Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа №8

«Мини-исследование: Утечка данных и цифровая гигиена»

Барсуков Максим Андреевич

Группа: P3415

2025

Выполнение

Проверка email-адреса на наличие в утечках

Для проверки использовался сервис Have I Been Pwned (https://haveibeenpwned.com/). Так как никакой из моих основных email-адресов не был найден в утечках, я проверю на сайте olga_neijko@mail.ru (почта одного из родителей). Как видно на рисунке 1, почта фигурирует в пяти утечках, произошедших в период с 2017 по 2022 год.

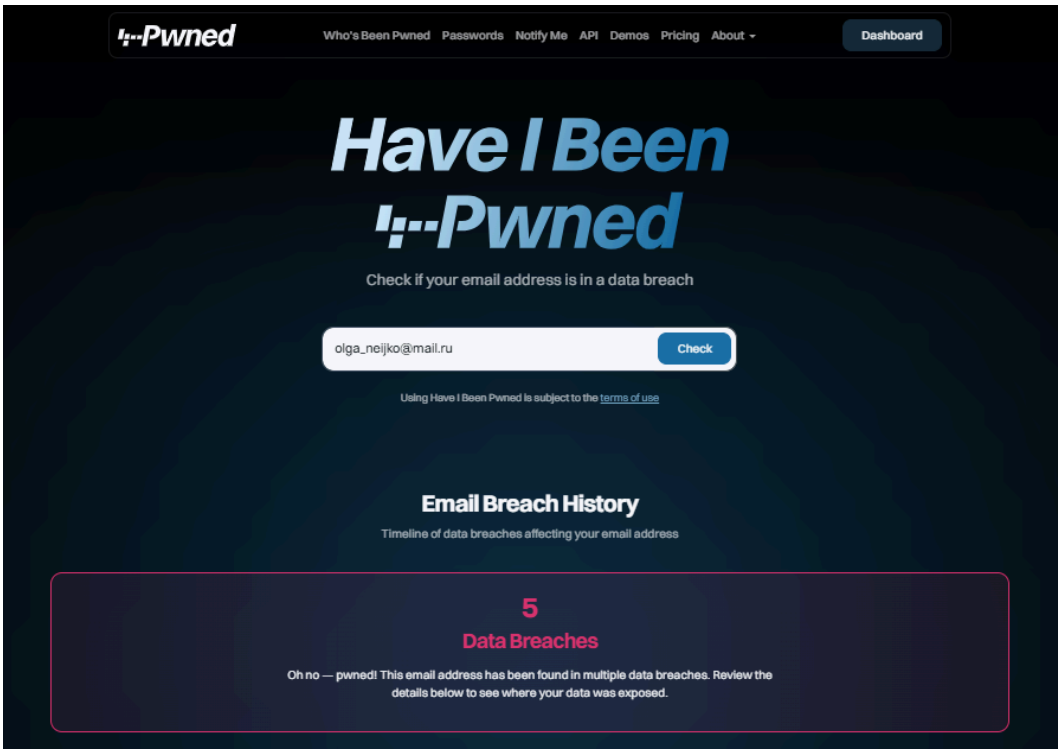

Рисунок 1 — Результаты проверки email-адреса в сервисе

Утечки произошли в сервисах Online Trade, CDEK, и MyHeritage, а также были обнаружены в коллекциях Cit0day и Collection #1.

В сервисе Online Trade скомпрометированы данные: дата рождения, email, IP-адреса, хэши паролей (MD5), имя, номер телефона (рисунок 2):

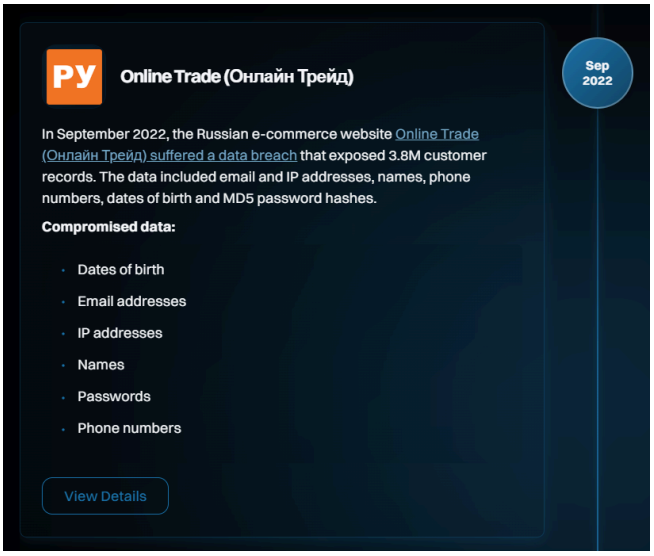

Рисунок 2 — Отчет по утечке данных от платформы Online Trade

В опубликованной базе сервиса CDEK содержались 19 млн записей с email-адресами, именами и номерами телефонов клиентов курьерской службы (рисунок 3). Следует отметить, что достоверность этой утечки не подтверждена независимо, и она помечена как «unverified». Тем не менее, наличие данных в открытом доступе создает риски для целевой фишинговой атаки:

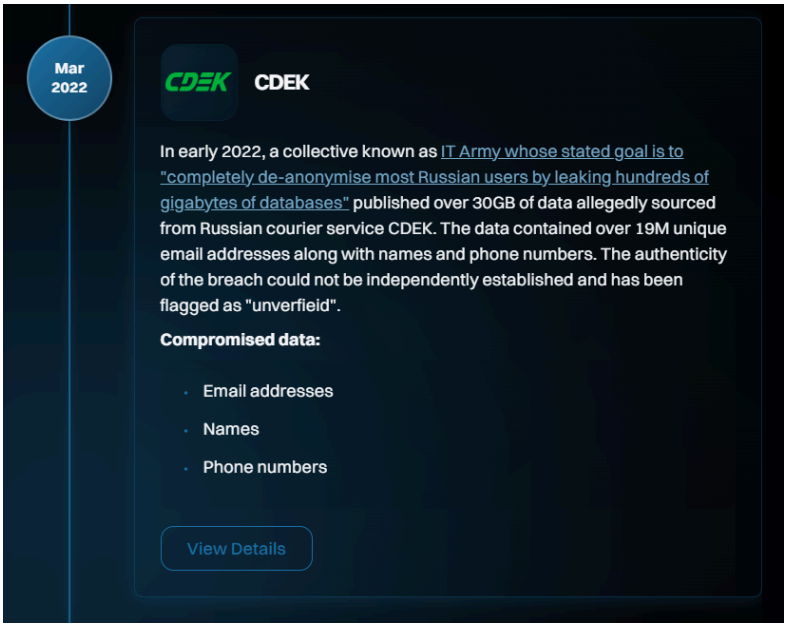

Рисунок 3 — Отчет по утечке данных от платформы CDEK

В сервисе MyHeritage раскрыты email-адреса и хэши паролей (salted SHA-1), как показано на рисунке 4:

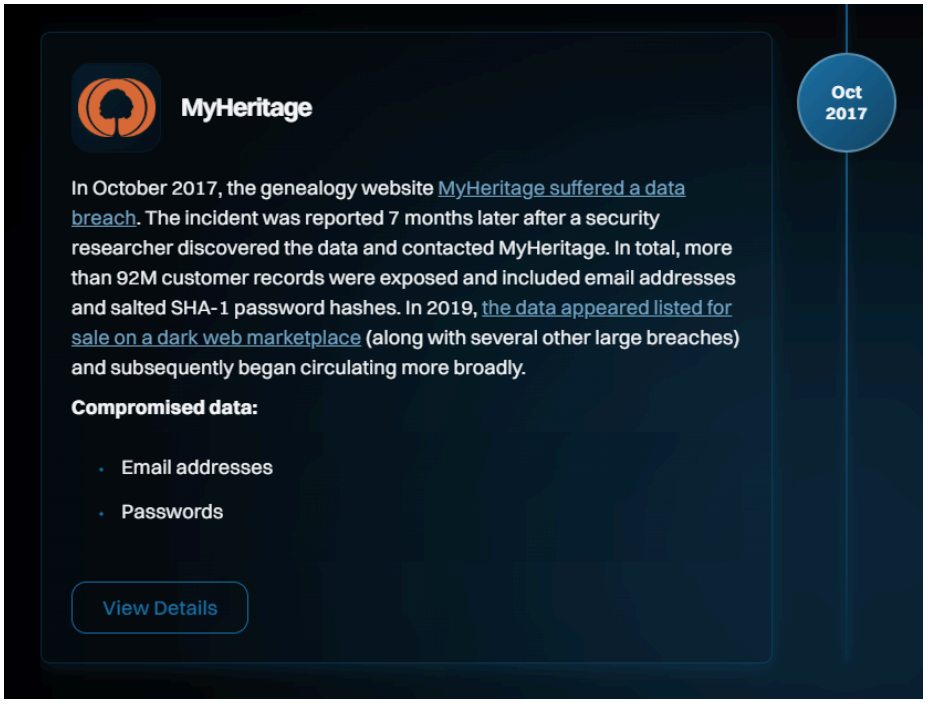

Рисунок 4 — Отчет по утечке данных от платформы MyHeritage

Также почта обнаружена в коллекциях утечек Cit0day и Collection #1, где скомпрометированы email и пароли (рисунки 5-6). Коллекция Cit0day включала данные из более чем 23 000 скомпрометированных сайтов. В ней содержались как хэши паролей, так и их расшифрованные (plain text) версии. Это делает утечку особенно опасной, поскольку злоумышленники могут напрямую использовать пароли для входа в другие аккаунты (атака типа credential stuffing):

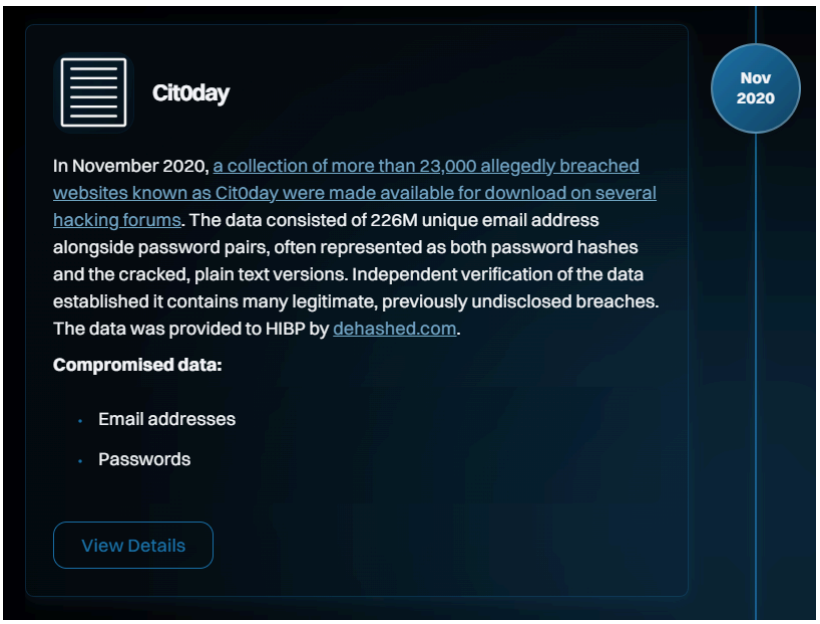

Рисунок 5 — Отчет по утечке данных в коллекции Cit0day

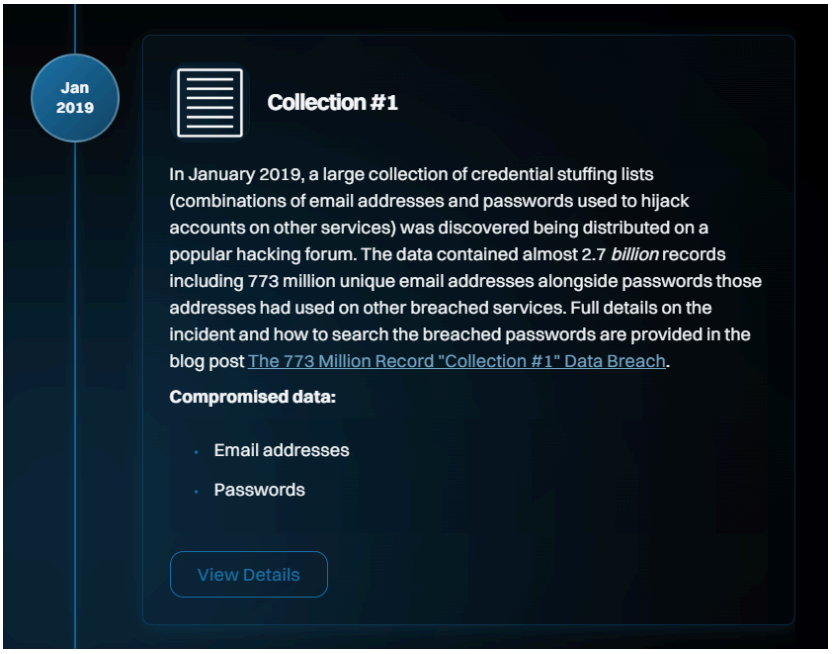

Рисунок 6 — Отчет по утечке данных в коллекции Collection #1

Аудит публичных данных в социальных сетях

Проведен анализ профилей в следующих платформах:

1) ВКонтакте: для пользователей вне списка друзей доступны только имя и фамилия, аватарка профиля не содержит изображения меня в жизни, видно подписки на группы, связанные с ИТМО (то есть можно предположить город и учебное заведение), как показано на рисунке 7.

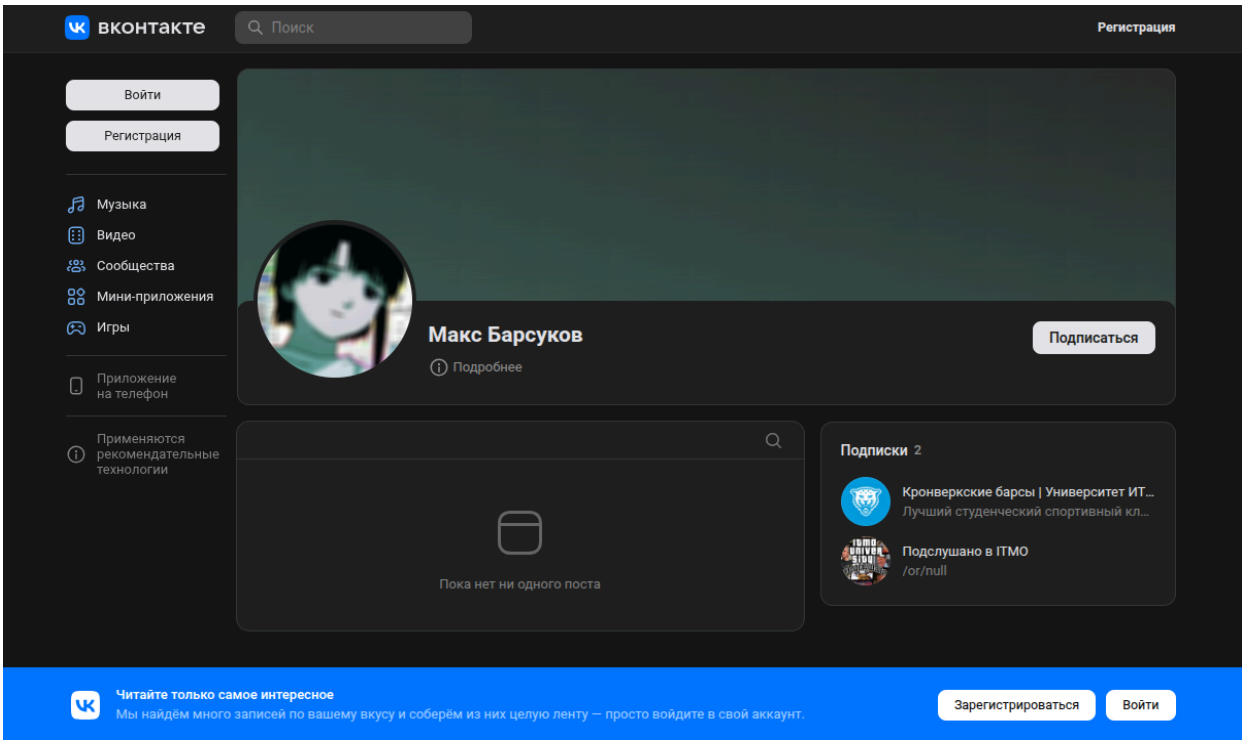

Рисунок 7 — Доступные данные на странице ВКонтакте

Никакие личные данные на странице не заполнены. Настройки приватности не позволяют незнакомцам просматривать список друзей.

2) Telegram: отображается имя, фамилия, никнейм и фото профиля, раздел «О себе» не заполнен, а прикрепленного telegram-канала нет. Номер телефона доступен только контактам, как показано на рисунке 8.

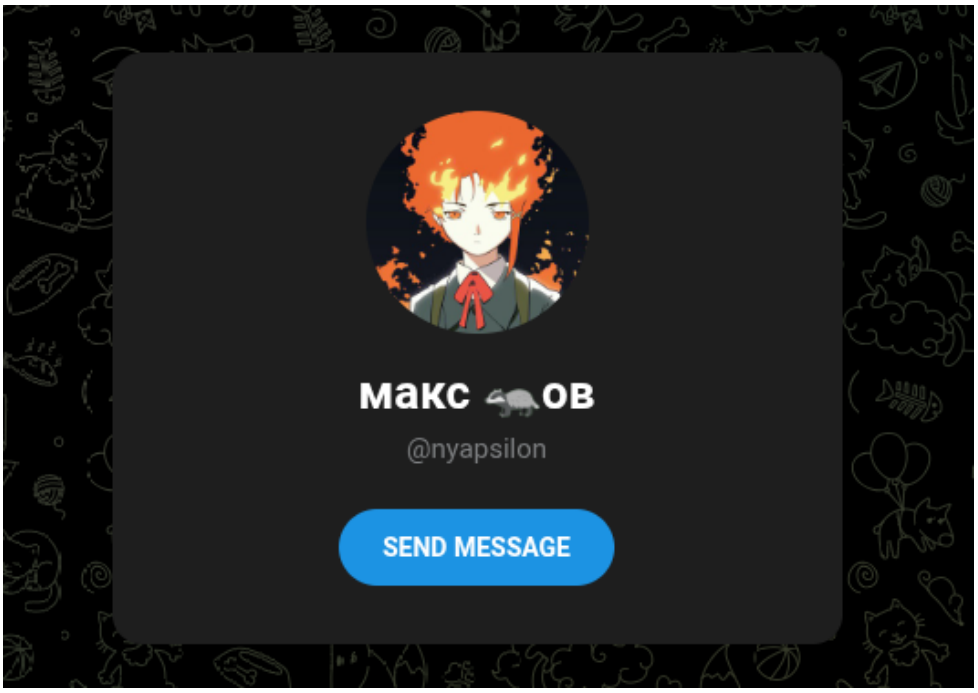

Рисунок 8 — Доступные данные для аккаунта в Telegram

Личные правила цифровой гигиены

На основе проведенного анализа сформулированы следующие правила:

1. Использовать уникальные сложные пароли для каждого сервиса и хранить их в менеджере паролей (например, Bitwarden).
2. Включить двухфакторную аутентификацию (2FA) на всех аккаунтах, поддерживающих эту функцию.
3. Раз в квартал проверять и корректировать настройки приватности в социальных сетях.
4. Не публиковать в открытом доступе информацию, которая может быть использована для восстановления доступа к аккаунтам (дата рождения, место учёбы, номер телефона).
5. Регулярно проверять, какие устройства и сессии авторизованы в ваших аккаунтах. Многие сервисы (Google, VK, Telegram, Apple ID и др.) позволяют просматривать активные сессии. Раз в месяц заходить в настройки безопасности и завершать подозрительные или устаревшие сеансы.
6. Ограничить использование геолокации в приложениях и соцсетях. Отключить геотеги в фото и не публиковать посты с точным местоположением в реальном времени — это снижает риски физического преследования, кражи или социальной инженерии.
7. Не публиковать в профиле прямые ссылки на мои аккаунты в других сервисах.