Классификация Интернет-угроз

Нежелательный контент

Сидя в интернете, ребёнок может с легкостью натолкнуться на нежелательный контент – особенно если на устройстве не установлены специальные, ограничивающие данные материалы, программы.
Нежелательный контент, такой как, например, сцены насилия, порнографии и другие материалы, вызывающие страх, ужас, панику и т.д. у ребёнка, может нанести вред здоровью и развитию. Если ребёнок продолжительное время подвергается воздействию таких материалов, его психическое здоровье серьёзно страдает.

Интернет-Хищники

Одной из самых больших опасностей в сети является встреча ребёнка с интернет-хищником. В качестве своих жертв эти преступники намеренно выбирают наиболее уязвимые слои населения – в том числе детей.
Особая опасность состоит в том, что преступники способны без особого труда скрыть свою подлинную личность – это затрудняет их поиски в реальной жизни. Спрятавшись за фальшивой личиной, интернет-хищники, с помощью онлайн платформ – особенно часто это происходит в социальных сетях – склоняют детей к незаконным действиям, в том числе и сексуального характера.

Киберпреступность

За годы существования интернета проблема киберпреступности становится только острее.Лишь за январь 2019 года в результате деятельности киберпреступников по всему миру произошло 1,7 миллионов случаев утечки информации.
Находясь в сети, ребёнок может стать жертвой преступника, даже не догадываясь об этом. Все это может привести к краже личной информации пользователя, включая имя, адрес, дату рождения, текущее местоположение и т. д. Но самое страшное, если для выхода в интернет ребёнок использует одно из устройств родителей, например, ноутбук – в этом случае может произойти похищение личных данных, которые в дальнейшем могут быть легко скомпрометированы.

Кибербуллинг (киберзапугивание)

Кибербуллинг — остро-социальная проблема. Исследования показывают, что в настоящее время более половины подростков становятся жертвами травли в интернете; еще столько же выступает в качестве преследователей.
Социальные сети образуют благоприятную среду для киберхулиганов, чье онлайн поведение несет в себе опасность. Риск подвергнуться травле в

интернете сейчас очень высок, поэтому родителям нужно следить за тем, что происходит с их ребёнком в социальных сетях, а также объяснять, что он может поделиться с родителями любой проблемой, какой бы она ни была, особенно если ребёнок становится жертвой кибербуллинга.

Предупреждение кибербуллинга:

- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать;
- Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
- Если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички;
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Как защититься от кибербуллинга:

- Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.
- Если по электронной почте или другим э-каналам кто-то направляет ребенку угрозы и оскорбления – лучше всего сменить электронные контакты (завести новый email, Skype, ICQ, новый номер мобильного телефона).
- Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и тем более не всегда знают, как ее предотвратить.

Фишшинг
вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Троллинг
форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это искушение, провокация и подстрекательство — то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям

«Груминг»
Термин "груминг" определяет действия злоумышленников по совращению детей в интернете. Он происходит от английского слова grooming, которое переводится как "уход" или "забота", что передает основную суть метода: создать у ребенка ощущение заботы и вызвать состояние устойчивой психологической связи для совершения последующих преступлений.

Как правило, хищник-грумер находит жертву, и все начинается с обыкновенного виртуального общения, которое может продолжаться довольно долго — до тех пор, пока он не войдет в доверие к ребенку. Грумер может использовать вымышленные личности и чужие фотографии, а также специально созданные для груминга учетные записи в социальных сетях.

Эти люди знают психологию и играют на интересах и проблемах ребенка, пока ребенок не станет считать злоумышленника другом и не согласится на встречу, где интернет-хищник сможет совершить над ним незаконные действия сексуального характера.