Интернет-безопасность

(на основе материалов, разработанных отделом по борьбе с противоправным использованием информационно-коммуникативных технологий ГУ МВД России по Иркутской области)

Интернет - уникальная реальность нашего с вами времени. Это безграничный мир информации, в котором есть как развлекательные и игровые порталы, так и полезные сведения для учебы и расширения кругозора. Именно с помощью интернета мы общаемся со своими друзьями в режиме онлайн, вступаем в сообщества по интересам, делимся последними новостями, веселимся и делаем домашнюю работу. Иными словами, интернет - это информация, оперативно обеспечивающая ваши ежедневные потребности и доступная в любой момент. Однако полицейские вынуждены предупреждать об опасностях виртуального мира. Определенная часть пользователей сети ищет в интернете не друзей, а своих жертв. Важно обезопасить себя и своих близких от преступных намерений других людей. Недобросовестные граждане (мошенники, наркодилеры, психически нездоровые люди) по своем у оценивают возможности интернета. Ведь именно сеть зачастую дает возможность преступникам действовать анонимно, поэтому небезопасное поведение в интернете может нанести вред вам, вашим родным и близким. Необходимо себя обезопасить для этого достаточно серьезно отнестись к проблеме киберпреступности и соблюдать простые правила:

1. ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

1) Исключите использование паролей по умолчанию и не сохраняйте пароли в ваших гаджетах и браузерах. Регулярно осуществляйте смену паролей и никому их не сообщайте. Не используйте один и тот же пароль на каждом сайте, который вы посещаете;
2) Пользуйтесь антивирусными программами, *вредоносные* программы в состоянии скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть денежные средства. Их называют «черви», «трояны», «шпионы», но суть одна все это вирусы. Для защиты компьютера на нем устанавливаются **специальные защитные программы и фильтры.** Использовать можно только лицензионное программное обеспечение с актуальными обновлениями. Также нельзя допускать истечения срока действия вашего антивируса в таком случае он будет работать неэффективно. Не стоит скачивать программы с непонятных сайтов, открывать и сохранять подозрительные файлы, отвечать на загадочные рассылки. И главное не посещайте сайты с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения, если у вас есть домашняя Wi-Fi сеть, подключите роутер к стационарному компьютеру или ноутбуку по проводам. Тогда весь трафик пойдет через устройство, и антивирусной программе будет легче отражать атаки мошенников;
3) Никому не передавайте свои конфиденциальные данные и следите за «цифровым следом». Это могут быть логины, пароли, данные банковских карт, свидетельство о рождении, паспортные данные, личные фотографии. Игнорируйте в интернете подобные запросы. Важно запомнить правило: «Документы всегда хранятся в сейфе». Если вы публикуете какую - либо информацию на своей странице в социальной сети, обязательно проверьте настройки конфиденциальности на сайте: убедитесь, что данные не доступны для просмотра широкой публике. То, что вы публикуете в интернете, останется там **навсегда, даже если вы удалите эти сведения**. Университеты и работодатели проверяют профили соискателей в социальных сетях, поэтому убедитесь в том, что вы публикуете в Интернете, уместно и не навредит вам в будущем.

2. ОСКОРБЛЕНИЯ И НАПАДКИ В СЕТИ ИНТЕРНЕТ

Самый распространенный вид хулиганства в сети это троллинг.

Троллинг — форма провокации или издевательства при общении в интернете, использующаяся людьми, заинтересованными в узнаваемости, публичности, эпатаже. Термин «троллинг» происходит из сленга участников виртуальных сообществ. Цель тролля подбросить вам такую наживку (обидное слово, насмешка, оскорбление), чтобы вы ее заглотили (начали расстраиваться, писать ругательства в ответ). Анонимность в сети позволяет троллям представлять себя совершенно другими и быть уверенными в своей безнаказанности, поэтому они пишут и делают такие вещи, которые в реальной жизни никогда бы не рискнули сотворить в присутствии оппонента. По причине как неизвестности, так и недосягаемости, травить, оскорблять и провоцировать людей, кажется им забавным занятием. Как показывает практика, больше половины сетевых грубиянов являются детьми, скучающими в интернете или не ладящими со сверстниками. Запомним простое правило: **не надо кормить троллей, это бессмысленно**. Если вы заметили, что кто то в сети ведет себя таким образом вы можете легко **победить его: не спорьте с ним, не пытайтесь оправдаться или что - то объяснить, не обращайте внимания.** Ведь единственное, что ему нужно это ваша реакция. Как только вы перестанете реагировать он очень быстро потеряет к вам интерес. Не доставить грубияну удовольствия видеть ваш гнев или обиду будет лучшим наказанием, ибо его цель не будет достигнута. Давайте будем разделять троллинг и юмор. Безусловно, никто не запрещает вам шутить над своими друзьями, обсуждать в сети вопросы, не обязательно используя литературный русский язык. **Просто не переходите грань: юмор не должен перерастать в оскорбления, хамство и откровенную травлю**. Гораздо опаснее ситуация, когда вас начинают обижать люди, которые знают вас лично. В случае, когда вы видите, что против вас начинается коллективная травля ни в коем случае не расстраивайтесь и не замыкайтесь. В сети людям свойственен стадный инстинкт, и многие из тех, кто включается в травлю, лично против вас ничего не имеют. Они просто пошли на поводу у группы людей, и это говорит о них очень красноречиво, значит у них нет своего мнения, они являются послушными куклами в чужих руках.

Тебя начинают атаковать в мессенджерах, социальных сетях или модных приложениях? Требовать фотографии или персональные данные, угрожать с разной аргументацией, против тебя организуется коллективное преследование? Оскорбления, угрозы, искажение твоих изображений все это не безобидные шутки, это **буллинг.**

Кибербуллинг — агрессивное преследование в сети Интернет одного из членов коллектива со стороны остальных членов коллектива или его части. При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от конфликта, где силы сторон примерно равны. Буллинг приводит к тому, что жертва теряет уверенность в себе. Также это явление может приводить к психическим отклонениям и явиться причиной жестокой агрессии в сторону тех, кто занимается травлей.

Виды кибербуллинга: - Н**ападки:** постоянные изнурительные атаки, повторяющиеся оскорбительные сообщения, направленные на жертву; - **Клевета:** распространение оскорбительной и ложной информации; - **Самозванство**: перевоплощение в определенное лицо, когда мошенник позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях; - Обман: выманивание конфиденциальной информации и ее распространение, получение персональных данных и их публикация в сети Интернет или передача тем, кому она не предназначалась. В этих случаях очень важно объяснить человеку, что его травят злоумышленники, причем травят безосновательно и нет причин для расстройства, снижения самооценки. Надо показать, как действовать в сложившейся ситуации. И вы не должны допускать такого в своем коллективе, друзья! **Обязательно сообщите взрослым (родителям, родственникам, учителям)** о преследовании вас или ваших одноклассников в сети интернет и примите вместе решение об обращении в полицию. Храните подтверждения фактов нападений в сети. Не переживайте в тайне от родителей такие ситуации. Если для травли используют ваши прошлые ошибки или

неправильное поведение гораздо проще сразу признаться в этом перед старшими, чем загонять проблему внутрь. Не спешите выбрасывать свой негатив в киберпространство, создавайте собственную онлайн - репутацию . **И никогда не принимайте сами участие в травле кого-либо. Ваше достойное поведение является главной защитой и гарантом спокойствия вас и ваших близких.**