Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников?

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;

2. Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;

3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно.

Предупреждение столкновения с вредоносными программами:

Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.

Периодически старайтесь полностью проверять свои домашние компьютеры.

Делайте резервную копию важных данных.

Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Как защитить детей от негативной информации?

Правило №1 Родители должны знать интересы и цели детей, которые используют сеть Интернет.

Правило №2 Рекомендуется допускать использование сети Интернет детьми в присутствии взрослых. Доступ к данному информационному ресурсу должен быть эффективным и безопасным.

Правило №3 Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Российской Федерации, может оказать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.).

Правило №4 В случае самостоятельного доступа детей к сети Интернет, родители должны контролировать использование информации несовершеннолетними. О характере и объеме информации, полученной детьми в интернет – ресурсах, необходимо узнавать в «Журнале обозревателя» программы "Internet Explorer" . Как ограничить доступ детей к негативной информации в сети Интернет? С целью ограничения доступа детей к «вредным» материалам родители и другие члены семьи могут установить на компьютеры программу «Касперский Интернет секьюрити 2010»: в настройке программы применить вкладку «Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков.

Информируйте ребенка о возможностях и опасностях, которые несет в себе сеть:

Объясните ребенку, что в Интернете как в жизни встречаются и "хорошие", и "плохие" люди. Объясните, что если ребенок столкнулся с негативом или насилием от другого пользователя Интернет, ему нужно сообщить об этом близким людям.

Объясните ребенку, что размещать свои личные данные (адрес, телефон, место учебы) в социальных сетях и других открытых источниках нежелательно и даже опасно.

Научите ребенка искать нужную ему информацию и проверять ее, в том числе с Вашей помощью.

Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернет, особенно путём отправки sms, - во избежание потери денег.

Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться Ваш ребенок, и посоветуйте их использовать.

Объясните, что нежелательно переходить по ссылкам в Интернете. Доказано, что за 6 кликов можно перейти от "белого" сайта к "чёрному".

Научите ребенка самостоятельно вносить адрес в адресную строку браузера. Это позволит избежать сайтов-клонов.