**Lab 2: Keylogger**

**Họ và tên:** Phạm Hoàng Minh

**MSSV:** 1050080144

**Lớp:** 10-ĐH-CNPM2

**Trả lời câu hỏi**

Câu 1:

**Biện pháp phòng tránh:**

* **Cập nhật phần mềm thường xuyên:** Đảm bảo hệ điều hành và các ứng dụng, phần mềm bảo mật trên máy tính hoặc điện thoại luôn được cập nhật phiên bản mới nhất, giúp giảm thiểu nguy cơ bị tấn công qua các lỗ hổng bảo mật.
* **Cài đặt phần mềm chống virus và chống phần mềm gián điệp:** Các phần mềm diệt virus như Kaspersky, Norton, Bitdefender, hoặc phần mềm chống gián điệp như Malwarebytes có thể giúp phát hiện và ngăn chặn các keylogger.
* **Tránh tải ứng dụng hoặc phần mềm từ nguồn không rõ ràng:** Chỉ tải các ứng dụng từ cửa hàng ứng dụng chính thức như Google Play, App Store, và tránh tải các phần mềm từ các nguồn không xác định.
* **Sử dụng mật khẩu mạnh và xác thực hai yếu tố (2FA):** Sử dụng mật khẩu phức tạp kết hợp với xác thực hai yếu tố sẽ giảm thiểu khả năng kẻ tấn công đánh cắp tài khoản của bạn qua keylogger.
* **Cẩn thận khi kết nối với mạng Wi-Fi công cộng:** Mạng Wi-Fi công cộng dễ bị tấn công, làm lộ thông tin cá nhân. Sử dụng mạng riêng ảo (VPN) khi kết nối với các mạng Wi-Fi công cộng.

**Cách phát hiện Keylogger:**

* **Giám sát hiệu suất máy tính hoặc điện thoại:** Nếu máy tính hoặc điện thoại của bạn trở nên chậm chạp hoặc có sự thay đổi bất thường trong hoạt động hệ thống, có thể đang bị cài keylogger.
* **Sử dụng phần mềm quét keylogger:** Các công cụ như Spybot Search and Destroy hoặc HitmanPro có thể phát hiện keylogger trên máy tính.
* **Kiểm tra danh sách ứng dụng và phần mềm đã cài:** Kiểm tra các ứng dụng hoặc chương trình đã cài, nếu có phần mềm lạ hoặc không nhận diện được, có thể đó là keylogger.
* **Chú ý đến các thao tác bất thường:** Nếu bạn nhận thấy việc gõ bàn phím hoặc các thao tác khác bị trì hoãn hoặc bị thay đổi, có thể máy đã bị nhiễm keylogger.

**Minh họa (ví dụ trên máy tính):**

* Cài phần mềm **Malwarebytes** và quét toàn bộ hệ thống để phát hiện keylogger.
* Kiểm tra bảng điều khiển trong Task Manager để xem có phần mềm nào đang chạy mà bạn không nhận diện được hay không.

Câu 2:

**Trên máy tính:**

* **Spyrix Keylogger:** Là một keylogger phần mềm mạnh mẽ trên Windows, nó không chỉ ghi lại các thao tác bàn phím mà còn có thể giám sát màn hình, nhật ký các hoạt động mạng và thậm chí có khả năng chụp ảnh màn hình. Nó hoạt động ẩn, rất khó phát hiện bằng các phần mềm bảo mật thông thường.
* **Refog Keylogger:** Một keylogger phần mềm phổ biến khác, có thể ghi lại bàn phím, màn hình, các trang web đã truy cập, tin nhắn và thậm chí email. Refog có khả năng chạy ẩn và có thể tự động gửi báo cáo về các hoạt động.
* **Elite Keylogger:** Đây là phần mềm theo dõi mạnh mẽ, có thể ghi lại tất cả các thao tác bàn phím và tạo báo cáo chi tiết, bao gồm cả việc ghi lại các nội dung trò chuyện, email, và nhiều hoạt động trực tuyến khác.

**Trên điện thoại:**

* **FlexiSPY:** Đây là một ứng dụng giám sát mạnh mẽ trên điện thoại di động, có khả năng ghi lại tất cả các thao tác trên bàn phím, đọc tin nhắn, theo dõi cuộc gọi và giám sát các hoạt động trên mạng xã hội. FlexiSPY hoạt động trên cả thiết bị Android và iOS.
* **mSpy:** Đây là một phần mềm giám sát điện thoại khá phổ biến, cho phép theo dõi các hoạt động của người dùng trên điện thoại, bao gồm việc ghi lại các thao tác bàn phím, tin nhắn và cuộc gọi. mSpy hoạt động lặng lẽ trên điện thoại mà người dùng không dễ dàng phát hiện.
* **Hoverwatch:** Một keylogger khác dành cho điện thoại, có khả năng ghi lại các thao tác trên bàn phím, chụp ảnh màn hình và theo dõi vị trí của điện thoại. Nó hoạt động trên cả Android và Windows.

**Thực hành**

* Phần mềm mở không lên dù đã được cài đặt chỉ hiện mỗi biểu tượng nhỏ ở **Show hidden icons** còn lại thì bấm hay gì điều không mở lên được (em đã tắt phần mềm diệt virus khi cài đặt phần mềm)

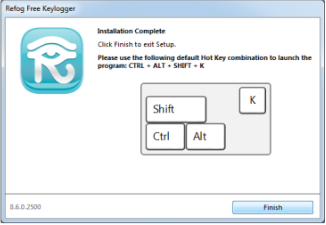


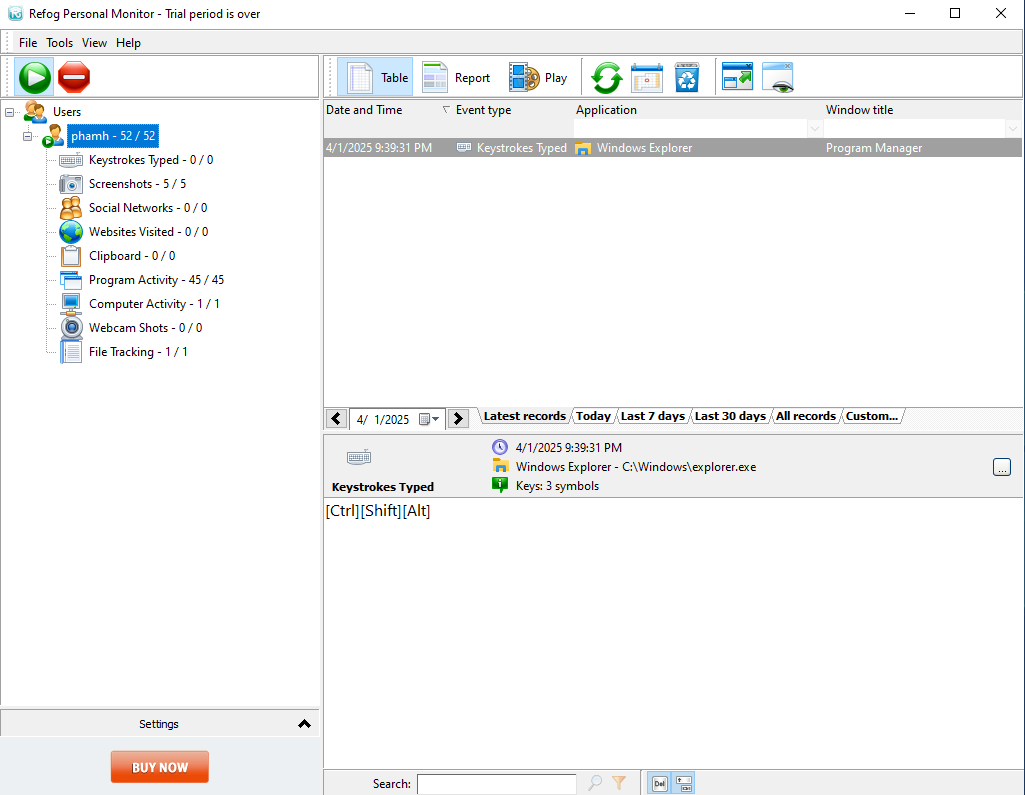
**Giải pháp: Em sẽ bổ sung bài thực hành sau. Em cảm ơn thầy**

**Bổ sung thực hành**

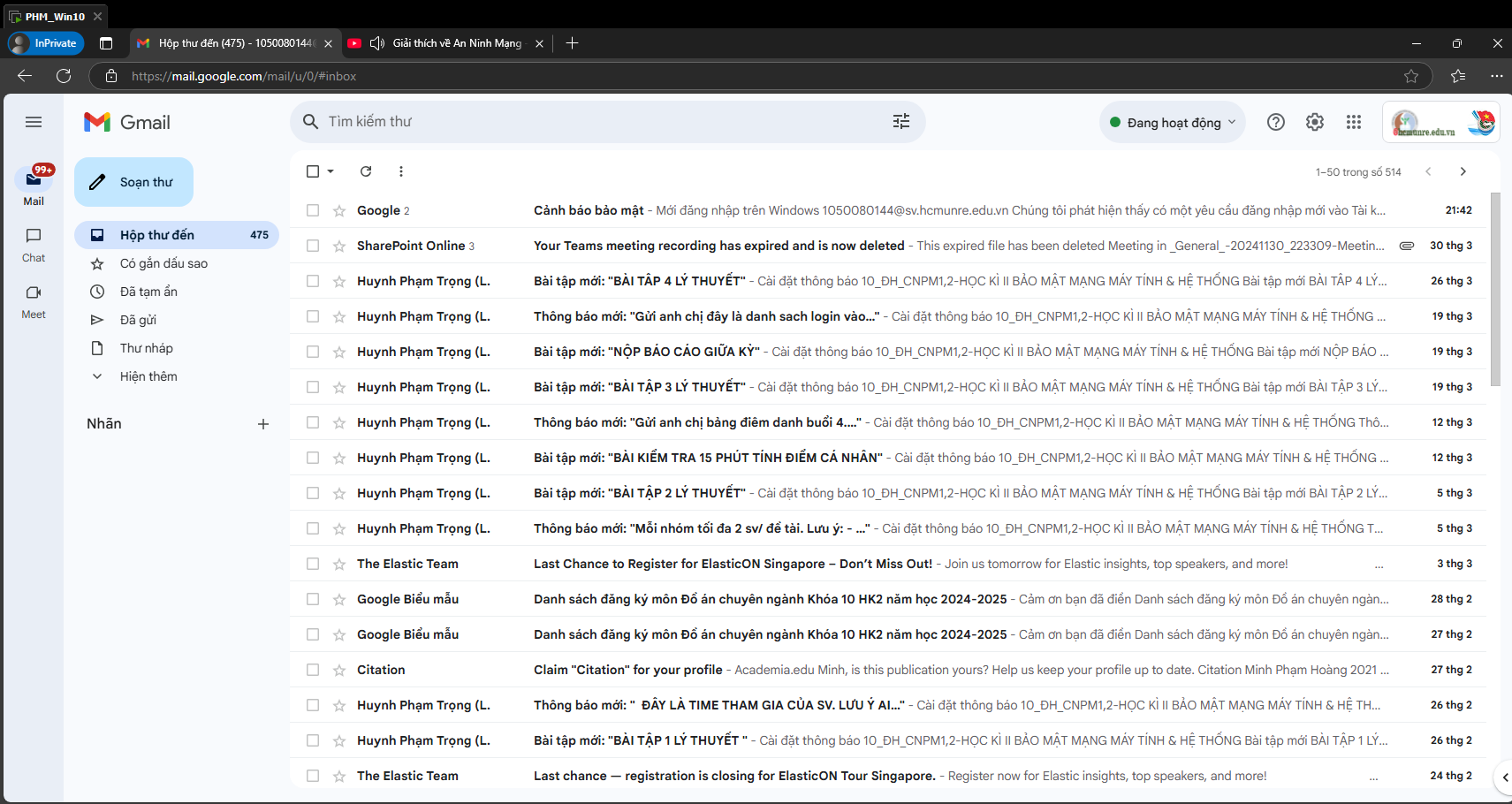
**Bài 1:**

**B1:**

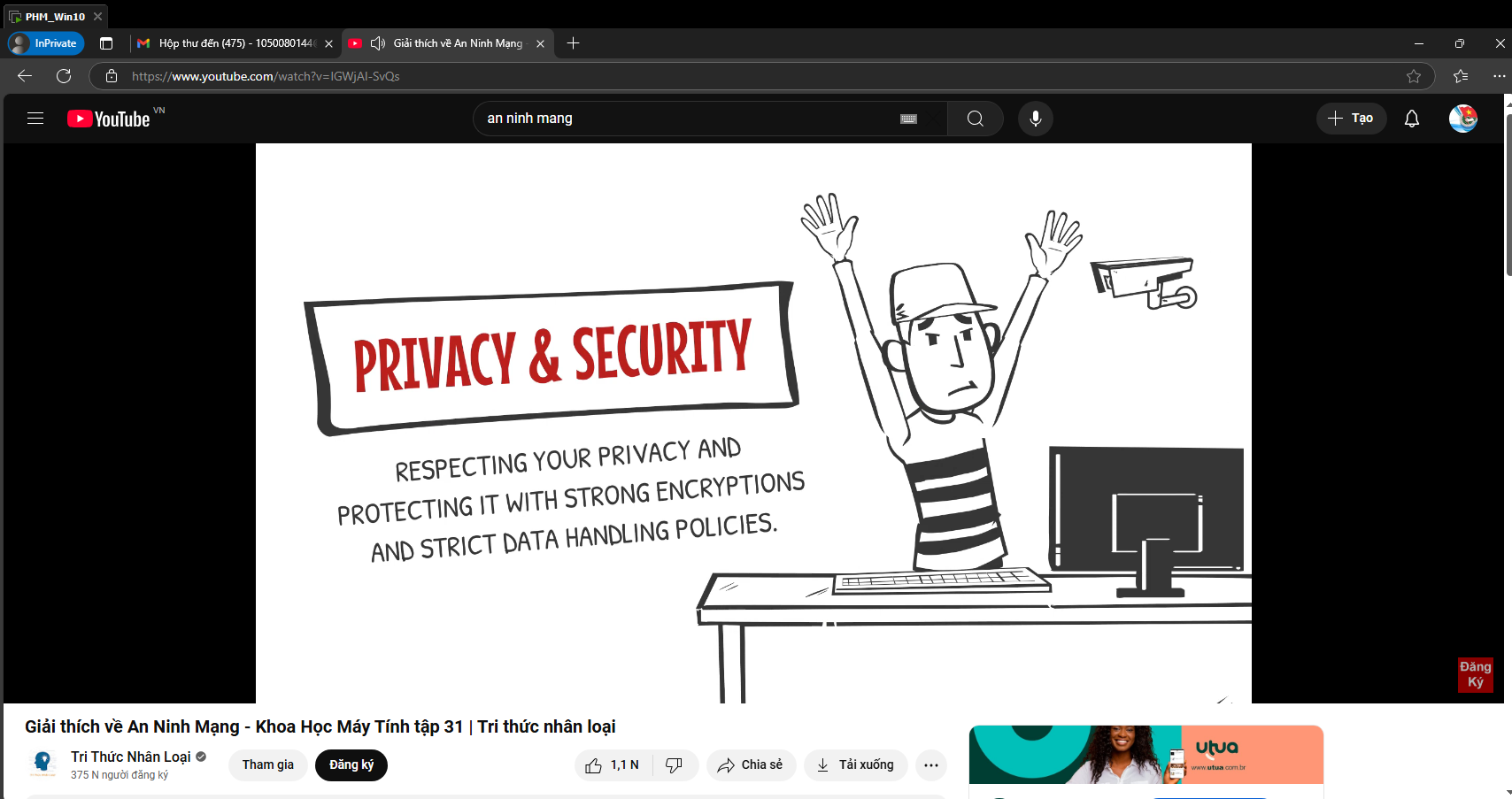
****

****

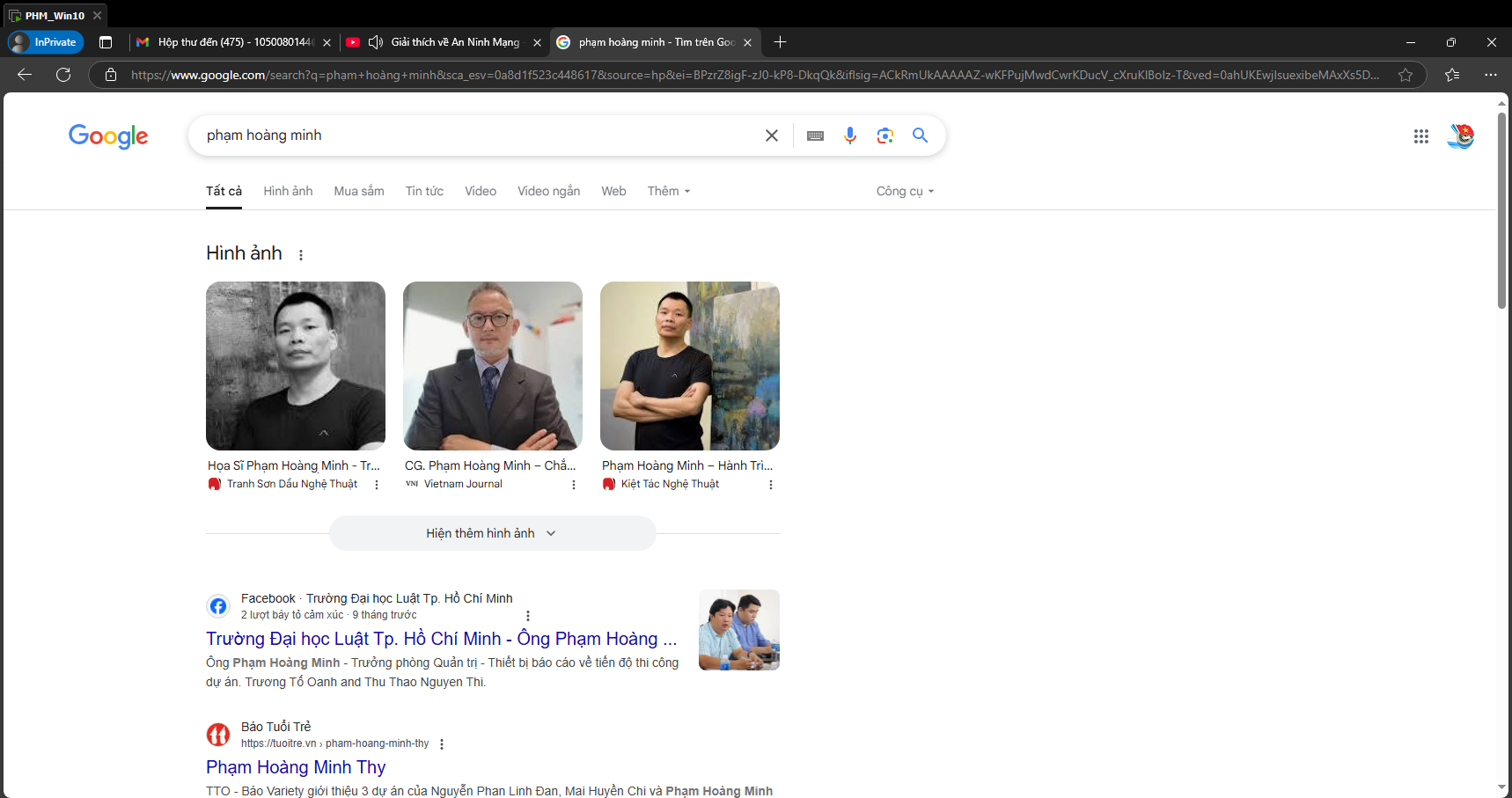
**B2:**

****

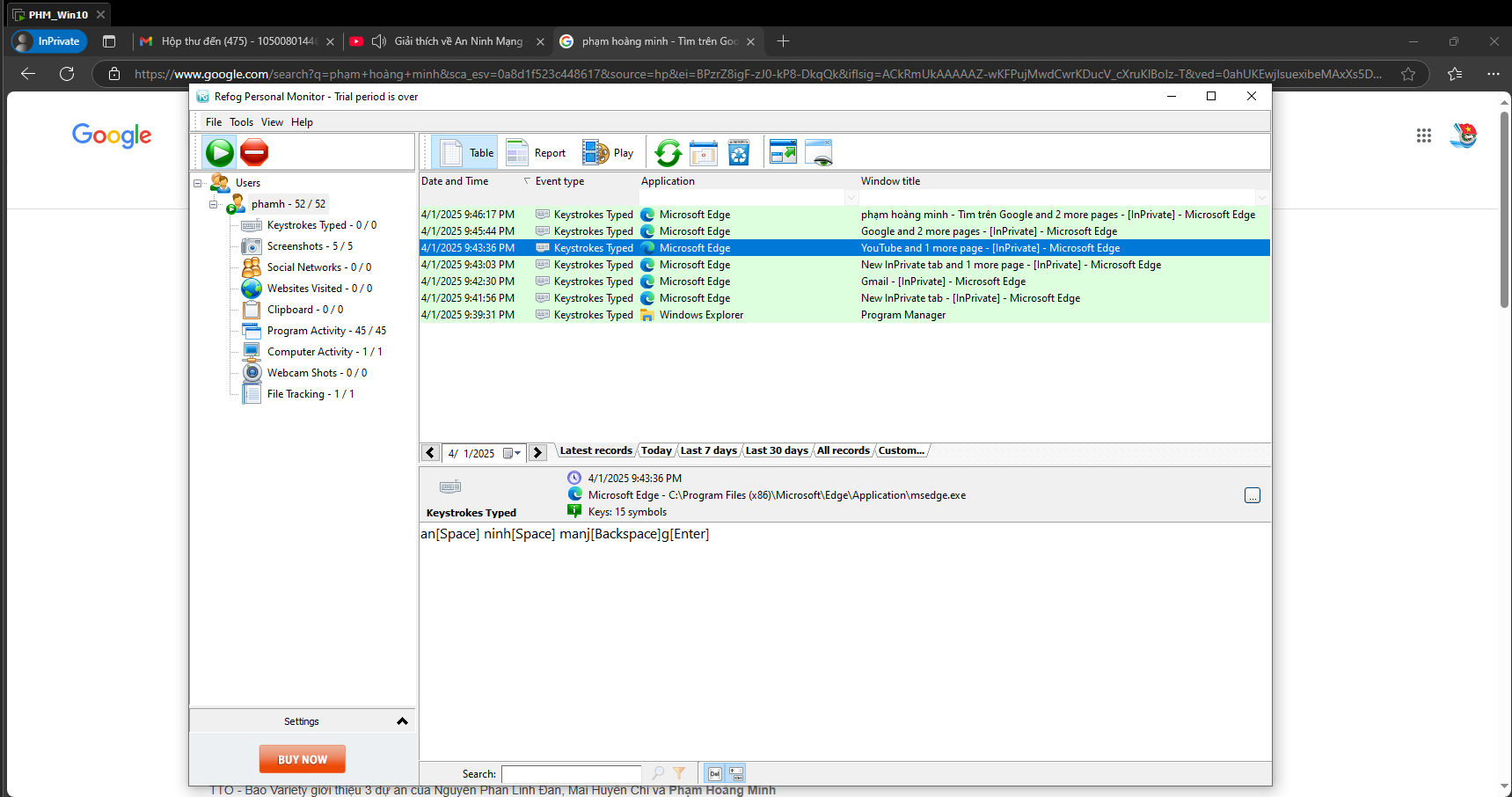
**B3:**

****

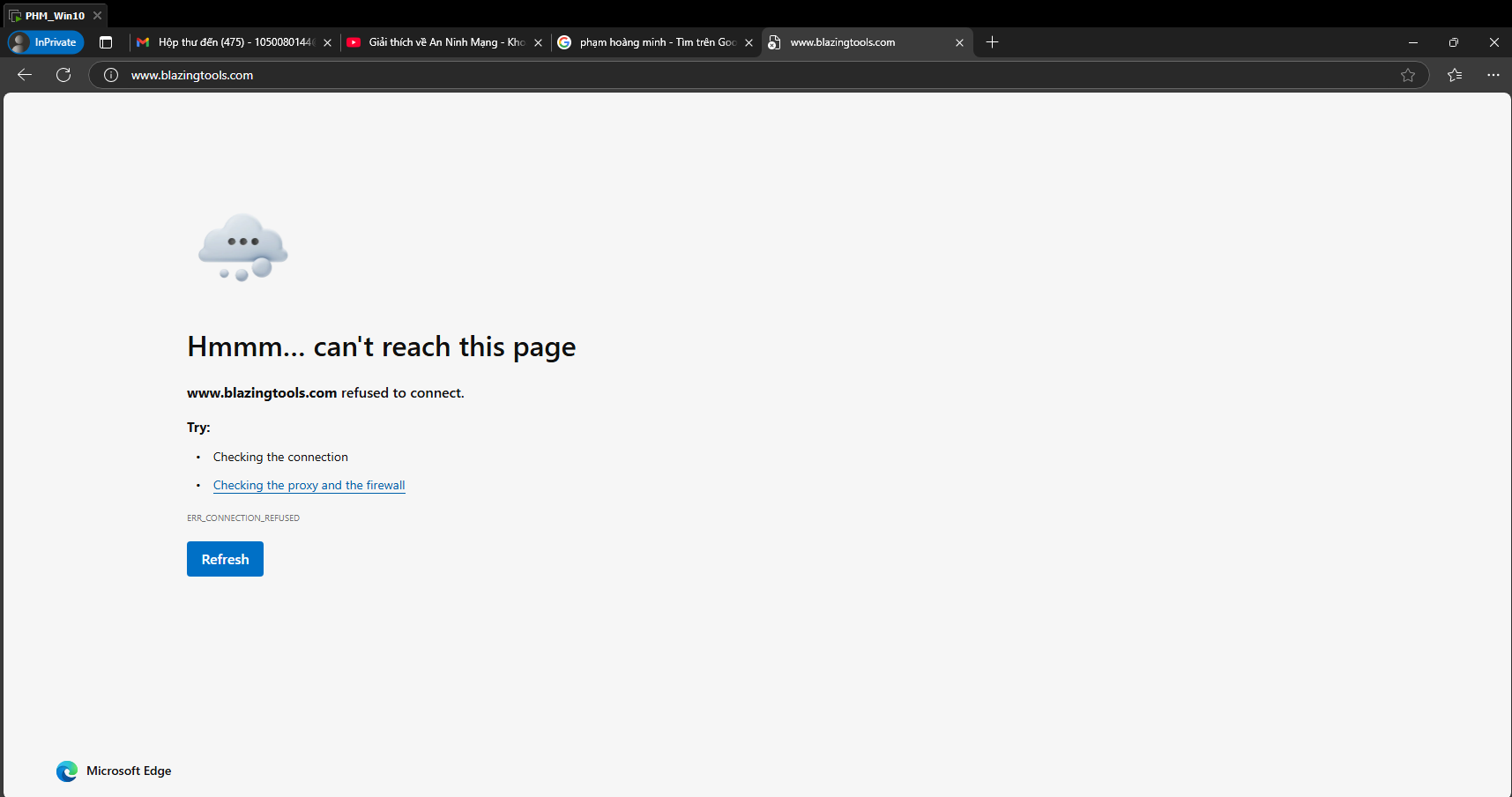
**B4;**

****

**B5:**

****

**Bài 2: Đường link đã bị chặn**

****