ОПАСНОСТИ СОЦИАЛЬНЫХ СЕТЕЙ.

АВТОР:

ЖМУРОВ ЛЕОНИД РУСЛАНОВИЧ

УЧЕНИК 9А КЛАССА

РУКОВОДИТЕЛЬ:

ПОЛУЭКТОВ НИКОЛАЙ АЛЕКСЕЕВИЧ

УЧИТЕЛЬ ИНФОРМАТИКИ.

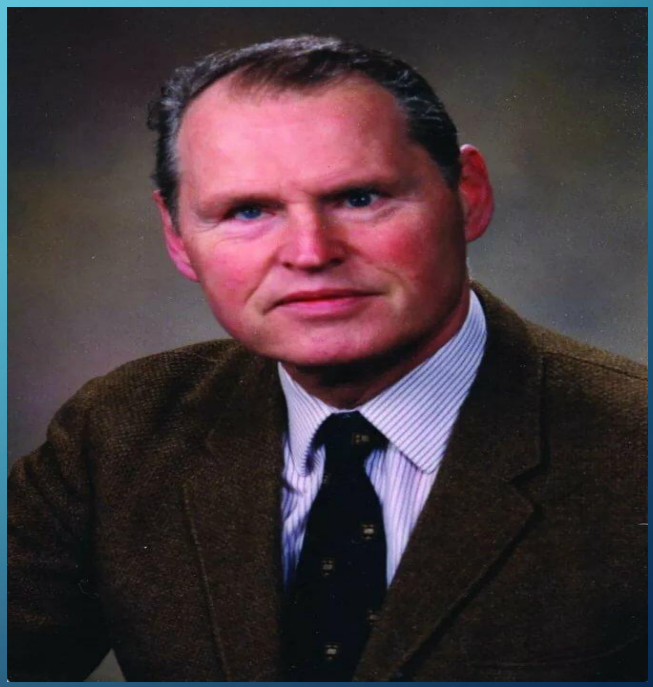
ЧТО ТАКОЕ ИНТЕРНЕТ И ЗАЧЕМ ОН НУЖЕН?

Развитие технического процесса породило такое явление как всемирная паутина – интернет. Без него мы уже не можем представить себе существования. А такое явление современного интернета, как социальные сети, приобрели множество поклонников среди населения. Но при этом мало кто из нас задумывается, что социальная сеть – это не только удобство и комфорт в общении, но и потенциальный источник опасности.

- **Актуальность:** Практически у каждого человека в этом мире есть цифровое устройство, телефон, и все люди у которых он есть могут быть подвержены опасности в социальной сети.
- **Цель:** Рассказать о самых распространённых опасностях Социальных сетей, и мерах безопасности
- **В ходе работы над проектом я поставил такие задачи:**
- Изучить литературу по данной теме;
- Проанализировать материал;
- **Гипотеза:** Наши личные данные опубликованные в какой-либо социальной сети, могут быть уже у

ПОНЯТИЕ И НАЗНАЧЕНИЕ СОЦИАЛЬНЫХ СЕТЕЙ, ПРИМЕРЫ:

- Термин «Социальная сеть» был введен в обиход в 1954 году социологом Джеймсом Барнсом. Социальная сеть - это Социальная структура, состоящая из узлов (ими могут быть люди, группы людей, сообщества и организации), связанных между собой тем или иным способом посредством Социальных взаимоотношений.



ВИДЫ СОЦИАЛЬНЫХ СЕТЕЙ:

- · Универсальные социальные сети. Например, Facebook, Вконтакте, Одноклассники и т.д.
- · Деловые социальные сети. Используются в основном для установки и поддержания деловых контактов. К таким сетям относятся LinkedIn, Мой Круг.
- · Тематические социальные сети. Здесь происходит объединение пользователей по интересам, например, сети веб-мастеров, программистов, фанатов игр и т.д. Например, в России существует социальная сеть ЗаБаранкой, объединяющая автолюбителей; Догстер - социальная сеть для собаководов и многие другие.
- · Геосоциальные сети. Налаживают социальные связи между участниками на основании физического положения пользователя, предоставляя ему возможность создавать профили мест, где он был. Например, AlterGeo, Foursquare.
- · Возрастные и гендерные сети. Создаются для общения одной возрастной или гендерной группы. Например, женские социальные сети myJulia.

ПСИХОЛОГИЧЕСКАЯ ЗАВИСИМОСТЬ ОТ СОЦИАЛЬНЫХ СЕТЕЙ:

- Психологи утверждают, что современное подрастающее поколение и люди средней возрастной категории привыкли к общению в Социальных сетях на столько, что у многих из них развилась серьезная зависимость.
  Если человек в утренние часы после пробуждения сразу открывает интернет в своем мобильном телефоне или на компьютере, то это является серьезным поводом задуматься..
- Как правило, зависимы от Социальных сетей на первом месте подростки. Тем не менее, среди зависимых можно найти людей более старшей возрастной категории.
- Страдающий Интернет аддикцией, теряет навыки общения с людьми. Любой диалог на улице с малознакомым человеком, способен вызвать стресс. Он все бесконечно жмет на кнопку обновить страницу, в Социальных сетях. У таких людей портится зрение, возникают рези в глазах. Происходит это вследствие того что, долгое пребывание за ярким экраном ухудшает глазные мышцы. Возникают проблемы со спиной и суставами. При долгом сидении происходит застой крови в тазовой области. Для мужчин это чревато проблемами плодотворности и потенции.

ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ В ЛИЧНЫХ ЦЕЛЯХ:

- И самой главной опасностью является свободный доступ к персональным данным, которые размещают на своей страничке социоманы, не задумываясь при этом, что-то кто может ими воспользоваться.
- Размещая информацию о себе в Социальных медиа, вы должны быть готовы к тому, что ее может увидеть большое количество людей. В итоге, ваша частная жизнь становится достоянием общественности.
- Довольно часто мошенники взламывают странички пользовательских аккуантов в Социальных сетях с целью получения доступа к персональным данным, размещенным в профиле или рассылке спамной информации от имени пользователя.

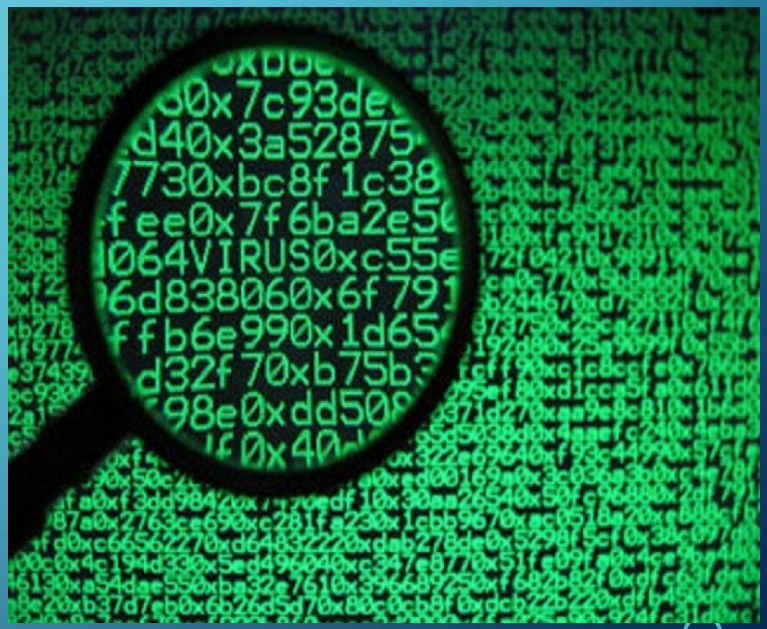
ФАЛЬШИВЫЕ СТРАНИЧКИ ДЛЯ КРАЖИ ВАШИХ ДАННЫХ:

- В глобальной сети уже достаточно давно прогрессирует хорошо продуманный вид мошенничества, целью которого является завладение вашей учетной записью для того чтобы похитить Вашу контактную и Социальную информацию или управлять аккаунтом для подачи информации от Вашего имени. Этот вид хакерской атаки называется фишингом и состоит в том, чтобы подсунуть ничего не подозревающему пользователю подложную веб-страницу с формой для ввода логина и пароля. После передачи данных пользователь может перейти уже к настоящей странице социальной сети, вот только вся секретная информация уже будет отправлена злоумышленнику.

- Схема подлога достаточно проста. На почту или мессенджер пользователя приходит сообщение с предложением завести дружбу в социальной сети, скачать интересную игру, послушать музыку, посмотреть новый видеоролик. При этом хорошо замаскированная ссылка, указывающая на ресурс, ведет к точной копии страницы какой-нибудь социальной сети. Все это может быть закамуфлировано настолько профессионально, что пользователь даже не догадается об обмане и сам передаст мошеннику все свои данные.

ОБМАН НА ДОВЕРИИ:

- Любая схема мошенничества основывается на доверии. В Социальных сетях такой вид преступления для злоумышленников имеет наиболее благодатную почву. Представьте, что от Вашего хорошего друга или родственника приходит сообщение с просьбой одолжить немного электронных денег, скачать новую программу или перейти по отправленной ссылке. При этом если Ваш приятель стал жертвой злоумышленников, похитивших его данные от учетной записи, то выполнив такую просьбу Вы можете, либо навсегда лишиться отправленных денег, либо заразить свою систему вирусом от закачанного контента. Конкретный вид ущерба зависит от цели, с которой мошенники решат связаться с Вами.



ПУБЛИЧНАЯ ИНФОРМАЦИЯ:

- Чем больше Вы оставляете информации о себе на Социальных веб-страницах, тем более упрощаете задачу мошенникам, собирающим подобные сведения для нахождения подходящих жертв. В милицейских сводках появляется все больше сведений о преступниках, нашедших своих жертв посредством Социальных сетей. Будьте благоразумны, оставляя о себе те или иные данные на страницах Интернета. Ваша безопасность в Ваших же руках.

Заключение:

В заключение над проектом, я бы хотел вас рассказать о правилах безопасного общения в Социальных сетях:

1. Не сообщайте в Социальных сетях о том, где вы находитесь в данный момент:

Одно дело – позвонить приятелям или членам семьи и сообщить, что вы сегодня задержитесь на работе, в гостях, в баре и т.д. Совсем другое – рассказать об этом нескольким сотням людей, многих из которых вы никогда не встречали в реальной жизни.

2. Остерегайтесь публиковать в интернете свои личные данные:

Выкладывание в интернете подробностей своей личной жизни может привести к тому, что злоумышленники будут о вас знать едва ли не больше, чем ваши ближайшие родственники.

4. Не сообщайте о дорогих покупках, которые вы совершаете:

Грабители выискивают потенциальных жертв, у которых есть деньги и дорогие новенькие гаджеты. Когда вы беззаботно рассказываете о дорогих покупках — вы даете сигнал потенциальным грабителям, что не плохо было бы порыться в вашей квартире или автомобиле.

9. Не сообщайте подробностей, которые кибер-хулиганы и тролли могут использовать против вас:

Не сообщайте в Социальных сетях подробности о себе, а также не публикуйте фото, которые кто-то может использовать для