

БУЛЛИНГ И ЕГО РАЗНОВИДНОСТИ

Кибербуллинг — это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала. Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Киберсталкинг и как от него защититься



Киберсталкинг — это преследование человека в сети с агрессивным или сексуальным подтекстом, распространение ложных обвинений в интернете, сплетни и клевету. Особенно уязвимы дети, которые не знают как реагировать на нападки, как справляться с эмоциями от негативных сообщений или даже шантажа. Если вы не знаете, что рассказать ребенку о безопасности в сети, этот материал станет для вас отличной шпаргалкой.

Пять правил безопасного интернета для детей и родителей

1. **Проверяйте настройки конфиденциальности в социальных сетях.** Правила настроек иногда меняются, а мы об этом и не подозреваем, поэтому стоит следить о том, какую информацию могут увидеть посторонние люди. Проще всего “закрыть” страницы, так вы сможете контролировать кто ее просматривает, одобряя заявки друзьям.

2. **Старайтесь не использовать общедопупный Wi-Fi,** а если без этого никуда, не забудьте разлогиниться после использования и “забыть” сеть на устройстве (это можно сделать в настройках подключения).

3. Многим из нас **хочется делиться информацией в сети**, но стоит помнить о последствиях того или иного выбора. Не выкладывайте свой домашний адрес, не делитесь гео-метками и слишком личной информацией.

4. На всех гаджетах установите **антивирус**, чтобы защититься от фишинга (мошенников).

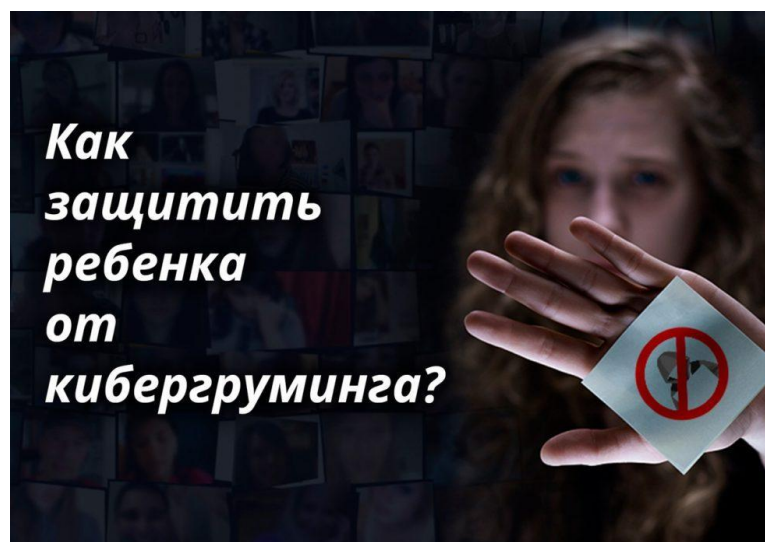
5. Не вступайте **в общение и споры** с незнакомыми людьми в интернете.

6. **Не делитесь информацией с незнакомцами**, не отправляйте им свои фотографии и видео. Интернет-преступники знают как втереться в доверие, как получить желаемую информацию, а иногда и провокационные фотографии. Любой информационный след может обернуться против человека, который его оставил.

Почему важно придерживаться этих простых рекомендаций? Киберсталкинг — это преследование человека не только в интернет-пространстве. Мошенник, преступник, злоумышленник может найти свою жертву и в реальной жизни. Поэтому, пользуясь социальными сетями, выкладывая какую-либо информацию о себе, стоит подумать о том, кто может это увидеть. И еще: не вступайте в диалог с теми, кто ведет себя неадекватно, не назначайте очных встреч и игнорируйте подобные диалоги, чаще всего этого бывает достаточно, чтобы аноним потерял интерес.

Почему дети часто становятся жертвами таких преступлений? Доверчивость, наивность, отсутствие жизненного опыта — все это может стать причиной потери бдительности в сети. Если у ребенка мало друзей, он не находит поддержки в семье или среди сверстников, это может подтолкнуть к поиску всего этого в интернете, а новые знакомства порой оборачиваются трагедиями. **Что делать родителям, как защитить?** Прежде всего, общаться, показывать, что вы всегда и везде на стороне ребенка, и что если случилась беда, он может не бояться вашего осуждения и ругани. Доверительные отношения в семье и знание правил поведения в сети — это основа безопасности как эмоциональной, так и физической!

Как защитить ребенка от кибергруминга?



Как защитить ребенка от кибергруминга?

Среди всех интернет-угроз, пожалуй, самая опасная — это **кибергруминг** — совращение ребенка в сети. В этом материале простые, но такие важные правила поведения в сети, которые нужно донести до детей.

Фишинг и как с ним бороться

1. **Никогда и не при каких обстоятельствах мы не отправляем фотографии** незнакомым людям! Особенно эротического содержания. Это правило распространяется и на общение с друзьями. Такие материалы потом могут использоваться для шантажа и издевательств.

2. **Не добавляем в друзья незнакомых людей**, не вступаем с этими людьми в диалог. Сегодня интернет-преступники могут без труда создать фейковую страницу, притворившись подростком, втереться в доверие. Начинается все безобидно: дружеское общение, обсуждение общих интересов, музыки, фильмов. Если общение уже завязалось, важно проверить кто находится по ту сторону экрана — договоритесь о встрече в скайпе.

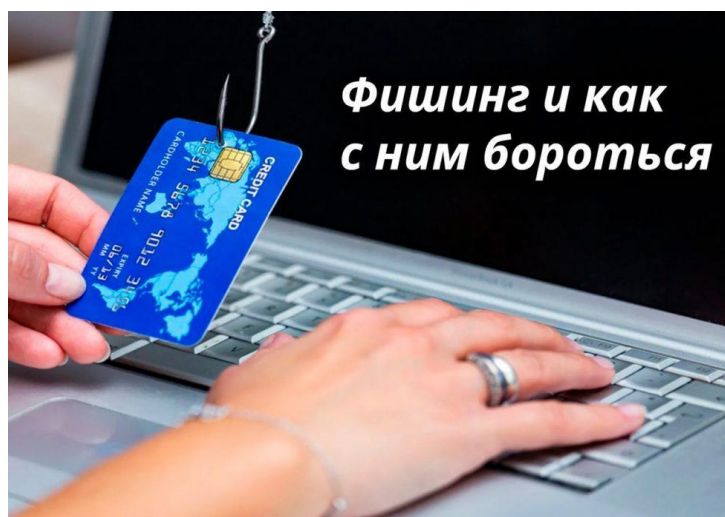
3. **Налаживаем доверительный контакт с ребенком**. Он должен понимать, что вы не осудите, поддержите и всегда будете на его стороне, что бы не случилось. Ребенку необходимо делиться с кем-то своими переживаниями, и если у него нет близких отношений с родственниками или друзьями, его легче склонить к откровенным разговорам в сети с человеком, который притворяется милым собеседником.

4. **Кибергруминг** — это всегда про шантаж и домогательства. Ребенок становится подавленным, тревожным, замыкается в себе. Если вы узнали, что в руки злоумышленников попали интимные фотографии вашего ребенка, первый шаг — прекратить общение с этим виртуальным “другом”. Материалы переписки можно предоставить в полицию.

Киберсталкинг и как от него защититься

Если ваш ребенок стал жертвой кибергруминга, он как никогда нуждается в поддержке: *ты не виноват, все мы иногда ошибаемся, мы с этим справимся*. Дети могут по-разному вести себя после пережитого стресса. Если вы понимаете, что вашей любви и поддержки не хватает, стоит обратиться к детскому психологу, который поможет восстановить эмоциональный баланс.

Фишинг и как с ним бороться



В условиях новой реальности мы еще больше времени стали проводить в интернете. Это понимают и мошенники, которые стали активнее вести себя в сети. Наверняка вам или вашим знакомым уже приходили странные сообщения о «штрафах» или «новых выплатах». Общий фон информационного шума снижает нашу бдительность! *«Ах да, я что-то слышал про выплаты... перейду по ссылке»* — так мы попадаем в цепкие лапки онлайн-мошенника. Давайте еще раз поговорим о том, как бороться с интернет угрозами. Будет полезно и детям, и родителям, и старшим родственникам.

Пять правил безопасного интернета для детей и родителей

Фишинг — это вид мошенничества в интернете, главной целью преступника является получение ваших данных (логинов, паролей) и кража средств со счетов. Как правило, человек попадает на крючок фишинг-мошенничества случайно, например, переходя по ссылке, которая кажется знакомой, а иногда и сам оставляет свои данные, участвуя в сомнительных лотереях, конкурсах и розыгрышах. Мошенники могут обмануть вас и по телефону, например, представившись компанией, которая обслуживает ваш дом или предлагая услуги, которые могут быть для вас актуальными. Войдя в доверие, они просят предоставить ваши данные (номер карты, логины и пароли).

Как избежать фишинговых атак?

1. Никогда и ни при каких обстоятельствах **не диктуйте** свои личные данные по телефону.

2. Установите **антивирусное программное обеспечение** на свои гаджеты. Регулярно обновляйте его.

3. **Избегайте всплывающих окон на сайтах.** Фишинг-мошенники часто скрываются за такими ссылками.

4. **Внимательно читайте электронные письма.** Если вы не запрашивали смену пароля на каком-либо сайте, не совершали покупки и не делали других запросов, не переходите по ссылкам из писем.

5. **Не делитесь в сети своими личными данными:** номером карты, логинами и паролями, паспортными данными.

6. **Регулярно меняйте пароли** в социальных сетях и электронной почте. Старайтесь придумывать сложные комбинации для каждого аккаунта.

7. Если вы получили **сомнительную ссылку** от друга, лучше переспросить его о том, что это, в другой социальной сети. Вашего друга могли взломать.

8. **Не отвечайте на незнакомые номера** или смело заканчивайте разговор, если он ведет к просьбам предоставить ваши персональные данные.

9. **Установите везде, где можно, двойную аутентификацию.** Так, при вводе пароля с новых устройств, вы должны будете ввести и код, который придет по смс.