Муниципальное бюджетное общеобразовательное учреждение «Лицей №159»
г.Казани

Творческая работа свободного формата

на тему «Безопасность в Интернет — пространстве».

Выполнила ученица 8Б класса

Ефимова Софья

Казань, 2022

Содержание

1. Введение.
2. В чем заключается опасность Всемирной паутины?
3. Правила безопасности в интернете.
4. Полезные советики для пользователей интернета.
5. Заключение.
6. Опрос школьников «Сталкивались ли они с опасностями в интернете».

Казань, 2022

Введение

В последнее время практически ни один человек не может представить свою жизнь без Интернета, но мало кто знает, что такое Интернет на самом деле и какая у него история.

Интернет - это всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины и множества других систем (протоколов) передачи данных. Часто упоминается как «Всемирная сеть» и «Глобальная сеть». В обиходе иногда говорят «Инет».

Хотя первые сети для передачи информации появились еще в 60-е годы, образование единой общемировой информационной сети можно отнести к началу 90-х годов прошлого века. Сегодня Интернет стал своеобразной альтернативной реальностью, многогранным культурным феноменом и выгодным бизнесом.

Но также в нем есть и много опасностей. Как сделать Интернет безопасным для детей и подростков? Ведь многие дети, регулярно посещают социальные сети, просматривают Интернет. Данная работа посвящается вопросам безопасного интернета дома для детей и их родителей. ВКонтакте, Instagram, You Tube - знаменитые сайты, социальные сети постепенно начинают проживать с нами всё больше и больше времени. Мы сами не замечаем, как уже автоматически кликаем на очередную ссылку, регистрируемся на новом сайте и придумываем логин для еще одного сайта. Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но так ли он безобиден?

Актуальность проекта:

Люди все чаще и чаще используют интернет конечно же вопрос о безопасности встает на первое место. Безопасность использования интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

Цель:

Предостеречь пользователей всемирной сети от возможных опасностей .

Задачи:

Выявить угрозы, которые нас подстерегают при работе с Интернетом и разработать рекомендации для безопасности.

В чем заключается опасность Всемирной паутины?

Сегодня огромное количество информации обрабатывают с помощью персональных или рабочих компьютеров, поэтому атаки на компьютерные системы получили большую распространенность. С каждым годом число активных пользователей Интернета растет, следовательно проблема безопасности при работе в сети все более актуальна. К сожалению, знания пользователей о основах компьютерной безопасности при использовании Интернет отстают от темпов развития сети и роста угроз безопасности. Как ПО может представлять угрозу информационной безопасности в сети Интернет? К таким угрозам мы можем отнести:

- вредоносное программное обеспечение (вирусы), интернет-мошенничество;
- атаки на отказ в обслуживании;
- кражи денежных средств;
- кражи персональных данных;
- несанкционированный доступ к информационным ресурсам и систем;
- распространение заведомо недостоверной информации.

Кроме того, вам уже известны основные угрозы информационной безопасности пользователя Интернета, которые идут от авторизованных пользователей и электронных методов воздействия.

От авторизованных пользователей:

- Умышленные повреждения или похищения данных хакерами
- Повреждения данных в результате неосторожных действий

Электронные методы воздействия:

- Компьютерные вирусы
- Спам
- Фишинг (Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям)

Правила безопасности в интернете.

1. Установите антивирусные программы

Вирус – это вредоносная программа, которая проникает на ваш компьютер, ноутбук или смартфон различными способами. Она способна не только помешать работе, например, сделать недоступной часть постоянной памяти, но и похитить конфиденциальную информацию: логины, пароли, банковские реквизиты. Для защиты от вирусов существуют антивирусы.

2. Используйте сложные логины и пароли

Логин в виде имени, фамилии и пароль типа 1234 или QWERTY – не лучшая идея. Если кто-то всерьез решит похитить вашу конфиденциальную информацию, он расколет такую «защиту» в два счета. Хороший логин и пароль – это сложная комбинация, в которой используются заглавные и строчные буквы, цифры и символы.

3. Выходите из своих аккаунтов на чужих устройствах**.**

Воспользовались чужим компьютером? После этого недостаточно просто закрыть страницу, на которую вы заходили. Не забывайте предварительно выходить из всех аккаунтов, соцсетей и мессенджеров на устройстве. В противном случае человек, который сядет за этот компьютер после вас, получит возможность войти в вашу учетную запись и сделать с ней все, что ему заблагорассудится.

4. Проверяйте безопасность соединений

Всегда обращайте внимание на то, что написано в адресной строке. Если вы видите, что адрес сайта начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP – это значит, что соединение не защищено. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию во всплывающем окне.

5. Будьте внимательны к соединениям **Wi-Fi**

Общедоступные соединения есть, например, в кафе, торговых центрах и аэропортах. Не используйте их, если собираетесь вводить логины, пароли, либо совершать оплату услуг и товаров через интернет. Либо вообще не пользуйтесь ими ни при каких обстоятельствах и ограничьтесь обычным мобильным интернетом.

6. Организуйте безопасный режим для ребенка

На многих компьютерах и мобильных устройствах предусмотрен безопасный «Детский режим». Также можно настроить ограничения с помощью домашнего роутера – обычно эта функция называется «Родительский контроль». Еще один вариант – использование специальных детских расширений для браузеров. Любой из перечисленных выше вариантов сводит к минимуму вероятность того, что ребенок попадет на опасный сайт. И, конечно, заведите ему собственную учетную запись.

Казань, 2022

7. Создайте две почты — для работы и личную

Это не только удобно. Это еще и помогает отслеживать мошенников. Если на рабочую почту приходит письмо, в котором утверждается, что его автор учился с вами в одном классе и вы сами дали ему этот адрес – сразу ясно, что дело нечисто.

8. Не передавайте конфиденциальные сведения

Не пересылайте пароли, логины, паспортные данные, ПИН-коды и прочую подобную информацию в мессенджерах, чатах или по электронной почте. Не делайте этого, даже если ваш собеседник утверждает, что он – представитель службы безопасности банка. Если есть сомнения, лучше перезвоните в ваш банк или иную организацию, сотрудником которой представляется человек, и уточните информацию.

9. Не храните сканы документов в почте

Лучше вообще не пересылать сканы и фотографии документов по электронной почте, в чатах и мессенджерах. Если такая необходимость все же возникла, например, по работе или если нужно дистанционно направить заявление, после удалите письмо или сообщение в мессенджере. Но перед этим убедитесь, что адресат получил документы.

10. Ограничьте информацию о себе в интернете

Лучше не выкладывать на всеобщее обозрение свой номер телефона, адрес электронной почты и другую контактную информацию. Если это нужно сделать в связи с должностными обязанностями или поиском работы, создайте адрес электронной почты и номер телефона, которые будут использоваться только для этого. Многие социальные сети позволяют настраивать список тех, кто может просматривать ваш профиль и отправлять сообщения. Можно, например, сделать так, чтобы писать вам было разрешено только тем, с кем у вас подтверждена дружба – и при этом, конечно, стоит убедиться, что вы имеете представление о каждом своем онлайн-друге.

11. Не открывайте подозрительные письма

Прежде чем открыть письмо, пришедшее на электронную почту, прочитайте заголовок и посмотрите, с какого адреса оно было отправлено. Если тема вам неинтересна, заголовок составлен с грубыми ошибками, адрес представляет собой хаотичное нагромождение символов или напоминает название вашего банка, но с переставленными буквами, сразу отправляйте письмо в корзину. И никогда не открывайте файлы .exe в подозрительных письмах.

12. Не переходите по подозрительным ссылкам

Даже если всплывающая ссылка обещает что-то очень интересное и выгодное, лучше не кликать на нее. Если ссылку прислал вам знакомый, причем без каких-либо комментариев, сначала уточните, что он имел в виду. Возможно, его взломали, и теперь мошенники используют его профиль для рассылки вредоносных программ.

14. Не устанавливайте сомнительные приложения

Есть два безопасных источника приложений:

официальные магазины, созданные Apple, Google, Microsoft и другими подобными компаниями;

официальные сайты компаний, разработавших приложения.

Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов.

15. Будьте аккуратны в интернете с незнакомцами

Виртуальная красавица (или красавец) предлагают обменяться интимными фотографиями? Не торопитесь соглашаться. Вы рискуете тем, что ваши снимки в жанре ню станут доступны в интернете всем желающим. Если вам предлагают личную встречу, тоже подумайте несколько раз. Романтическое свидание вполне может обернуться обычным ограблением.

16. И со знакомыми будьте аккуратнее

Люди и общение бывают разными: сегодня вы лучшие друзья, а завтра злейшие враги. И совместные фотографии, видео, цитаты из переписок могут быть использованы против вас. Поэтому прежде чем отправить что-то личное даже хорошо знакомому человеку, подумайте, не превратится ли в последующем этот контент в компромат.

17. Блокируйте подозрительных пользователей

Если у вас появились подозрения, что тот, кто пишет вам в интернете – мошенник, смело блокируйте его. Это не займет много времени, но поможет сберечь нервы и денежные средства. Многие из мошенников знают, как вызвать жалость, обмануть, запугать и заговорить человека. Поэтому с такими людьми лучше даже не вести бесед и смело отправлять в черный список. Также у нас есть удобная услуга «Безопасный режим», подключив которую, нежелательные сообщения, спам и интернет-подписки будут блокироваться автоматически – обратите внимание.

18. Будьте осторожны с бесплатными предложениями

Видите слова «бесплатно», «заработок без вложений», «скидки 99%» или что-нибудь еще в этом роде? Обходите такие сайты стороной. Все они предлагают золотые горы, но на деле вы либо потеряете деньги, либо заплатите солидную сумму за дешевую китайскую подделку.

19. Создайте отдельную карту для платежей в интернете

Необязательно вводить данные вашей основной банковской карты в интернет-магазинах. Зарегистрируйте отдельную, с которой вы будете оплачивать все онлайн-покупки, и не храните на ней большие суммы. Если ее реквизиты как-то попадут к мошенникам, ваши финансовые потери не будут слишком серьезными.

Полезные советики для пользователей интернета.

- Помните, в Интернете вы общаетесь с живым человеком. Представьте, как бы вы общались с этим человеком в реальной жизни. Точно так же общайтесь с ним и в Интернете. Будь то ваш друг, новый знакомый на сайте или на форуме или специалист онлайн-поддержки, который готов вас проконсультировать по разным вопросам.
- Если у вас возникла какая-нибудь проблема, не поленитесь поискать ее решение на форумах. Возможно, кто-то уже дал ответ на ваш вопрос. Если захотите развить старую тему и создадите интересное и уместное сообщение (называется такое «некропостинг»), то оно способно реанимировать забытый всеми топик и поднять его на первую страницу.
- Будьте дружелюбными с другими пользователями, не используйте грубых слов. Помните, как вы будете общаться с людьми, так и они с вами. Хамить и грубить в Интернете – это не круто. Хотя бы потому, что в реальной жизни вы бы так не сделали.
- Если вам грубят, оскорбляют, унижают – не отвечайте. На сайтах и форумах есть такая функция – заблокировать обидчика или пожаловаться на него модератору. Воспользуйтесь ей и не бойтесь: хулиган не узнает, что это сделали вы.
- Никогда не отправляйте незнакомым людям номера мобильного и домашнего телефонов, домашний адрес, адрес электронной почты. Это личные данные, а личные – это значит, только ваши.
- Хорошо подумайте перед тем, как разместить свои фотографии в Интернете. Представьте, как вы будете себя чувствовать, если ваши фотографии не очень приличного содержания увидят родители или учителя.
- Если все-таки какой-то гадкий человек преследует вас, сохраните все его письма или смски и покажите взрослым, которым доверяете: родителям, старшим братьям и сестрам.

Казань, 2022

Опрос на тему «Знают ли ученики 8 класса правила безопасности в Всемирной паутине»

Чтобы узнать полезны ли вообще проекты, сообщения, доклады на данную тему, я решила провести опрос среди одноклассников. В результате опроса половина класса не знала многих опасностей, которые могут их ждать в интернете. Благодаря этому мы можем сделать вывод, что тема «Безопасность в Интернет – пространстве» очень даже актуальна и нуждается в распространении.

Заключение

Мной достигнута цель моей работы: «Предостеречь пользователей всемирной сети от возможных опасностей».

Также я выполнила все задачи выше поставленные мной, а именно выявила угрозы, которые нас подстерегают при работе с Интернетом и разработала рекомендации для безопасности.

Как я и думала, эта тема оказалась очень актуальна в наше время. Я рада, что мой проект принесет пользу другим людям, а может быть и остановит их от глупых поступков.

Спасибо, что уделили время моему проекту! Надеюсь, он оказался полезным для вас)

Казань, 2022