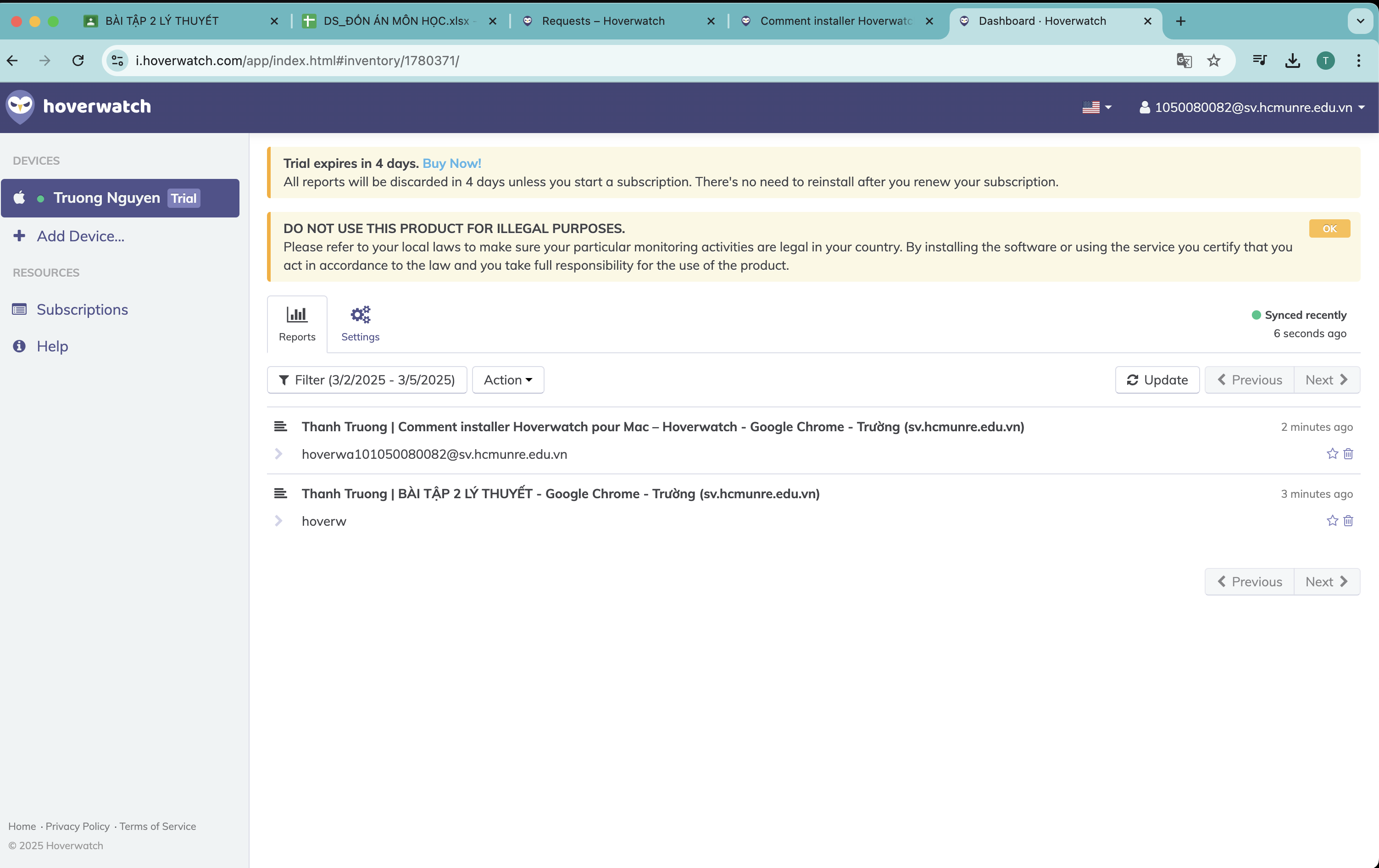
Bài tập lý thuyết 2

Tên: Nguyễn Thanh Trường

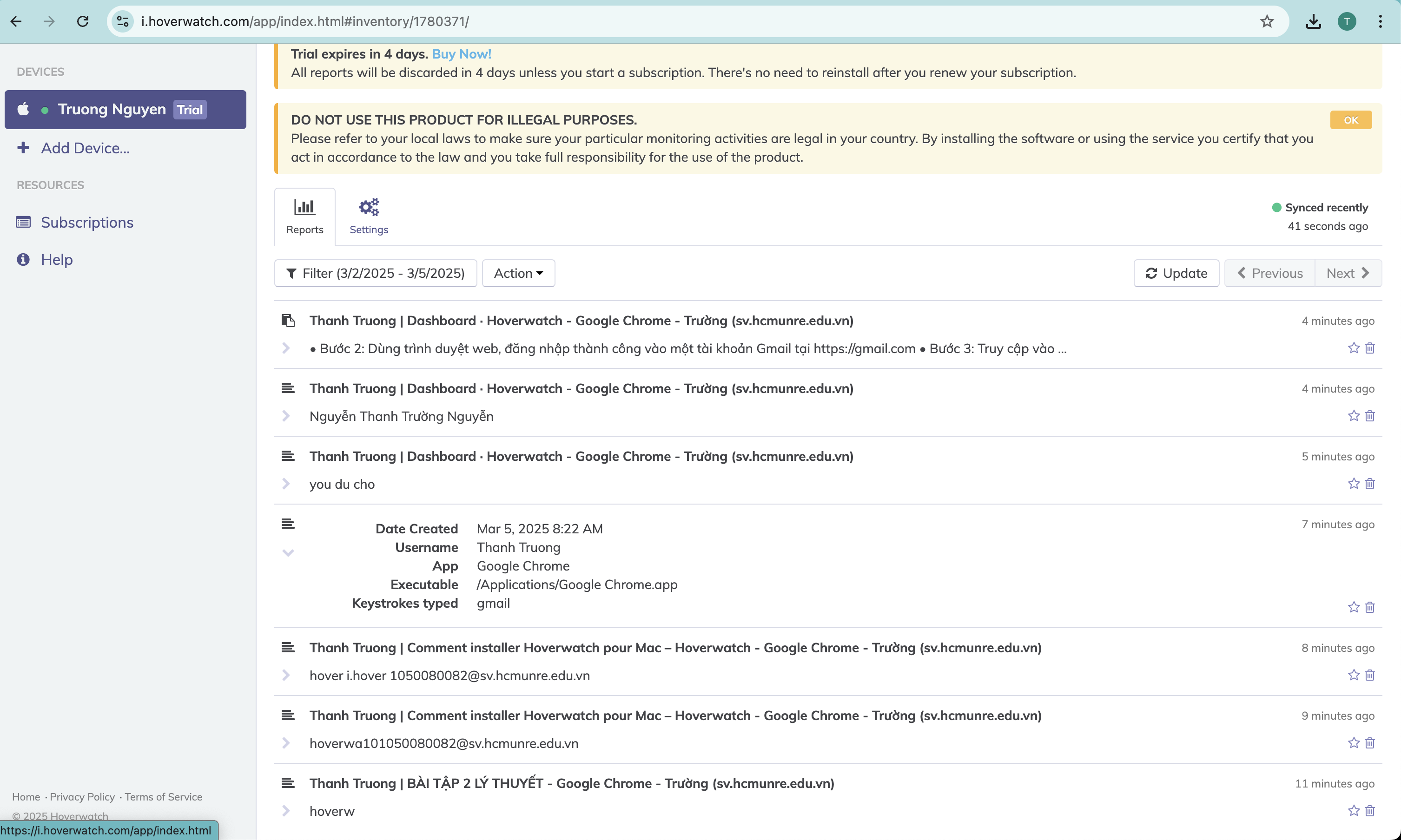
Lớp: 10\_ĐH\_CNPM1

MSSV: 1050080082

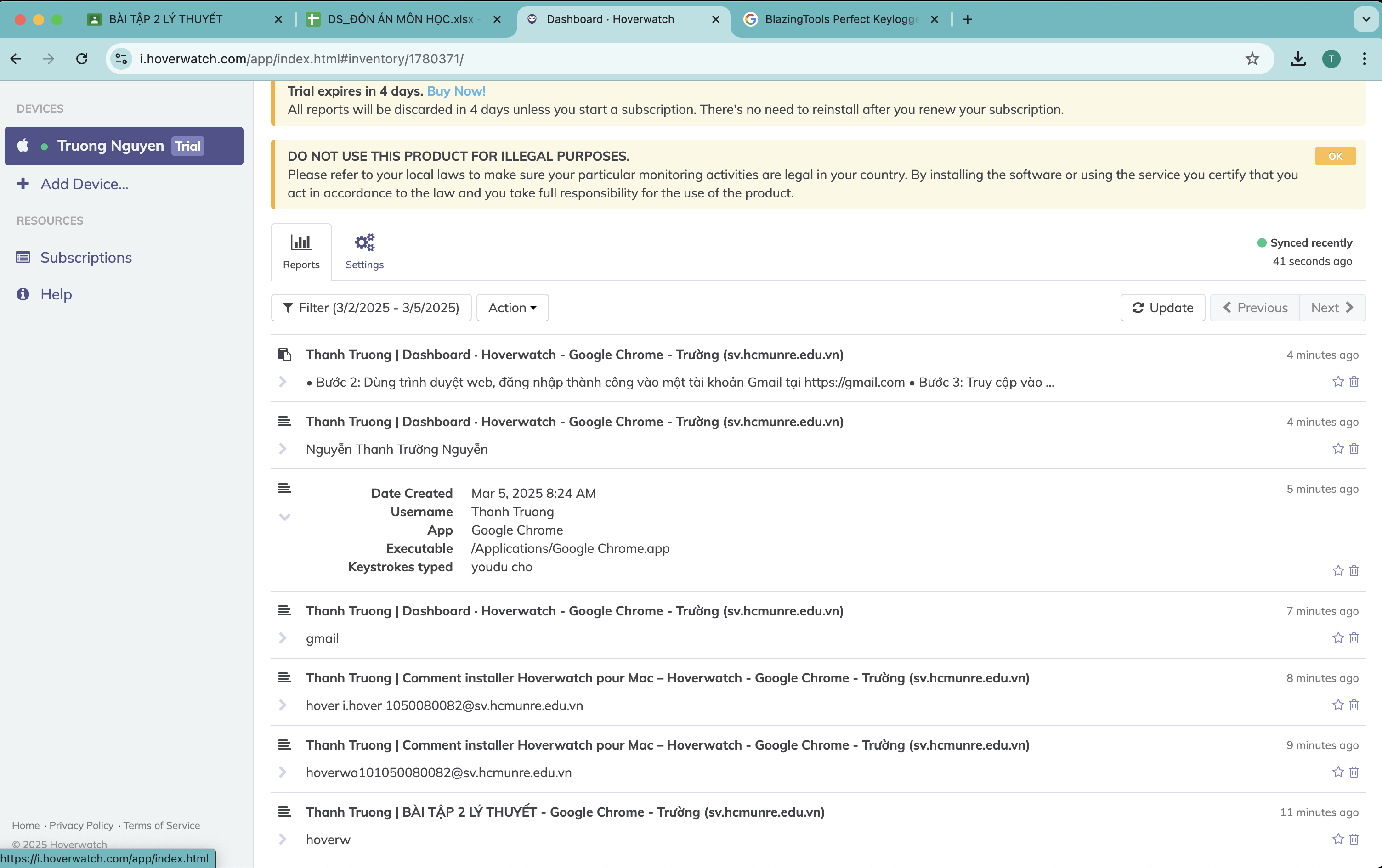


• Bước 2: Dùng trình duyệt web, đăng nhập thành công vào một tài khoản Gmail

tại <https://gmail.com>

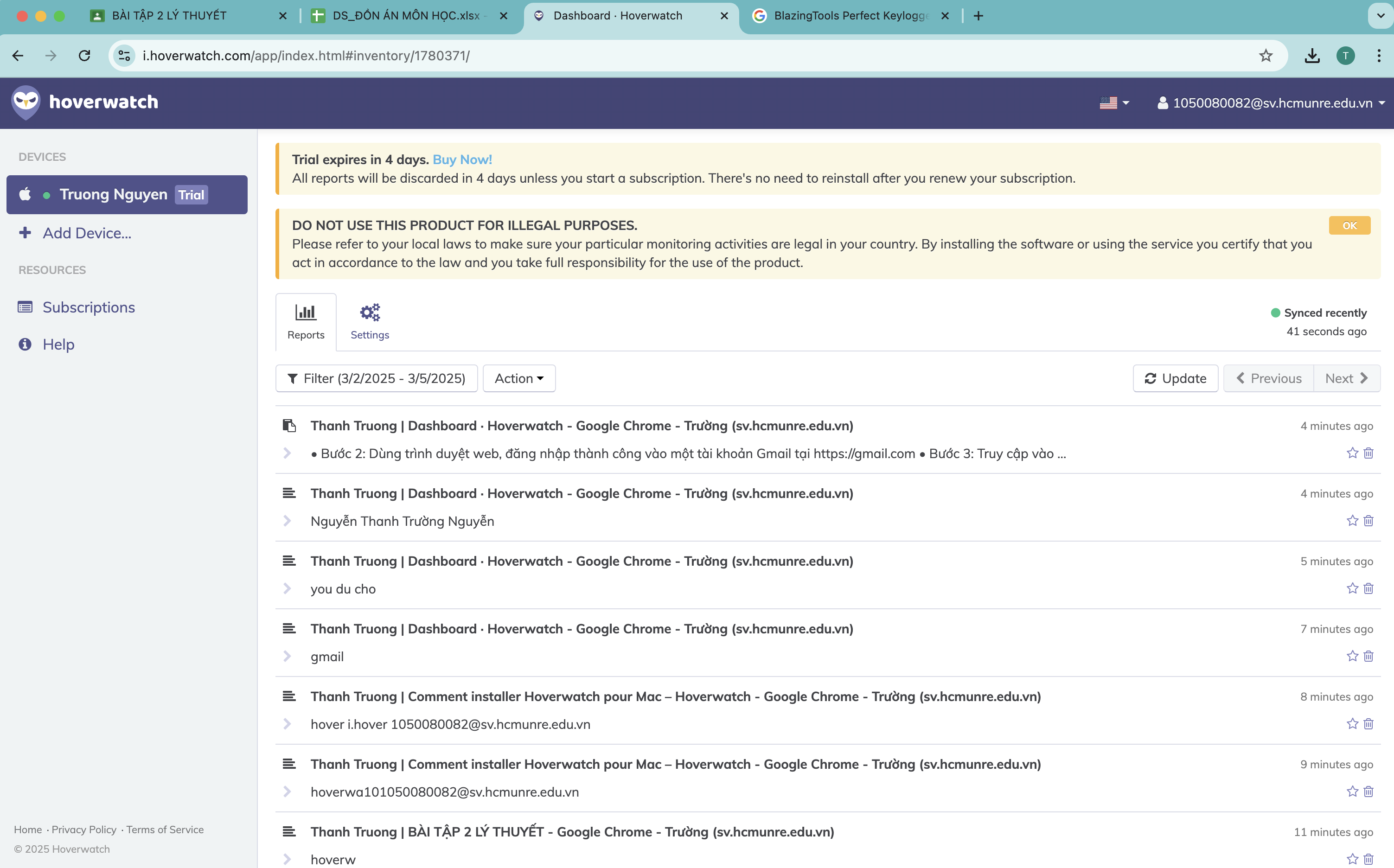


• Bước 3: Truy cập vào Youtube.com và chọn xem một video bất kỳ.



• Bước 4: Truy cập Google.com và tìm kiếm với từ khóa là tên sinh viên, chọn xem

một kết quả bất kỳ.



**C: CÂU HỎI**

**1. Biện pháp phòng tránh và cách phát hiện Keylogger trên máy tính - điện thoại**

**Biện pháp phòng tránh:**

* **Cài đặt phần mềm bảo mật**: Sử dụng phần mềm diệt virus và các chương trình chống Keylogger như Malwarebytes, Windows Defender, hay Norton Security.
* **Không tải phần mềm không rõ nguồn gốc**: Tránh tải ứng dụng từ các trang web không chính thức hoặc không rõ nguồn gốc.
* **Bật xác thực hai yếu tố (2FA)**: Giúp bảo vệ tài khoản ngay cả khi mật khẩu bị lộ.
* **Sử dụng bàn phím ảo**: Khi nhập thông tin quan trọng, đặc biệt là mật khẩu hoặc thông tin ngân hàng.
* **Cập nhật hệ điều hành và phần mềm thường xuyên**: Giúp vá các lỗ hổng bảo mật có thể bị lợi dụng bởi Keylogger.
* **Kiểm tra thiết bị ngoại vi**: Đối với máy tính, tránh sử dụng bàn phím công cộng hoặc USB không rõ nguồn gốc vì có thể chứa phần cứng Keylogger.

**Cách phát hiện Keylogger:**

* **Kiểm tra danh sách tiến trình đang chạy**: Sử dụng Task Manager (Windows) hoặc Activity Monitor (Mac) để kiểm tra các tiến trình lạ.
* **Quét bằng phần mềm bảo mật**: Dùng phần mềm diệt virus hoặc anti-malware để quét và phát hiện Keylogger.
* **Kiểm tra thư mục khởi động cùng hệ thống**: Keylogger thường tự động chạy khi khởi động máy. Kiểm tra trong Task Manager > Startup hoặc msconfig (Windows).
* **Kiểm tra hoạt động mạng**: Dùng Wireshark hoặc Netstat để theo dõi các kết nối mạng bất thường.
* **Kiểm tra file log khả nghi**: Một số Keylogger lưu dữ liệu thu thập được vào file log trên máy tính. Có thể kiểm tra các thư mục ẩn hoặc file lạ trong ổ cứng.

**2. Một số loại Keylogger trên máy tính và điện thoại**

**Trên máy tính:**

1. **Hook-Based Keylogger**: Chặn và ghi lại thao tác phím bằng cách can thiệp vào API của hệ điều hành.
2. **Kernel-Based Keylogger**: Chạy ở mức kernel, khó phát hiện hơn do không hiển thị trong Task Manager.
3. **Form Grabbing Keylogger**: Đánh cắp dữ liệu khi người dùng nhập vào các biểu mẫu trực tuyến (web forms).
4. **USB Keylogger (Hardware Keylogger)**: Thiết bị cắm vào giữa bàn phím và máy tính để ghi lại mọi thao tác phím.

**Trên điện thoại:**

1. **Spyware Keylogger (Android/iOS)**: Ứng dụng gián điệp cài vào điện thoại để ghi lại thao tác phím và gửi dữ liệu ra ngoài. Ví dụ: mSpy, FlexiSPY.
2. **Screenlogger**: Chụp màn hình sau mỗi lần nhập thông tin thay vì ghi lại từng phím bấm.
3. **Accessibility Keylogger**: Lợi dụng quyền Accessibility trên Android để theo dõi nội dung nhập liệu.