Творческий Проект

<<Безопасность в интернете>>

Выполнил:

Володин Владислав

Ученик 9в класса

Куратор:

Ольга Леонидовна

Учитель информатики

- **Цель работы**: Раскрыть источники угроз, которые несет всемирная сеть.
- **Задача работы**: Выявить угрозы, которые нас подстерегают при работе с Интернетом, и разработать рекомендации для безопасности.
- **Объект исследования**: Безопасность в Интернете.
- **Предмет исследования**: Использование правил безопасности при работе в сети Интернет
- **Методы исследования**: беседа, сравнение, обобщение, анкетирование, статистическая обработка данных.
- **Работа состоит** из введения, двух глав, заключения, списка используемой литературы.

Глава 1. Где находятся источники угроз, которые несет всемирная сеть?

+ Самыми распространенными из них являются:
+ Социальная инженерия, основанная на определенных психологических уловках и рассчитанная на доверчивых пользователей;
+ Большинство вирусов спрятано в различных бесплатных программах для скачивания;
+ Заражение компьютера может происходить через так называемые дыры в программном обеспечении, которые умело используют хакеры;
+ Зачастую вирусы внедряются посредством фишинга (организации поддельных сайтов, которые копируют странички популярных фирм);
+ С какими целями злоумышленники взламывают персональный компьютер? Среди основных целей стоит выделить:
+ кражу паролей от почтовых ящиков, различных сайтов, аккаунтов, а также электронных кошельков;
+ осуществление рекламных рассылок.
+ Опасности, подстерегающие при регистрации в социальной сети?
+ Регистрируясь в Одноклассниках, Контакте или Твиттере, следует быть очень осторожными. Известно, что при регистрации предлагается внести свои персональные данные, а также предоставить фото. Далее для облегчения поиска друзей рекомендуется заполнить данные о месте учебы, работы, указать номер мобильного телефона, для того чтобы получить на него СМС-сообщение для смены пароля.
+ Чтобы избежать угрозу мошенничества необходимо не рассказывать о себе. Особенно это касается социальных сетей. Везде, где вы зарегистрированы, измените свои настройки конфиденциальности. Ваш профиль должен быть виден только вашим друзьям. Это касается и публикации статусов, и сообщений в ленте, на вашей стене и т.д.

Что мы знаем о мошенниках?

+ Существуют различные виды мошенничества:
+ **Кардинг** - способ мошенничества с использованием банковских карт. Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя.
+ **Фишинговые сообщения** - это уведомления, отправленные от имени администраторов банковских или других платежных систем. Они призывают пользователей пройти по фальшивой ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету.
+ **Уведомления о выигрыше:** В письме сообщается о том, что ты выиграл крупную сумму денег. Цель мошенника - выманить у тебя деньги за получение выигрыша.
+ **Попрошайничество:** Мошенники давят на жалость и отправляют письма с просьбой о помощи якобы от благотворительных организаций или нуждающихся людей.
+ В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные**.**
+ Незнакомцы с которыми общаемся в сети могут оказаться:
+ Маньяками, педофилами, извращенцами.
+ Интернет-ХАМАМИ (Тролли) которые провоцируют на необдуманные поступки и необоснованную агрессию!
+ Киберпреступниками зачастую обманом похищающими чужое имущество!
+ Хакерами использующими анонимность для распространения вредоносного программного обеспечения, завладения учётными данными, платёжными реквизитами, персональной информацией.

Глава 2. Как избежать угроз, которые несёт всемирная сеть?

+ В этой главе рассмотрим советы и рекомендации на вопросы: Как не стать жертвой мошенников? Как определить подделку? Как обезопаситься?
+ Во-первых, используй функционал браузера: «избранное», «закладки» и проверяй адрес сайта.
+ Во-вторых, обрати внимание на настоящий адрес сайта (при наведении мыши реальный адрес отображается во всплывающей подсказке) и проверь систему антивирусом.
+ В третьих авторизуйся под своими аккаунтами и убедись, что все в порядке или смени пароли к аккаунтам, которые используешь.
+ Ещё одной угрозой вашему компьютеру является спам. Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания. Поэтому необходимо помнить, что идя на поводу у СПАМа есть риск:
+ Отправить платное СМС, оплатить навязанную услугу.
+ Получить платную подписку на ненужную информацию.
+ Потерять учётные и (или) иные данные и стать жертвой обмана.

+ Советом как избежать угрозы от спама является:
+ настройка безопасности браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты);
+ использование дополнительного расширения браузеров, которое позволяет блокировать СПАМ и рекламные блоки;
+ использование Антивируса и файервола.
+ Файервол - это специальная программа, которая служит для предотвращения несанкционированного доступа к вашему компьютеру.
+ Необходимо осторожно использовать свои персональные данные при общении в социальных сетях. Наши советы следующие:
+ При регистрации в социальных сетях используй только Имя или Псевдоним (ник).
+ Настрой приватность в социальных сетях и других сервисах.
+ Не публикуй информацию о своём местонахождении и (или) материальных ценностях!
+ Хорошо подумай, какую информацию можно публиковать в Интернете.
+ Не доверяй свои секреты незнакомцам из Интернета.

Как обманывают в Интернете?

- Общаясь в социальных сетях и работая в Интернете можно попасть на обман, который выглядит следующим образом:
- Просят подтвердить логин/пароль.
- Предлагают бесплатный антивирус, а устанавливают вредоносное ПО, вирусы.
- Просят отправить СМС (платное).
- Крадут пароли.
- Распространяют вредоносное ПО.
- Навязывают платные услуги.
- Просят указать персональные данные.
- Кому нужны наши персональные данные?
- 80% преступников берут информацию в соц. сетях.
- Личная информация используется для кражи паролей.
- Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение!
- Чтобы не быть обманутым в открытых и небезопасных сетях, нужно помнить, что подключение к ложной сети может моментально лишить всей персональной информации, хранящейся в электронном устройстве: преступнику станут доступны пароли, и другая информация. Опасно оставлять свои учётные данные на устройстве, которое тебе не принадлежит, этими данными могут воспользоваться в преступных целях.

Советы по безопасности

- Удаляй письма, которые содержат не относящуюся к тебе информацию, связанную с денежными средствами, особенно от неизвестных людей. Не будь слишком доверчивым, проверяй всю информацию, содержащую просьбы о помощи, иначе помощь потом потребуется тебе самому. Не сообщай посторонним лицам свои персональные данные, номера счетов, пин-коды и т.п. Не переходи по ссылкам, указанным в подозрительных письмах. Используй антивирусную защиту и регулярно обновляй систему и антивирус. Настрой дополнительные функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска). Используй официальное лицензионное и (или) свободное программное обеспечение.
- В уголовном кодексе Российской федерации существуют статьи, которые наказывают за обман, мошенничество в социальных сетях, только пока в нашей стране не всегда находят хакеров и мошенников.

Сравнительный анализ использования советов по безопасности В Интернете студентами колледжа

+ В анкетировании участвовало 47 человек Была предложена анкета, состоящая из 5 вопросов..

+ ***1.****Где вы пользуетесь интернетом чаще?*

+ 2.Используете интернет:

+ 3.Какой вред здоровью несет интернет?

+ 4. Какую информацию нельзя сообщать?

+ 5. Ваш возраст и пол?

- Все анкетируемые и мужчины, и женщины независимо от возраста ответили, что в основном Интернетом пользуются дома.
- Как средство общения используют Интернет студентки до 18 лет, а после 18 лет – в основном для выполнения рефератов и докладов

Заключение:

- Анкетирование показало, что иногда многие забывают о безопасности при работе в Интернете. Поэтому необходимо напоминать пользователям ПК основные правила безопасности в Интернете, какие угрозы их подстерегают. Ведь предупреждён, значит вооружён.
- В работе были рассмотрены различные виды угроз и даны советы, как их избежать.
- Компьютерные вирусы и другие вредоносные программы.
- Интернет – мошенники
- Материалы нежелательного содержания
- Интернет-зависимость
- Психологическое воздействие через интернет
- Каждый должен помнить правила поведения в Интернете:
- Никому не сообщай свой логин с паролем и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.
- Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете.
- Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.
- Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям.

Список литературы

1. Юрьева, Т. Ю. Словарь информационных продуктов и услуг / Т.Ю. Юрьева. - Кемерово.: - РОСТИКС,2006.- 50 с.
2. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / Петр Николаевич Девянин. — М.: Издательский центр «Академия», 2005. — 144 с.
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.
4. Башлы П.Н. Информационная безопасность / П.Н. Башлы. —Ростов н/Д: Феникс, 2006. — 253 с.
5. Мельников В. П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. — М.: Издательский центр «Академия», 2005. — 336 с.

Спасибо за внимание!