**Nguyễn Bá Hùng\_1050080264\_CNPM3**

**Các biện pháp phòng tránh:**

**Cài đặt phần mềm bảo mật**: Sử dụng các phần mềm diệt virus như Kaspersky, Bitdefender, Malwarebytes để quét và phát hiện Keylogger.

**Không tải phần mềm từ nguồn không rõ ràng**: Chỉ tải ứng dụng từ trang web chính thức hoặc cửa hàng ứng dụng (Google Play, App Store).

**Cập nhật hệ điều hành và phần mềm thường xuyên**: Giúp vá các lỗ hổng bảo mật mà Keylogger có thể khai thác.

**Sử dụng bàn phím ảo**: Khi nhập mật khẩu hoặc thông tin quan trọng, sử dụng bàn phím ảo để tránh bị ghi lại thao tác gõ phím.

**Bật xác thực hai yếu tố (2FA)**: Giúp bảo vệ tài khoản ngay cả khi bị lộ mật khẩu.

**Kiểm tra danh sách ứng dụng chạy nền**: Xem các ứng dụng đang chạy để phát hiện chương trình đáng ngờ.

**Cách phát hiện:**

Kiểm tra trình quản lý tác vụ (Task Manager - Windows) hoặc Trình quản lý hoạt động (Activity Monitor - macOS)

Kiểm tra danh sách phần mềm cài đặt

Sử dụng phần mềm quét Keylogger

Kiểm tra các tiện ích mở rộng trên trình duyệt

Kiểm tra thư mục hệ thống

Dùng phần mềm phát hiện Keylogger

Một số loại Keyword trên máy tính và điện thoại khác

* Trên máy tính:

+ Software Keylogger:

+ Remote Access Trojan (RAT) Keylogger:

+ Hardware Keylogger:

* Trên điện thoại

+ mSpy

+ FlexiSPY

+ Spyzie

+ Hoverwatch