить максимальные настройки приватности. Помните, что не стоит размещать в социальных сетях личные фото и видео, а также фото и видео с участием ваших друзей. Важно осознать самим, что излишняя откровенность в сети еще никому не приносила пользы. Любая личная информация о себе или своих родственниках на руку только злоумышленникам. Неважно, будет ли это номер телефона или школы, большое количество фотографий или геометки, – чрезмерная открытость чревата последствиями.

МОШЕННИЧЕСТВО

В современном мире все чаще встречаются мошеннические действия в сети Интернет, когда злоумышленники используют различные способы для получения выгоды за счет других пользователей. Такие действия включают в себя фишинг, кражу личных данных, создание поддельных интернет-магазинов и множество других уловок, направленных на обман.

Решение: Не стоит переходить по подозрительным ссылкам, раскрывать свои пароли, номера карт и другую личную информацию. Настройте двухфакторную аутентификацию на всех аккаунтах, чтобы повысить уровень защиты. Научитесь проверять подлинность сайтов и продавцов, перед тем как совершать покупки в интернете. Помните, что предосторожность и внимательность – ключ к безопасности в сети.

ОПАСНЫЕ НЕЗНАКОМЦЫ

В социальных сетях, так, 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 с ним в реальной жизни или получить приватные фотографии или видео, в том числе для дальнейшего шантажа.



Решение:

Проверьте, что на вашей странице в социальных сетях нет номера школы, где вы учитесь, номера телефона, информации о родителях, других личных данных, а сам профиль закрыт для посторонних. Не стоит излишне доверяться собеседникам в Интернете, особенно, если не вы начали общение. Если собеседник становится излишне навязчивым, или агрессивно требует что-то от вас – прекратите это общение, возможно придется заблокировать этого пользователя.