

ПАМЯТКА УМНОГО ПОЛЬЗОВАТЕЛЯ ИНТЕРНЕТА

Кибербуллинг, груминг, буллицид, кибермошенничество, опасный контент... Знакомы ли тебе эти слова? Каково их значение? И это лишь некоторые из опасностей, которые могут подстергать тебя в интернете. Знаешь, есть замечательные пословицы: «Предупрежден – значит, вооружен»; «Врага нужно знать в лицо». Поэтому, мы думаем, что тебе будет интересно прочитать нашу небольшую памятку, прежде чем снова отправиться в очередное не всегда безопасное путешествие по Сети.

Опасности, которые могут подстергать тебя в интернете, и как их избежать

ГРУМИНГ – это установление дружеских отношений с ребенком (подростком) с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника, модного фотографа, владельца модельного агентства и т.д. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию (адрес, телефон и пр.) и договориться о встрече.

Несколько советов, которые помогут тебе предупредить груминг:

1. Следи за информацией, которую ты выкладываешь в интернете. Не выкладывай свои личные данные в интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы родителей и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях.
2. Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями, использовании онлайн-играми и других ситуациях.
3. Не размещай и не посылай свои фотографии незнакомцам. Будь внимателен, если тебя просят прислать или провоцируют на какие-либо действия перед веб-камерой.
4. Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать как можно меньше личной информации о себе.
5. Если новый знакомый пытается говорить с тобой на неприятные или пугающие тебя темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщи об этом родителям или взрослым, которым ты доверяешь.
6. Сохрани факт груминга, например, сделай снимок с экрана (screen-shot).
7. Если ты пользуешься чужим устройством для выхода в интернет, не забывай выходить из своего аккаунта на различных сайтах. Не сохраняй на чужом компьютере свои пароли, личные файлы, историю переписки.
8. Никогда не соглашайся прийти в гости к человеку, с которым познакомился в интернете и не приглашай его к себе! Твои собеседники могут оказаться совсем не теми, за кого себя выдают. Или приходи на встречу только со взрослым. Не поддавайся на уговоры встретиться один на один, особенно – в безлюдном месте!

Всегда помни, что в интернете каждый может представить себя не тем, кем на самом деле является!

КИБЕРБУЛЛИНГ. Под этим относительно новым словом понимают «использование электронных устройств и информационных технологий, таких как электронная почта, службы мгновенных сообщений, текстовые сообщения, средства мобильной связи, web-сайты, с помощью которых можно публиковать жестокие или оскорбительные сообщения о личности или группе личностей», т. е. унижение или травля в интернете (подростковый виртуальный террор).

Несколько советов, которые помогут тебе при столкновении с кибербуллингом:

1. Не бросайся в бой. Успокойся. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт. Кроме того, преследователь только и ждет, когда ты выйдешь из равновесия. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии. Лучшая защита от нападения – игнор.

2. Не стоит игнорировать сообщения, которые содержат угрозы, особенно систематические. Следует скопировать эти сообщения, рассказать об этом родителям, обратиться в правоохранительные органы. По поводу размещения оскорбительной информации, размещенной на сайте, следует обратиться к администратору.

3. Помни, что анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом. Так что в случае нанесения реального вреда, найти злоумышленника можно.

4. Управляй своей киберрепутацией. Самому так же не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Если вдруг ты стал свидетелем кибербуллинга, то ты должен выступить против агрессора, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в Сети.

6. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

БУЛЛИЦИД – доведение до самоубийства путем психологического насилия. Может быть как результат кибербуллинга. Уже в некоторых странах принят закон «О вредных цифровых коммуникациях», согласно которому кибербуллинг (издевательства в Сети) и онлайн-троллинг признаны уголовными преступлениями, и теперь тот, кто использует лексику с угрозами, запугиваниями или оскорблениями в адрес другого человека в Сети, может быть оштрафован или даже получить тюремный срок. Также караются пользователи, занимающиеся подстрекательствами, издевательствами и унижениями.

КИБЕРМОШЕННИЧЕСТВО – один из видов киберпреступлений, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), а также злоупотребление доверием человека с целью причинить ему материальный или иной ущерб.

Несколько советов, которые помогут тебе не стать жертвой кибермошенников:

1. Посоветуйся со взрослыми перед тем, как воспользоваться теми или иными услугами Сети.
2. Установи на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу личных данных или другие подобные действия.
3. Прежде чем совершить покупку, собери информацию об интернет-магазине: ознакомься с отзывами покупателей; избегай предоплаты; проверь реквизиты владельца магазина; уточни, как долго существует магазин (посмотреть это можно в поисковике или по дате регистрации домена); поинтересуйся о возможности выдачи кассового чека; сравни цены в разных интернет-магазинах; позвони, если это возможно, в справочную магазина; обрати внимание на правила интернет-магазина; выясни, сколько точно тебе придется заплатить за товар.
4. Никогда не сообщай в интернете пароль от своей электронной почты, номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и другую личную информацию!

ОПАСНЫЙ КОНТЕНТ – информация, представляющая угрозу или вызывающая у человека неприязнь (видеоролики, изображения и тексты сексуального, экстремистского характера, призывы к насилию, пропаганда и распространение наркотиков, информация суицидального характера и т.д.).

Всегда помни:

1. Далеко не все, что можно прочесть или увидеть в интернете – правда.
2. В интернете каждый может представить себя не тем, кем является на самом деле.

Интернет может быть прекрасным и полезным средством для обучения, отдыха и общения с друзьями. Но, как и реальный мир, Сеть может быть опасна! Будь бдителен! Уважай и береги себя и своих близких!