

РИСКИ И УГРОЗЫ СОВРЕМЕННОЙ ИНТЕРНЕТ – СРЕДЫ

Современную жизнь человека в обществе практически невозможно представить без Интернета. Наряду с представляющимися возможностями использования интернета как инструмента социализации, благодаря которому раздвигаются границы познания, возрастают возможности удовлетворения потребностей, расширяются рамки общения и взаимодействия, многократно возрастают и риски негативного влияния на психологическое самочувствие, эмоциональное благополучие, здоровье и даже жизнь человека

В ряду актуальных для сегодняшней интернет - среды рисков, связанных с использованием интернета детьми и подростками, специалисты выделяют следующие:

- **Контентные риски** — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

- **Коммуникационные риски** связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

- **Электронные (кибер-) риски** — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.

- **Потребительские риски** – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные подделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

- **Интернет-зависимость**, навязчивое желание войти в интернет и невозможность выйти из интернета, патологическая, непреодолима тяга к интернету, «оказывающая пагубное воздействие на бытовую, учебную, социальную, рабочую, семейную, финансовую или психологическую сферы деятельности».

В последнее время все большую тревогу вызывает распространение рисков, связанных с вовлечением молодежи в опасные группы, сообщества. Это, прежде всего, так называемые «группы смерти», которые вовлекают молодых людей в выполнение опасных заданий, приводящих в конечном итоге к суициду. Это так же экстремистские группы, внушающие идеи о несправедливости мироустройства и их особом предназначении в «улучшении мира», посредством его «очищения от недостойных» и вовлекающие в незаконную экстремистскую деятельность. Это и группы, предлагающие «работу», заключающуюся в незаконной деятельности (прежде всего, в распространении наркотических и других запрещенных веществ, литературы и т.п.). Действие этих рисков очень трудно контролировать, т.к. закрытые группы возникают в сети с другими названиями, а вместо заблокированных страниц создаются новые. Создатели таких групп используют ухищренные способы распространения информации о себе, используя «хештеги». Организаторы таких групп искусно эксплуатируют все социально-психологические механизмы моды. Так, группа создается с использованием современных технологий, что отражает такую ценность моды как современность.

Принадлежность к такой группе демонстрируется через выкладывание в сеть отчетов о выполнении заданий, что опирается на использовании ценности демонстративности моды. Эксплуатируется и такая ценность моды как игра. Участники групп вовлекаются в опасную игру, связанную с выполнением

эвристических, поисковых сложных заданий, связанных с риском. Получение «лайков» за отчеты о выполненных заданиях создают у подростка чувство радости «победы», сопряженным с самоудовлетворенностью.

Организаторы в качестве ведущего механизма моды для вовлечения в группы используют эмоциональное заражение, проявляемое через передачу определенного эмоционального состояния на фоне возбуждения. Благодаря поддержке переживания «тайны», скрытого обсуждения этой «тайны» с многими участниками группы, получая свидетельства «восхищения», человек подсознательно усваивает образцы диктуемого модой поведения. Активно эксплуатируется механизм внушения. Используются различные способы вербального и невербального воздействия на подростков с целью создания у них определенного эмоционального состояния, побуждения к определенным действиям. Эмоциональная насыщенность информации, ее постоянная пополняемость создает эффект «эмоционального заражения» и стимулирует желание следовать навязываемым образцам. Подростки, в силу малого жизненного опыта и незначительного социального статуса, более подвержены внушающему воздействию моды. Большое значение играет и механизм подражания. У подростков всячески поддерживается чувство принадлежности к «особой касте» закрытой, тайной группе, принадлежать к которой престижно, что создает основу для действия механизма подражания. «Подвиги» участников группы (часто совершивших непоправимое), обсуждаются и героизируются членами группы, отдельные участники возводятся в ранг «звезд». «Звезды» усиливают привлекательность поступков, что создает базу для действия механизма идентификации – отождествления себя со значимым другим. Все указанные механизмы моды достаточно эффективны и, накладываясь на возрастные особенности подростков, приводят к интенсивному распространению среди них модного поведения и вовлечению в группы все большего их числа.

ИНФОРМАЦИОННАЯ ПАМЯТКА

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твоё местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

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;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

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

Основные советы по борьбе с кибербуллингом:

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;

2. Управляй своей киберрепутацией;

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

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

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель 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.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайти в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоём номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;