КАК ЗАЩИТИТЬ ДЕТЕЙ ОТ ТЕЛЕФОННЫХ И ИНТЕРНЕТ-МОШЕННИКОВ?

Дети и подростки часто становятся жертвами телефонных и интернет-мошенников в силу своей наивности, неосведомленности и недостаточности навыка критического мышления.

Мошенники же в своих уловках становятся всё более изобретательны: взламывают социальные сети, отправляют фишинговые ссылки, используют нейросети с имитацией голоса и личности знакомых, генерируют скрипты для общения с жертвой.

Защитить детей от цифрового шантажа возможно наладив доверительное общение в семье, развивать эмоциональный и социальный интеллект, заниматься просвещением о кибербезопасности в школе на уроках и используя технические средства, например, программы родительского контроля.

Задача взрослых ознакомить ребенка с правилами цифровой гигиены и безопасности.

Доверительные отношения в этом вопросе стоят на первом месте: потому как, даже если ребенок уже попал в неприятную ситуацию, ему будет проще и легче с ней

справиться, если он будет уверен в том, что родители отнесутся с пониманием, примут сторону ребенка, встав на его защиту и не будут его ругать и обвинять.

Общайтесь с ребенком на тему времени, проведенном в интернете, интересуйтесь в какие игры он играет, спрашивайте про обновления этих игр. Зачастую дети и подростки попадают на крючок к мошенникам тогда, когда хотят приобрести улучшения в игре, или купить дорогостоящую покупку по привлекательной цене, контрафактные телефон, наушники или одежду.

Объясните детям, что существуют сайты-двойники, что деньги на карте – это не бездонная бочка, что покупка игровой валюты в игре – это не первая необходимость. Связывайте счета детей и свои, подключайте смс- и пуш-уведомления о покупках, так вы сможете видеть траты.

КАК ЗАЩИТИТЬ ДЕТЕЙ ОТ ТЕЛЕФОННЫХ И ИНТЕРНЕТ-МОШЕННИКОВ?

Интернет-это новый вид коммуникаций и в современном мире процесс социализации происходит в том числе через него. Поэтому полностью изолировать ребенка от гаджетов и интернета вряд ли удастся, но стоит объяснить некоторые правила безопасности нахождения в киберпространстве и не просто установить галочки в приложении родительского контроля, а ввести в ручную все нежелательные для посещения ребенком ресурсы.

Системы контроля гаджетов бывают разные. Настроить можно нативную систему, которая предложена на самих устройствах, например, Google Family Link на Android или контроль экранного времени на iPhone.

Еще один тип родительского контроля – это системы фильтрации данных, например, Яндекс DNS. Для роутеров мобильных устройств и компьютеров разных операционных систем есть свои настройки, как можно включить DNS в формате семейной фильтрации. Это позволяет отсечь неприемлемую информацию в автоматическом режиме.

Бывает так, что блокируется больше информации, чем было задумано. Например, если ребенок увлекается жизнью насекомых, то ему не удастся посмотреть некоторый контент, т.к там возможно будет присутствовать слово «спаривание», хотя этот термин используется даже в учебниках. Да и нынешнее поколение с легкостью научилось обходить родительские блокировки и запреты, этого контента в интернете тоже хватает.

Некоторые обязательные правила всё же есть: всегда стоит устанавливать антивирус, не переходить по ссылкам незнакомых сайтов, с высокой долей скепсиса относитесь к сообщениям от незнакомых людей. Если шантаж всё же произошел - важно сохранить скриншоты переписки и обратиться в правоохранительные органы. Так же можно обратиться на ***горячую линию «Ребенок в опасности» 8-800-200-19-10*** и к специалистам по кибербезопасности.