проект

Тема: **БЕЗОПАСНЫЙ ИНТЕРНЕТ**

Сагимбекова Инеш Жарылгасыновна
учитель начальных классов
МБОУ СОШ № 54 г. Новосибирск

Новосибирск, 2025 г.

СОДЕРЖАНИЕ

Введение

Актуальность этой темы со временем будет только увеличиваться, так как интернет развивается, а видов преступлений в сети ежегодно растет. Интернет стал как параллельный мир, в котором «живут» и работают мошенники, преступники и просто люди, которым нравится создавать проблемы другим.

Цель проекта: Научиться распознавать потенциальные опасности и угрозы в сети, чтобы обезопасить себя и других школьников от киберпреступлений.

Задачи:

1) Познакомить с основными видами мошенничеств в сети.

2) Показать на примерах, последствия неправильных действий в сети.

3) Рассказать, как предотвратить неприятности, которые могут встретиться в интернете.

4) Создать памятку поведения в сети для школьников.

ГЛАВА1.Вредоносные программы

Вирусы, шпионы, черви- название вредоносных программ, которыми можно заразить свой смартфон, планшет, ноутбук или компьютер, и даже смарт-часы. Эти программы пишут программисты с различными целями, и если самый безобидный – это просто поломать ваш гаджет, то самым распространенным является похищение вашей личной информации, такой как личные фотографии, сведения о вас, включая ваше ФИО, адрес, номера телефонов, имена ваших друзей и т.д. Есть несколько основных способов заражения ваших гаджетов:

- через флешку, которую вы не проверили перед тем, как вставить в свой компьютер;
- возможно вы зашли на какой-то вредоносный или зараженный сайт;
- прошли по ссылке, которую вам выслал знакомый, которая содержала вирус;
- или скачали в интернете программу или игру, от непроверенного производителя.

WI-FI - это точка доступа беспроводной сети. Она бывает индивидуальная и общедоступная – это когда к одной точке может подключиться много людей. Обычно ее используют в Торговых центрах, аэропортах, больницах и других местах, где обычно скапливается большое количество людей. Такие сети могут быть небезопасны. Злоумышленники могут украсть сведения взломав точку доступа, они получают всю информацию от подключенных устройств напрямую. Чаще всего крадут платежную информацию, сохраненные логины

и пароли и приватные файлы. Если по какой-то причине вы пользуетесь такой сетью – лучше использовать ее для просмотра фильмов или соцсетей, но без отправки личной информации. Оплаты, авторизации, пересылка личных данных – лучше проводить через личный интернет в своем мобильном устройстве.

Глава 2. Способы и виды мошенничества в сети

Фейк – это недостоверная информация, выдуманная новость, то, чего нет, чья-то выдумка. В интернете можно встретить много разной информации. Информация, так же как и оружие может таить опасность. Вырабатывайте в себе способность критично мыслить – не верить всему, что пишут и показывают в интернете. Ведь сейчас даже видео с самим президентом может быть просто фейком. Умение фильтровать информацию – это высший уровень пользования интернетом.

Как распознать, что перед вами фейк?

1. Посмотрите, из какого источника пришла информация;
2. Дата публикации новости;
3. Спроси у эксперта (мамы, папы, учителя);
4. Будь умным – знание лучшее оружие!

Что делать, как защититься?

1. Создать надежный (сложный) и разный пароль на разных аккаунтах.
2. Двухфакторная аутентификация. Это метод аутентификации, требующий от пользователя предоставить два фактора проверки для получения доступа к веб-сайту, приложению или ресурсу.
3. Не переходить по ссылкам, даже если вам прислали его друзья, не убедившись, что это безопасная ссылка.

ФИШИНГ – с перевода с английского означает «рыбачить». Это сайт «Под капирку», с измененной буквой в названии сайта. Мошенники подделывают интернет страницу и выдают ее за настоящую. И ловят вас, как рыбку на удочку. Так, вместо настоящего сайта, вы попадаете на сайт-копию, который принадлежит мошенникам.

ВИШИНГ – Это попытка мошенников обманом выведать личные сведения по телефону. Чаще всего – это код подтверждения. Когда звонящий вас торопит, угрожает и затронута тема денег или срочно нужно назвать код, который пришел на ваш телефон, можете быть уверены – это мошенники!

СМИШИНГ – мошенничество, посредством СМС. Т.е. мошенник отправляет на телефон сообщение со ссылками на левые сайты, которые требуют от вас ввода персональных данных.

Как же защититься от этих угроз?

1.Сбросить звонок, не вступайте в общение.
2. Проверяйте адреса сайтов, не переходите по незнакомым ссылкам.

3. И самое главное – говорите родителям обо всех подозрительных звонках и сообщениях.

Глава 3. Виды манипуляций в сети

Всех мошенников, независимо от того, каким способом они связываются с вами, объединяют способы манипуляций, с помощью которых они достигают своих целей. Они играют на человеческих чувствах и пороках. Вот несколько примеров.

ХАЛЯВА: «Вы выиграли Айфон-14! Срочно отправьте код с СМС сообщения».

СТЫД: «Привет, увидел ролик с тобой. Ну ты даешь! Ты вообще в курсе, что тебя снимали? Вот ссылка: youtubbe.com/sadasdds»

ЖАЛОСТЬ: Здесь мошенники давят на жалостливые и благородные чувства интернет пользователей. Например, отправляют фото бедных животных в приютах и просят денег на их содержание, или показывают фото больных детей и организуют сборы на лечение.

«Друзья, поспрашивайте, кому нужны щенки бегло. Не могут раздать и хотят усыпить. Жалко! Может кому нужно? Бесплатно! +7 903 722 02 03. Максимальный репост!»

СТРАХ: Это чувство, которое неизбежно возникает, если нам или родным угрожают. Вы с большой долей вероятности испугаетесь за родителей и будете выполнять требования мошенников.

«Доча, это мама. Мы с папой попали в аварию, папа в больнице. Срочно нужны деньги. Пришли на этот номер фото карты с двух сторон. На мой телефон не звони!!! Срочно!!»

Если сомнительное предложение поступает от знакомого контакта или того, кто представляется знакомым, нужно обязательно перепроверить информацию с использованием тех номеров, что есть у нас в телефонной книге. Позвоните другу и спросите, он ли вам пишет? Или, может, его взломали.

Если звонят или пишут с незнакомого номера – блокируем номер и сообщаем родителям.

Глава 4. Общение в сети

Существует три основных способа общения в сети:

1. Анонимный (в играх). Вы общаетесь абсолютно с любыми пользователями, не ограничивая себя, но никому не раскрывайте свою личность. При этом вы тоже не знаете, кто ваш собеседник в игре, т.к. в онлайн игры играют люди всех возрастов и с разных точек земного шара. Поэтому используйте вымышленный Никнейм и никому не сообщайте данные о себе в игре, т.к. риск столкновение в играх с мошенниками очень высок. Никогда не переносите общение из игры в личные мессенджеры, не сообщайте номеров телефонов, настоящего имени и других личных данных. В случае подозрительной активности таких игроков, сразу блокируйте и прекращайте общение.

2. Личный профиль. Такой профиль в основном используется в социальных сетях. В личных аккаунтах правило такое: в друзьях только те, кого мы знаем лично. А страницу лучше закрыть и не вступать в переписку с незнакомыми пользователями. Критично относится к сообщениям даже от друзей, ведь их страницу тоже могут взломать злоумышленники.

3. Публичный профиль. Публичным ваш аккаунт становится тогда, когда вы не знаете хотя бы одного из своих подписчиков. Здесь правила еще более жесткие. Поэтому самостоятельно вести публичный блог очень опасно. На данном уровне необходимо не только уметь противостоять хэйту, но и хорошо знать законы и многое другое. Но самое главное правило – что интернет все помнит, и даже если вы удалите сообщение или свою публикацию, фотографию – все это может быть использовано против вас.

В общении в сети важно:

- С кем вы общаетесь и кого добавляете в близкий круг.
- О чем вы беседуете и какую информацию о себе отправляете. Исключите из общего доступа и личной переписки персональные данные: ваш Е-мэйл, номер телефона, паспортные или банковские данные, адрес, геолокацию, номер школы.
- Знаете ли вы как отфильтровать опасных людей и группы? Вас должно насторожить, если новый друг в сети представляется блогером, популярным певцом, представителем модельного агентства. Такие люди не будут писать вам в личные сообщения и, как правило, у публичных людей социальные сети ведут помощники, а не лично сами звезды. Также существуют 4 темы, которые должны тебя насторожить и говорят об опасности:

1. Контент, не соответствующий возрасту (например политика, темы отношения между мужчиной и женщиной, сообщения с просьбой отправить фото в интимном виде или в купальнике или предложения о просмотре какого-то странного ролика);

2. Денежные спекуляции (призывы к заработку, игры на деньги, сообщения, в которых вам сообщают о том, что ты выиграл приз или предлагают бесплатный смартфон, присылают ссылки для участия в конкурсах и опросах с денежными призами);
3. Насилие или призывы к насилию (насилие над кем-то или упоминание об оружии, войне);
4. Смерть (обсуждение смысла жизни, или предложения совершить над собой какие-то действия, наносящие вред своему телу или здоровью, причем эти приказы могут звучать с угрозами и шантажом).

Важно во всех этих случаях все рассказать родителям!

Во всех соцсетях есть кнопка пожаловаться на человека или группу, в которой такой диалог состоялся.

Заключение

Работа над проектом была проведена в 4 этапа:

1. Поиск информации по безопасности в интернете;

2. Изучение основных видов преступлений в сети и способы их предотвращения;

3. Разговоры с друзьями и одноклассниками о кибербезопасности, узнать, насколько они информированы о данной проблеме.

4. Обобщить информацию и создать памятку поведения в сети для школьников.

В процессе работы были проведены исследования: просмотр различных обучающих видео о безопасности в сети, чтение статей, посвященных этой теме, изучение реальных примеров преступлений.

В ходе решения задач были получены следующие результаты:

1. Знания об основных вредоносных программах, которые используются хакерами и другими кибер-преступниками, для преступлений в сети.

2. Получение информации о способах мошенничества в сети и основных видах опасности в интернете.

3. Узнала характерные особенности манипуляций мошенников и как не попасться к ним на их уловки.

4. Обобщила правила общения в сети.

5.Составила краткую памятку по безопасности в интернете.

По результатам работы сделаны следующие выводы:

Безопасность в интернете зависит в первую очередь от информированности пользователей. Понимание, что все действия в сети, как и в реальной жизни, имеют реальные последствия. На мой взгляд, каждый ребенок, которому в

руки попадает гаджет (планшет, смартфон или компьютер) должен знать правила безопасности в сети. Возможно, в будущем в школе появится такой предмет, как кибербезопасность, и дети будут с детства учиться не только не попадать в руки мошенников, но и критично мыслить, учиться анализировать информацию и фильтровать информацию в сети. Все это сократит количество киберпреступлений.

В процессе работы над проектом, я сделала для себя главный вывод:
интернет, как и наша жизнь – это большие возможности, это громадная база информации, это параллельный мир, в котором мы живем. И только от нас зависит, как мы будем проживать эту жизнь в виртуальном мире.
Предупрежден – значит вооружен.

Каждый раз, выходя в интернет, я буду стараться быть бдительной. Для этого мне предстоит еще получить много знаний, чтобы иметь компетенцию в разных отраслях жизни. Учиться критично мыслить помогают знания. Я составила памятку, которая, я надеюсь, поможет не попадать в опасные ситуации в сети.

Список используемых ресурсов и литературы:

1.Проект Центрального банка России: www.fincult.info
2.Академия безопасности Ольги Бочковой: www.bochkova.academy
3.CISOCLUB – информационный портал и профессиональное сообщество специалистов по информационной безопасности Источник: https://cisoclub.ru/

Приложение 1

Памятка безопасного пребывания в сети

1. Пользуйтесь антивирусами, проверенными программами, сайтами и приложениями.
2. Выбирайте защищенное подключение.
3. Включайте критическое мышление. Образовывайтесь! Только ум и знания позволяют мыслить критично. Получайте информацию для своего самообразования только из надежных источников, например из школьных пособий. Это позволит фильтровать фейковые аккаунты и новости, чтобы исключить обман мошенников.
4. Общайтесь с людьми в сети, которых знаете лично в реальной жизни. Не стесняйтесь перепроверять информацию о тех, с кем переписываетесь. Не бойтесь обидеть собеседника отказом.
5. Берегите персональные данные и личную информацию.
6. Вовремя замечайте травлю в сети. Не позволяйте травить себя и своих друзей. Блокируйте и жалуйтесь на таких пользователей. Не вступайте с ними в диалог!
7. Обращайтесь к родителям за помощью!

.