Безопасный Интернет детям. «Основные правила безопасности в сети Интернет»

Интернет – уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учебы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, — все это Интернет.

Почему же необходимо предупреждать об опасностях виртуального мира, если в нем так много всего хорошего и полезного? Достаточно большая часть интернет-пользователей ищет в Интернете не друзей, а свои жертвы. Дело в том, что недобросовестные граждане - мошенники, наркодилеры, иные злоумышленники, асоциальные и психически нездоровые люди по-своему оценили возможности Интернета. Ведь именно Всемирная паутина дает возможность преступникам действовать анонимно.

В связи с этим небезопасное поведение в сети Интернет может нанести вред и вам, и вашим родным и близким людям. Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила.

ТРИ самых общих правила, которые в наш информационный век должны стать вашими спутниками на всю жизнь:

1. ПАРОЛИ (как ключ от дома).

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Статистика говорит о том, что большинство людей мало уделяют внимания парольной политике. Третий год подряд самым популярным паролем в мире является «123456». Подобрать такой пароль к вашим порталам и персональным данным злоумышленнику не доставит труда. Регулярно осуществляйте смену паролей, обеспечивая каждый раз их конфиденциальность. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом. Правило первое: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

2. ВИРУСЫ и АНТИВИРУСЫ («моем руки с мылом»)

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета. Программы «Черви», «Трояны», «Шпионы» - их множество

разновидностей и красивых названий, а суть одна – все это вредные вирусы! Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями. Устанавливать надо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия вашего антивируса. Не качайте программные продукты из сомнительных источников (файлообменных сетей и торрентов). Не открывайте и не сохраняйте подозрительные файлы – сразу удаляйте. Не отвечайте на непонятные вам рассылки. И главное - не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – не нажимайте «да» или «ENTER». Здесь можно провести простую параллель – держимся подальше от вирусов, моем руки регулярно, хорошим и качественным мылом. При любой сомнительной ситуации: «Моем руки с мылом, к вирусам не прикасаемся».

3. ПЕРСОНАЛИЗАЦИЯ (как документы в сейфе)

Никому не передавайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться за вами всю жизнь. Могут навредить вам на пути к достижению поставленной цели. Игнорируйте в сети Интернет подобные запросы. Получается странно – дома и на работе мы храним свои документы в сейфе, закрываем на ключ. Мы понимаем их важность. А потом по непроверенному запросу открываем сейф, достаем документы, фотографируем и посылаем посредством ресурсов в сети Интернет. Количество лиц, которые могут получить доступ к таким посланиям, даже трудно прогнозировать. Интернет-мошенники используют разные способы, чтобы получить конфиденциальную информацию – логины и пароли для доступа к личным страницам пользователей. Если злоумышленники все-таки взломали страницу, необходимо предупредить друзей и знакомых, что возможна рассылка вредоносных сообщений с взломанного аккаунта, и обратиться в техническую поддержку сайта. Давайте запомним третье правило: «Наши документы всегда в сейфе».

Так же имеются другие угрозы на просторах «Интернета», давайте поподробней поговорим об этом:

Электронные платежи. Оплачивать товары и услуги с помощью компьютера или телефона очень удобно и быстро. Тем не менее следует соблюдать особую осторожность, чтобы не лишиться своих финансовых средств. Очень важно покупать товары, а также вводить данные карт и личные данные только на проверенных сайтах, а свои страницы на сервисах электронных платежей защищать сложным паролем, лучше с СМС-подтверждением.

Вредные материалы, не соответствующие возрастным особенностям, негативно влияют на психическое здоровье детей. В сети Интернет содержится много вредной, бесполезной, недостоверной информации. Поэтому не стоит безоговорочно доверять тому, что пишут в сети, посещать подозрительные сайты, переходить по ссылкам, которые «всплывают» в окне браузера. Лучше всего установить приложение для блокировки рекламы - АНТИСПАМ.

Социальные сети. Большой популярностью у пользователей Интернета пользуются социальные сети - онлайн-платформы, которые люди используют для общения, создания социальных отношений с другими людьми, объединения по интересам. Социальные сети дают возможность отправлять сообщения и изображения, делиться видео- и аудиозаписями, тегами, создавать свои группы и сообщества, играть в онлайн-игры. Среди преимуществ социальных сетей – расширение круга общения, простота и доступность общения, в т.ч. с людьми из других городов и стран, получение информации, позволяющей быть в курсе последних событий, возможность выбирать друзей и сообщества по интересам. В то же время социальные сети имеют и немало недостатков. В первую очередь, это связано с возникновением зависимости у подростков, которые предпочитают виртуальный мир реальному общению. Анонимность в сети, когда человек может зарегистрироваться под любым именем, скрывая свою личность, может привести к вседозволенности. В Интернете можно легко добавлять и удалять друзей, любой разговор можно начать и прервать, перестав отвечать на сообщения, избежать ненужного знакомства, игнорировать тех, кто не нравится. В реальном мире не всегда можно прямо высказать мнение, иногда необходимо промолчать, всегда нужно быть вежливым. После «свободы» Интернета у детей, подростков, да и взрослых людей возникают трудности в общении. И наоборот, иногда пользователи соцсетей сообщают о себе подробную информацию, включая личные данные, и выкладывают фотографии, которые могут привлечь внимание злоумышленников. Кроме того, нет никакой гарантии, что человек, который «добавился в друзья», тот, за кого себя выдает.

Кибербулинг. Одной из острых проблем, связанных с Интернетом и соцсетями, является кибербуллинг. Об актуальности этой проблемы говорит тот факт, что, согласно исследованиям, более половины Интернет-пользователей сталкивались с онлайн-агрессией. Кибербуллинг – это травля с помощью гаджетов, соцсетей, вообще использование виртуального пространства, чтобы запугивать, угрожать, преследовать другого человека. В отличие от буллинга (англ. bullying – «травля», школьное насилие, издевательства и унижения в отношении ученика со стороны других учащихся или учителей) кибертравля, во-первых, может быть анонимной. Когда человек не знает, откуда поступает тревога, он чувствует себя более беззащитным. Анонимность – одна из основных причин возникновения травли в сети. Из-за возможности скрыться за выдуманным именем и сказать что угодно под маской, люди считают, что им все можно, в том числе унижать

другого человека. Во-вторых, кибербуллинг не имеет ни территориальных, ни временных границ. Он никогда не прекращается. Даже при выключенном телефоне или компьютере в виртуальном пространстве травля продолжается. Ребенок будет продолжать получать сообщения или оповещения о новых комментариях. В-третьих, травля в сети подобна вирусу: даже если про нее знал один-два человека в школе, то с помощью Интернета злая шутка или оскорбление может стать достоянием всего мира. Есть дети, равнодушные к соцсетям. Но есть те, кто активно общается в сети, они всегда онлайн, у них много друзей в виртуальном мире, есть свой блог или канал на YouTube. Таким детям вне зависимости от возраста проще стать жертвой кибербуллинга. В современном мире уровень агрессии очень высок, это же отражается и в виртуальном пространстве. Злоба выливается в сеть и принимает различные формы травли.

Сегодня различают множество форм травли в сети:

Исключение, интернет-бойкот – когда одного человека намеренно не добавляют и не приглашают в группы, чаты, форумы. Например, создается школьный или классный чат и кого-то одного туда не включают. Или дети играют в онлайн-игру и кого-то одного туда не приглашают.

Хейтинг - умышленная травля с использованием оскорблений, угроз, негативные комментарии под фотографиями и постами ребенка. Этот вид кибербуллинга может иметь серьезные последствия для детей. Такие сообщения пугают ребенка, он становится нервным, неуверенным в себе, не знает, что ему делать, чаще всего пытается обороняться в той же агрессивной форме.

Аутинг – это публикация личной информации ребенка, каких-то интимных деталей о нем, чтобы унизить. Это может быть, как незначительная информация, так и что-то серьезное. Личную информацию о человеке нельзя разглашать или взламывать. Если такое происходит с ребенком, он должен сообщить о проблеме и в службу технической поддержки сайта, и в школе, и, конечно, родителям.

Киберсталкинг, домогательства – это тяжелая форма травли, которая представляет реальную угрозу для безопасности и здоровья ребенка. Иногда так называют случаи, когда взрослые пытаются связаться с детьми и подростками через интернет (чаще всего педофилы). Это очень опасно! Дети должны рассказывать о подобных случаях родителям. А родителям стоит немедленно обратиться в полицию.

Фрейпинг – форма буллинга, когда обидчик получает контроль над учетной записью ребенка и публикует нежелательный контент от его имени, портит его репутацию.

Диссинг – это форма буллинга, когда распространяют онлайн-публикацию, порочащую репутацию человека. Это могут быть видео, фото, скриншоты, чаще всего поддельные (фейковые).

У всех форм травли одна цель – регулярно причинять вред человеку. Единичный конфликт в сети, один злобный комментарий – это еще не кибербуллинг.

Знать правила безопасного поведения в Интернете (не посещать сомнительные сайты, не раскрывать личную информацию, не доверять первому встречному, даже в личной переписке не сообщать о себе то, чем не готов поделиться со всеми и т.д.) При общении в Интернете надо соблюдать те же морально-этические правила, что и при общении в реальном мире. Надо относиться уважительно к собеседникам, не вступать в споры по переписке, не оскорблять других людей. Во многих социальных сетях есть важные кнопки – «заблокировать» или «пожаловаться». С их помощью можно оградить себя от неприятного общения. Если же травля все-таки происходит, необходимо обратиться к родителям или учителям. Не нужно сразу удалять нежелательный контент. Нужно сохранить всю переписку, обидные слова, чтобы было что показать и обсудить с администрацией школы, модераторами сайтов, полицией. Если есть доказательства (скрины, заявление от родителей потерпевшего, его показания), то в полиции заведут дело, виновных вычислят, родители хулигана заплатят штраф. Если человек уверен в своей правоте, обращается в официальные инстанции и добивается справедливости, он подает положительный пример окружающим: надо добиваться правды, уметь защищать себя и уметь просить о помощи. Игнорировать факт травли ни в коем случае нельзя. Можно попробовать самому поговорить с обидчиками, сказать им, что вам не нравится происходящее. В случае неудачи все же стоит обратиться ко взрослым, которым вы доверяете. Сейчас соцсети пытаются использовать свои способы борьбы с кибертравлей. Например, в случае выявления оскорблений в комментарии автор получает совет отказаться от обидного фрагмента, не тратить время на агрессию. Непристойные, содержащие ненормативную лексику комментарии удаляются, а нарушающие правила пользователи блокируются. Дети и подростки должны чувствовать ответственность за свои действия, понимать, что нет безграничной анонимности и вседозволенности. Жертвой кибербуллинга может стать абсолютно каждый. И просить помощи взрослых в сложной ситуации – это нормально и правильно. Важно помнить, что кроме социальных сетей есть реальный мир, в котором много добрых и хороших людей. Надо наполнить свою жизнь разнообразными и интересными занятиями, учиться вживую налаживать отношения с окружающими людьми.

Кибертерроризм. Несмотря на растущее в последние годы международное признание угрозы, которую несет с собой использование террористами Интернета, в настоящее время не существует универсального инструмента, специально посвященного этому приобретающему все более значительные масштабы направлению террористической деятельности. По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Всемирная сеть привлекает возможностью свободного доступа, анонимностью (что важнее всего), быстрой передачей информации, огромной аудиторией, техническими

возможностями, дистанционным характером воздействия на компьютерные системы в различных регионах мира. Но, несмотря на это, на данный момент популярным и заметным видом кибер-терроризма это взлом сайтов и размещение на них лозунгов и призывов. Террористы могут использовать Интернет, с целью содействия террористическим группам для осуществления сбора информации, о местонахождении целей и их характеристики, сбора средств для поддержки какого-либо движения, с помощью интернета могут совершать сборы различных групп людей и могут давать им указания о времени и месте проведения встречи, формах различных протестов. Интернет обладает огромным рекламным потенциалом и с его помощью террористы могут обратиться к большому числу людей по всему миру. Терроризм часто называют одной из форм психологической войны. Ведение такого вида войн стало возможным из-за массовой информатизации всех сфер общества. Сеть активно используется террористами для дезинформации, распространения угроз, создания в обществе ощущений страха и беспомощности. Одно из основных применений Интернета террористами – распространение пропаганды. Интернет может быть использован не только для публикации экстремистских материалов, но и для налаживания контакта и развития отношений с аудиторией, которая наиболее подвержена влиянию террористической пропаганды. Для вербовки террористические группировки все чаще используют защищенные паролем сайты и порталы с ограниченным доступом. Сеть Интернет используется для вербовки и мобилизации сторонников, способных на активную роль в поддержке террористических действий. В дополнение к таким средствам привлечения новых членов, как технологии веб-сайтов (звук, видео и т.п.), террористические организации собирают информацию о пользователях, просматривающих их сайты. С теми из них, которые кажутся наиболее заинтересованными в деятельности организации или подходящими для выполнения ее поручений, устанавливают контакт. Вербовщики применяют онлайн технологии – перемещаются по чатам и форумам в поиске наиболее восприимчивых пользователей, особенно из числа молодежи. Как бороться с терроризмом? Тем же методом – информированием. Террористы используют ложную информацию с целью вербовки. У мирного населения должно быть информирование с целью знания – что такое терроризм, как он проявляется в Интернете, какие сайты существуют, какова их цель, к чему приводит участие в подобных группировках и прочее.