The background is a complex digital visualization. It features a grid of glowing blue and red lines, with various data points and trends. Binary code (0s and 1s) is scattered throughout, some appearing as large, glowing characters. There are also faint bar charts and line graphs overlaid on the scene, suggesting data analysis or network activity. The overall color palette is dominated by deep blues, teals, and vibrant reds, creating a high-tech, futuristic atmosphere.

Мошенничество в сети
Интернет
Выполнил: Шабала Дмитрий

Цель исследования

- + Создать рекомендации по безопасному использованию сети Интернет, сделав из них буклет.

Задачи

Рассмотреть историю появления мошенничества.

Рассмотреть влияние мошенничества на пользователей.

Рассмотреть основные способы мошенничества.

Рассмотреть способы борьбы с мошенничеством.

Проинформировать учеников нашей школы о том, как не попасться на уловки мошенников.

Сделать рекомендации по безопасному использованию сети Интернет.



История появления

Российская Федерация является уникальным со всех сторон развития общества государством. Самобытность истории, и путей развития Россия определяется как обширными территориями страны, так и этнологическим составом населения. Развитие Российской преступности так же проходило самобытно, при этом, на разных исторических этапах развития общества она видоизменялась, выражаясь в новых формах

Влияние мошенничества на пользователей интернета

Жертвы мошеннических действий, а также пользователи знания которых недостаточны для защиты своих личных данных, зачастую перестают пользоваться и доверять ресурсам, находящимся в сети:

интернет-магазинам.

площадкам с объявлениями.

личным кабинетам банковских услуг и т.п.

Виды мошенничества :

Ложные сайты

Вредоносные программы

Сокращенные URL-адреса

Подозрительные запросы на добавление в друзья

Запросы от людей, которые уже были в списке друзей

Сообщения о чрезвычайных ситуациях

Практическая часть

- **Подводя итоги, мы решили сделать памятку, какие действия нельзя совершать в сети интернет:**

Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость! Не оставляйте номер своего мобильного на сомнительных сайтах!

Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.

Проверьте регистрационные данные самого сайта, на какую компанию или частное лицо было зарегистрировано доменное имя и как давно.

Если вам предлагают работу, то платить должны вам, а не вы. Не отправляйте деньги за регистрацию, за почтовые расходы, как залог за комплектующие, с которыми вам предстоит работать и т. п.

Почитайте отзывы других пользователей сети об этой компании, сайте или лице.

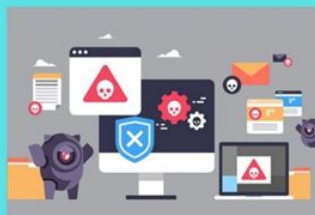
Вывод

- + При работе над проектом *«Мошенничество в сети Интернет»* выполнены все поставленные задачи:
- + Просмотрели историю появления мошенничества.
- + Узнали какое влияние оказывает мошенничество на пользователей Интернета.
- + Рассмотрели основные способы мошенничества.
- + Проинформировали учеников нашей школы, посредством создания буклета.
- + Составили рекомендации по безопасному использованию сети интернет.
- + Продукт нашей деятельности позволяет ознакомиться с основными правилами безопасного использования сети Интернет.

Приложение

МАОУ ЦО №82 "РАЗВИТИЕ"

Вредоносные программы в Интернете



Рекомендации по обеспечению безопасной работы в Интернете

1. Антивирусные программы – ваши первые защитники

Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. Обновления – это полезно и безопасно

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. Настройте свой компьютер против вредоносных программ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети. Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. Проверяйте новые файлы

Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов. Подозрительные сообщения лучше немедленно удалять.

5. Будьте бдительны и осторожны

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их. При получении извещений о доставке почтовых сообщений обращайтесь внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. Резервное копирование – гарантия безопасности

Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

Литература

- + Баранов, И.Р. Виды телекоммуникационного мошенничества / И.Р. Баранов // Вестник Владимирского юридического института. – 2015. – № – С. 218-243.
- + История развития мошенничества, современные виды мошенничества и способы борьбы с ними - Алпатов, А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / А.С. Алпатов // Трибуна молодого ученого. – 2016. – № 2. – С. 16-37.
- + Колескин Д. В. История развития мошенничества, современные виды мошенничества и способы борьбы с ними // Социально-гуманитарные проблемы современности: сборник научных трудов по материалам Международной научно-практической конференции 24 апреля 2020г. : Белгород : ООО Агентство перспективных научных исследований (АПНИ), 2020. С. 37-42.