Факультет программной инженерии и компьютерной техники

Лабораторная работа №8

«Мини-исследование: Утечка данных и цифровая гигиена»

по дисциплине «Информационная безопасность»

Выполнил:

Студент группы P3432

Чмурова М.В.

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2025

Задание

1. Проверьте свой основной email-адрес на сайте https://haveibeenpwned.com/ (сервис проверяет, не фигурирует ли ваша почта в известных утечках данных). Внимание: Используйте только email! Не вводите здесь свои пароли!
2. Если ваши данные были найдены, проанализируйте, в каких утечках они фигурируют и какие данные были скомпрометированы (пароли, имена, номера телефонов и т.д.).
3. Проведите аудит своих публичных данных в социальных сетях (ВК, Telegram и др.). Какая информация о вас доступна незнакомым людям?
4. На основе проведенного анализа составьте 5-7 личных правил цифровой гигиены (например, "не использовать один пароль на разных сайтов", "проверять настройки конфиденциальности в соцсетях раз в полгода").

Выполнение

Для проверки на вышеуказанном сайте воспользуюсь своей основной почтой:

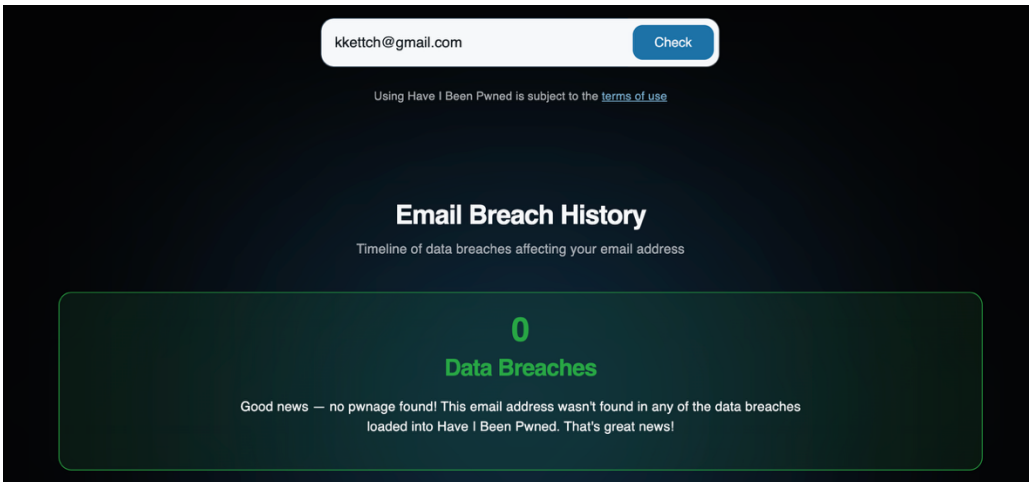

Рисунок 1. Проверка основной почты

Так как сайт показал, что никаких утечек почты не было найдено, проведу проверку все остальных email адресов, которые я использую. При следующей же проверку нахожу 4 утечки на разных сайтах за период с 2018 по 2024 год с таких сайтов, как: Trello, Twitter, Shein

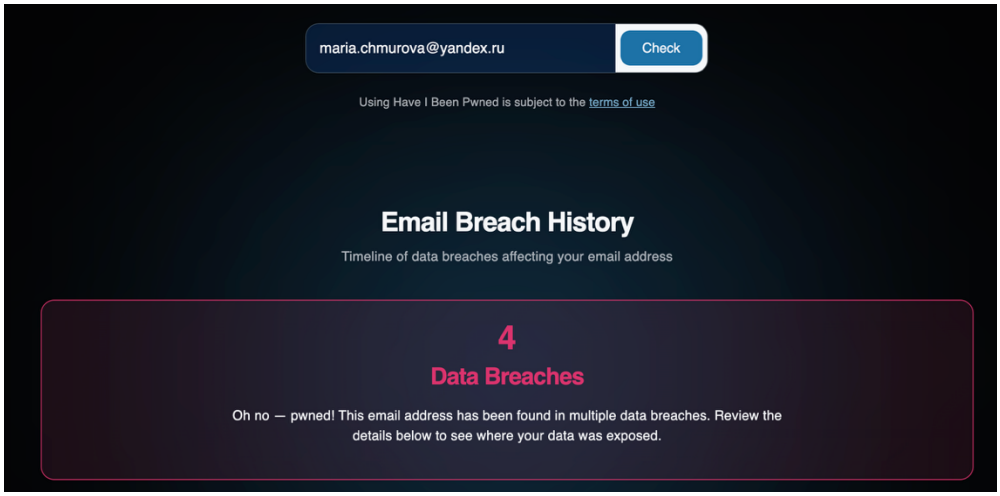

Рисунок 2. Проверка дополнительной почты

Основными скомпрометированными данными являются адрес электронной почты, имя, фотографии профиля. Однако с двух сайтов была слита информация паролей: один из них в виде хэшей bcrypt и другой в виде хэша паролей MD5

Для оставшихся проверенных email не были обнаружены утечки.

Аудит доступной другим людям информации

vk.com: Я давно активно не пользуюсь этой соцсетью, однако на ней остается публичной некоторая моя информация. Такая как: мои фотографии, дата рождения, город проживания, место обучения. А также список моих друзей. Однако на ней недоступна информация о моих подписках и моей музыки.

Telegram: В нем почти не указано никакой публичной информации обо мне, за исключением моих фотографий. Номер телефона и дата рождения скрыты.

WhatsApp: Содержит публичное указание моей фотографии профиля

Instagram: Содержит публичное указание моих подписок, моих фотографий, недавних поездок, ссылок на другие соц. сети.

В целом, можно сделать вывод, что наиболее открытой соц. сетью является Instagram. Для минимизирования цифрового следа можно ограничить доступ к аккаунту и скрыть персональные данные (фото, ссылки на другие аккаунты)

Правила личной гигиены

1. Использовать двухфакторную аутентификацию – с ее помощью можно защитить учетные записи от взлома даже при утечке пароля, так как вход без дополнительного кода будет невозможен
2. Не публиковать точное местоположение и информацию о текущих поездках – лучше делать это по возвращению, когда уже не находишься в том месте, на котором ставишь геометку. Это снизит риск отслеживания перемещений и возможных краж во время отсутствия
3. Избавиться от кросс-ссылок между соцсетями – это затруднит сопоставление аккаунтов и усложнит деанонимизацию

4. Регулярно удалять старую и ненужную информацию – в том числе удалять неиспользуемые аккаунты. Это уменьшит объём личных данных, доступных посторонним
5. Проверять настройки конфиденциальности каждые полгода – в том числе на каких устройствах произведен вход в аккаунт. Также это поможет вовремя ограничить видимость личных данных при изменениях политик соцсетей
6. Быть осторожным с фишингом: не переходить по подозрительным ссылкам в письмах и сообщениях – это защитит от кражи логинов и паролей через фальшивые сайты.
7. Регулярно обновлять приложения и операционную систему – обновления могут включать исправления уязвимостей, которыми могут воспользоваться хакеры на старых версиях

Вывод

В ходе данной лабораторной работы, я узнала, что некоторые сайты подвергались утечкам моих персональных данных. Безусловно, это полезная информация для того, чтобы осознать масштаб своего цифрового следа и принять меры в случае необходимости. Таким образом, работа демонстрирует, что цифровая гигиена - это конкретные действия: от очистки старых аккаунтов до регулярной проверки настроек, которые минимизируют ущерб от прошлых и от возможных будущих утечек.