ПРОЕКТНАЯ РАБОТА

Выполнил: ученик 9 «М» класса Махотин Иван

Руководитель: учитель информатики Добролюбова Н.П.

Введение

Актуальность работы заключается в том, интернет в наше время таит в себе много опасностей, и его пользователи не знают, как защитить себя от них.

Проблема: слабая защищённость пользователей и их компьютеров из-за плохих знаний.

Цель работы: создать инструкцию для повышения уровня безопасности людей, пользующихся интернетом.

Гипотеза: защищённость компьютеров и их пользователей увеличится, если люди будут больше знать об опасностях интернета.

1.1 Понятие компьютерных преступлений

Компьютерные преступления — это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и средством совершения преступления.

1.2. Опасности интернтернета

Коммуникационные — это потенциальные опасности, которые таит в себе интернет-общение. Сеть создает иллюзию доверительных отношений. Мы беспечно раскрываем перед широкой аудиторией подробности своей личной жизни, быстро переходим на доверительный уровень общения с незнакомцами. Одной из опасностей, связанной с коммуникационными рисками, является киберпреследование.

Интернет-мошенничество — это одна из важных и острых проблем всего Интернета. Постоянно появляются все новые и новые схемы по выкачиванию денег с наивных пользователей. Безнаказанность мошенников, анонимность и простодушность самих людей, вечно тяготеющих к легкой выгоде и простым решениям, создают благодатную почву для процветания мошенничества в Сети.

1.2.1 Экстремизм в Интернете

Информационный экстремизм – деятельность, направленная на социально-психическое деструктивное воздействие граждан через использование информационных технологий для достижения противоправных целей

Признаки ИЭ:

1.Антисоциальность

2.Аморальность

1.3 Фишинг

В основном воруются такие данные:

Имя, никнейм, адрес проживания пользователя.

Пароли, логины от почты и социальных сетей.

Номера телефона, банковского счёта.

Данные банковской карточки, её номер, CCV-код, PIN-код.

Номер социальной страховки.

1.3.1 Фишинговые письма

Фишинговые письма – это основной способ распространения ссылок на фишинговые сайты.

Признаки:

-Фишинговые письма обозначают надуманную проблему как срочную и жизненно важную, чтобы пользователь напугался и быстро прислал всё, что нужно. Также в таких письмах может быть много восклицательных знаков;

-В них множество стилистических и грамматических ошибок. Разумеется, никто не может на 100% застраховаться от опечатки или лишней запятой, однако рассылки от фишеров просто напичканы всевозможными описками, двойными либо тройными пробелами, ошибочными названиями сервисов и т.д.

1.3.2 Советы по защите от фишинга

Для защиты от фишеров следует учитывать следующие моменты:

1. Помните, что пароль – только ваш, ни одна организация не станет требовать его от вас. Он необходим только для доступа к определённому сервису и только вы должны знать его.
2. Внимательно проверяйте каждое полученное почтовое сообщение с неизвестного адреса на предмет наличия всевозможных просьб перейти по ссылке.
3. Всегда проверяйте с помощью адресной строки, на том ли сайте вы вводите свои идентификационные данные. Обычно подделывается и домен, поэтому он бывает похожим на свой оригинал. Различие может заключаться лишь в одной букве (например, mail.ru легко превращается в meil.ru).
4. Используйте последние версии интернет-браузеров и лицензионные антивирусные программы.
5. При входе на банковские сайты следите за тем, чтобы было установлено защищённое соединение https

РАЗДЕЛ 2: ПРАКТИЧЕСКАЯ ЧАСТЬ

Я провёл опрос среди учащихся своего класса. Я раздал брошюры с советами по защите информации, рассказал про кибербезопасность и все отвечали на вопросы викторины. До и после лекции я проводил тест. Результаты теста:

1)До классного часа: 15 из 27 человек ответили на тест правильно.

2)После классного часа: 24 из 27 человек ответили на тест правильно.

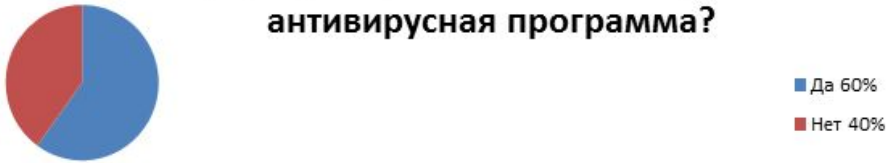
2.1. Результаты анкетирования

В проведенном анкетировании приняли участие 27 человек в возрасте 15-16 лет. Каждый из них пользуется интернетом. Что бы было все наглядно и удобно видно, я представлю это в виде круговой диаграммы.

1)Был ли у тебя какой-либо неприятный случай, связанный с Интернетом?

2)А в какие именно неприятности?

3)Присутствует ли на твоём гаджете антивирусная программа?



4)Поддерживаете ли вы свою киберграмотность?

РАЗДЕЛ 3: ВЫВОДЫ И РЕКОМЕНДАЦИИ

Исходя из всего вышесказанного, можно сделать вывод что:

1.Всегда нужно быть внимательным пользуясь сетью и быть готовы к различным уловкам мошенников.

2.Не вводить свои данные на сторонние сайты, которым мало доверяешь

3.Быть внимательным при переходе по ссылкам и всегда смотреть на домен.

4.Не открывать подозрительные письма приходящие на электронный ящик.

Заключение

Цель проекта я выполнил, после проведения классного часа мои одноклассники узнали, как защитить свою информацию и практически все ответили на тест правильно. Гипотеза мною также была доказана. На лекции они узнали, как защитить себя и свой компьютер, и я думаю, что они будут пользоваться этими знаниями в жизни.

Эта тема будет актуальна всегда, так как постоянно будут появляться новые способы обмана людей, но на данный момент я считаю, что при изучении этой темы никаких вопросов у меня не появилось.