**Безопасность детей на каникулах**

**Безопасность не только в реальном, но и виртуальном мире!**

Именно дети и подростки, психика которых не до конца сформирована, склонны попадать в интернет-зависимость. Исследования показывают, что среди молодежи интернет-зависимых больше, чем среди людей зрелых.

 Когда ребенок проводит возле компьютера большую часть времени, его личность оказывается совершенно неадаптированной к реальности. Маленький человек испытывает трудности в общении со сверстниками и постепенно уходит из социума, из реальной среды обитания в виртуальную.

Дети и подростки должным образом не владеют собой, не имея волевой регуляции, легко поддаются влиянию, им непросто отличать хорошее от плохого, у них не сформированы адекватные схемы поведения и восприятия. Они активно исследуют жизнь, в том числе при помощи Интернета..

Наиболее типичной и массовой интернет-угрозой для детей и подростков в настоящее время является киберунижение и кибертравля .

 Иллюзия анонимности и безнаказанности приводит к тому, что некоторые пользователи дают выход агрессии в Интернете, оскорбляя других пользователей или провоцируя их на конфликт. Подобное поведение в Интернете называют «троллингом».

 Троллинг и кибербуллинг преимущественно встречаются в социальных сетях, на форумах и в чатах. Для кибертравли используются также электронная почта и онлайн-мессенджеры, например, WhatsApp, Telegram. Опасность распространения унижающей ребенка информации заключается в том, что в отличие от обычного унижения, сцены, изображающие сам процесс унижения, распространяются на неограниченный круг лиц. Такие видео или фото могут быть доступны будущим друзьям и знакомым даже в случае переезда ребенка в другой город. Еще одна опасность заключается в том, что на данный момент удалить все экземпляры унижающих текстов или изображений из Интернета почти невозможно — ничто не мешает кому-то сохранить их на своем компьютере и опубликовать в Сети повторно даже через несколько лет.

Кибербуллинг — вид психологического давления, которое выражается в преследовании жертвы в социальных сетях, sms-сообщениях и размещением материалов, порочащих честь и достоинство жертвы.

Не менее актуальной угрозой, исходящей из Интернета, является вовлечение несовершеннолетних в преступные экстремистские и радикальные группировки.

 Экстремизм (от лат. extremus — крайний) — приверженность к крайним мерам и действиям в политике, совокупность идей, намерений, оправдывающих при принятии решений крайние меры. Девизы экстремистов: «Кто не с нами — тот против нас», «Гильотина — лучшее лекарство от перхоти» предполагают отказ от таких инструментов общения, как диалог, переговоры, компромиссы, которые называются «пустой болтовней». Нормальным считается конфликтное, агрессивное навязывание собственной точки зрения.

Набирающей масштабы интернет-угрозой является использование интернет-технологий для пропаганды и популяризации потребления наркотиков среди молодежи. Опасность заключается в использовании Интернета для наркотизации подрастающего поколения.

Особую опасность для детей и подростков представляют ролевые и сетевые компьютерные игры, которые приводят к психологической зависимости от компьютера и Интернета.

Игровая зависимость — форма психологической зависимости, проявляющаяся в навязчивом увлечении видеоиграми и компьютерными играми.

Игроманы отказываются от друзей, переходят на нездоровую пищу, забрасывают учебу, у них повышается агрессивность, склонность к насилию и ряд других факторов. Считается, что зависимые геймеры (игроки) нуждаются в психологической помощи, их проблемы — несложившаяся личная жизнь, неудовлетворенность собой, потеря смысла жизни и обычных человеческих ценностей. Появляются и другие трудности — подавленное настроение, плохое самочувствие, низкая активность, повышенный уровень тревожности и социальная дезадаптация.

Широкое распространение получили сегодня и некоторые виды интернет-мошенничества. Каждый пользователь Интернета сталкивался с предложениями отправить СМС на определенный номер, чтобы получить причитающийся выигрыш. Сформировалось целая отрасль способов интернет-мошенничества, получившая название фишинг.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на фейковый сайт, внешне очень похожий на настоящий.

Фейками называют поддельные страницы или сайты, которые имитируют страницы других реальных пользователей или компаний, например, банков. Основная задача такой страницы — убедить другого пользователя в том, что он попал на реальную страницу сайта. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

**Необходимо помнить, что в Интернете обитают не только добропорядочные пользователи, но и мошенники, которые с легкостью могут добыть ценную для них информацию!**