Сафина Замира
ученица 8г класса
МБОУ «Гимназия 183»

Безопасность д е т е й в интернет - пространстве

Раскрывая нашу тему, наверное для начала нам надо понять, а что для нас подразумевает слово «Интернет» и как нам обеспечить детей от нежелательного контента в такое нелёгкое время.

Интернет – это на сегодняшний момент смысл всей жизни для многих людей, в том числе и детей. Мы постоянно сидим и не понимаем, сколько вреда и опасностей получаем от вредоносных сайтов, иногда не можем уберечь детей от самых ненужных сайтов. Интернет проникает во все сферы жизни: общение, развлечения, образование. Он приносит пользу, но становится не менее опасным, чем реальная жизнь. Всемирная сеть дает злоумышленникам возможность придумывать новые форматы преступлений, с которыми человечество не сталкивалось ранее. Конечно, есть даже место, где занимаются такими проблемами безопасности детей в пространстве, это ЮНЕСКО. Их цель поддерживать стабильность в плане сохранения здоровья детей в разных странах. Работники очень стараются, формулируют правила, положения, способные защитить детей от злоумышленников в интернете.

Начнём с видов опасностей которые могут преследовать детей в интернет-пространстве. Это: спам, кибербуллинг, кибершпионаж, мошенничество, компьютерные вирусы. Подробно разберем каждую из них.

1. **Спам** - массовая рассылка электронных реклам вместо информации. Бывают разные виды спама:

Переизбыток ключевых фраз. Когда в тексте очень много ключевых фраз, с помощью которых, завышается его позиция в поиске.

Дорвеи - это промежуточные веб страницы, которые занимаются переадресацией читателя на другой сайт.

Ссылочный спам. С целью накрутки веса веб мастер использует массовое приобретение гиперссылок с автоматических бирж или спамерских ссылок

получаемые с блогов, так же целой сети спамерских сайтов.

Опасность спама. Одно из главных проблем это возрастающая нагрузка коммуникации, ведь спам замусоривает каналы связи, создаёт трафик, оплачивать который приходится либо провайдеру, либо пользователю. Так же спамеры занимаются рассылкой ссылок на заражённые сайты или же непосредственно самих вирусов. Открывая такое спам-письмо, вы рискуете заразить компьютер вредоносной программой.

Для того что бы защитить себя от спама нужно: чтобы у вас был надежный пароль и что бы вы нигде его не публиковали. Ни в коем случае не отвечайте спамеру и не пытайтесь отписаться от рассылки. Может случиться так, что ответ прочитает «робот» и пометит ваш адрес как «живой» — тогда спама будет приходить ещё больше. Вы можете настроить фильтрацию писем и их использование резко снизит количество спама.

2. **Кибербуллинг.** Кибербуллинг - это кибер травля-оскорбления, угрозы с помощью современных средств комуникации. Сейчас я бы хотела рассказать о кибербуллинге в интернете, так как большая часть подростков в наше время страдают от этого. Поддержанные травле мучаются не понарошку, причем это может быть не только психологическая, но и физическая боль. Причинами кибербуллинга могут выступать разные факторы. Чаще всего им занимаются ради завоевания признания внутри коллектива, избавления от скуки или преодоления личностного кризиса.

Как же избежать кибербуллинга? Лучше всего обратиться к психологу, чтобы обработать проблему. Постарайтесь научиться отстаивать свои границы, чтобы защититься от агрессии. Не забывайте, что вы всегда можете прекратить общение с человеком просто заблокировав его.

3. **Кибершпионаж** - несанкционированное, часто незаконное получение доступа к защищённой информации с различными целями. Происходит это за счёт обхода систем компьютерной безопасности. Применяются специальные шпионские программы и трояны. Взлом осуществляется через интернет и локальные сети, посредством физического

доступа. Во многих странах кибершпионаж расценивается как преступление, но квалификация отдельно взятых деяний зависит уже от конкретных обстоятельств дела.

4. **Мошенничество.** В интернете можно столкнуться с мошенниками, цель которых — обманным путем получить от вас деньги или завладеть личными данными. Узнав ваши фамилию, имя, отчество, номер телефона, пароли от учетных записей, паспортные данные, реквизиты банковских карт и другие сведения, преступники могут использовать их для доступа к переписке, для рассылки сообщений от вашего имени и для кражи денег. Виды мошенничества:

Поддельные (фишинговые) письма. Мошенники присылают письма от имени банков, сервисов или других организаций и запрашивают ваши конфиденциальные данные, например для подтверждения учетной записи или активации почтового ящика.

Фишинговые сайты. Фишинговые сайты — это поддельные сайты, которые маскируются под настоящие. Пытаясь зайти на популярный сайт, пользователь попадает на сайт-подделку, который очень похож на оригинал. Все данные, введенные на таком сайте (пароли, номера банковских карт, паспортные данные и т. д.), окажутся у злоумышленников.

Мошенничество в социальных сетях. Мошенники в социальных сетях рассылают сообщения с предложениями приобрести товар с большой скидкой или получить выигрыш за предоплату, а также с просьбами о помощи. Цель таких сообщений — убедить вас отправить деньги.

Мошенничество на маркетплейсах. Злоумышленники могут выступать в роли продавцов или покупателей на торговых площадках и сайтах объявлений. Их цель — перенаправить вас на фишинговый сайт или заставить заплатить по ложным реквизитам.

Обман (скам). Некоторые сайты приглашают пользователей пройти опрос или заполнить анкету за вознаграждение. Чтобы получить заработанную сумму, предлагают оплатить комиссию или регистрационный сбор. На самом деле эти

деньги достаются мошенникам, пользователи ничего не получают. Как правило, на таких сайтах предлагают неоправданно большую оплату за простые задания.

Обезопасить личные финансы позволит соблюдение базовых правил:

1. создавать сложные пароли и использовать разные данные для почтовых ящиков, соцсетей, других сайтов, ведь пароль восстановить проще, чем вернуть украденные деньги;

2. не кликать по неизвестным ссылкам, которые приходят по электронной почте, в мессенджерах, социальных сетях, особенно если предлагают что-то бесплатное или на выгодных условиях;

3. не сообщать посторонним личные данные карты и не вводить их на незнакомых сайтах, не указывать коды безопасности из смс-сообщений;

5. Компьютерные вирусы - вид программного обеспечения, способного копировать себя и внедряться в код других программ. Для его предотвращения необходимо скачать Антивирус. Это программа которая обнаруживает файлы с вирусом и устраняет его.

Классификация вирусов по степени воздействия:

Безвредные вирусы никак не влияющие на работу компьютера;

Неопасные вирусы не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти, действия таких вирусов проявляются в каких-либо графических;

Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера; Очень опасные

Вирусы, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

И напоследок хочется сказать, чтобы родители следили за своими детьми и могли вовремя им помочь в интернет рутине. Обеспечение безопасности детей в интернете — это важно, но стоит быть реалистами: никогда не получится создать волшебный мыльный пузырь и оградить ребёнка от всего плохого, что существует в мире. Рано или поздно дети в интернете сталкиваются и с нежелательным контентом, и со страшными фильмами, и с травмами. Ваше дело

— помочь, поддержать, всегда быть рядом. Всегда оставайтесь на стороне ребёнка.