

Кибербуллинг или виртуальное издевательство

преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.



КИБЕРБУЛЛИНГ: ПОСЛЕДСТВИЯ В РЕАЛЬНОЙ ЖИЗНИ



Несмотря на то что кибербуллинг «живет» в цифровом пространстве, у него вполне ощутимые последствия в физическом мире. Только **5% родителей** отметили, что никакого видимого влияния от кибербуллинга у их детей не было.



Среди наиболее распространенных последствий кибербуллинга для детей (по ответам родителей):



С КАКИМИ ВИДАМИ КИБЕРБУЛЛИНГА СТАЛКИВАЛИСЬ ДЕТИ

ТРОЛЛИНГ (грубость, оскорбления и негативные эмоции)

83,6%

ФРЕЙПИНГ (взлом личного аккаунта)

30,2%

АУТИНГ ИЛИ ДОКСИНГ (размещение личной информации без разрешения)

21%

ДРУГОЕ

1,2%



Если ты подвергся кибербуллингу

1. Не бросайся в бой.

Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться.

Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт

Если ты подвергся кибербуллингу

2. Управляй своей киберрепутацией

3. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно

4. Игнорируй единичный негатив.

Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии

Если ты подвергся кибербуллингу

5. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом

6. Бан агрессора.

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

Если ты стал свидетелем кибербуллинга. Твои действия:

- выступить против преследователя, показать ему, что его действия оцениваются негативно,
- поддержать жертву, которой нужна психологическая помощь,
- сообщить взрослым о факте агрессивного поведения в сети.

Фишинг или кража личных данных

главная цель - получение конфиденциальных данных пользователей - логинов и паролей.

На английском языке phishing читается как фишинг (от fishing - рыбная ловля).



Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

Основные советы по борьбе с фишингом:

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе.

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни.

"Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.



ЦИФРОВАЯ РЕПУТАЦИЯ

- Подумай, прежде чем что-то публиковать и передавать у себя в Блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.



