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

**Biện pháp phòng tránh:**

* **Cài đặt phần mềm diệt virus:** Sử dụng các phần mềm diệt virus và anti-malware uy tín như Kaspersky, Bitdefender, Malwarebytes để quét và loại bỏ keylogger.
* **Không tải phần mềm không rõ nguồn gốc:** Tránh tải và cài đặt phần mềm từ các trang web không đáng tin cậy.
* **Cập nhật hệ điều hành và phần mềm:** Luôn cập nhật hệ điều hành và phần mềm bảo mật để vá lỗ hổng bảo mật.
* **Sử dụng bàn phím ảo:** Khi nhập mật khẩu quan trọng, có thể dùng bàn phím ảo để tránh bị ghi lại thao tác gõ phím.
* **Không click vào liên kết lạ:** Không mở email lạ, tin nhắn có liên kết không rõ nguồn gốc để tránh bị cài đặt keylogger qua phishing.
* **Sử dụng xác thực hai yếu tố (2FA):** Giúp bảo vệ tài khoản ngay cả khi mật khẩu bị đánh cắp.

**Cách phát hiện Keylogger:**

* **Kiểm tra Task Manager (Windows) hoặc Activity Monitor (MacOS):** Xem các tiến trình đang chạy có tiến trình nào lạ hoặc ngốn tài nguyên bất thường không.
* **Dùng phần mềm quét Keylogger:** Sử dụng các công cụ như SpyShelter, Zemana AntiLogger để phát hiện keylogger.
* **Kiểm tra phần mềm cài đặt:** Vào danh sách phần mềm đã cài đặt trên máy tính/điện thoại để kiểm tra có phần mềm lạ nào không.
* **Kiểm tra kết nối mạng:** Một số keylogger gửi dữ liệu ra ngoài qua mạng, có thể kiểm tra lưu lượng mạng bất thường bằng phần mềm như Wireshark.

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

* **Hardware Keylogger:** Dạng thiết bị cắm vào giữa bàn phím và máy tính để ghi lại mọi thao tác gõ phím.
* **Software Keylogger:** Dạng phần mềm cài đặt trên hệ điều hành để ghi lại thao tác bàn phím (ví dụ: Revealer Keylogger, Ardamax Keylogger).
* **Keylogger dạng trojan:** Lây nhiễm vào máy thông qua phần mềm độc hại hoặc file đính kèm email.
* **Keylogger trên điện thoại:** Có thể cài vào điện thoại Android/iOS thông qua ứng dụng độc hại, ví dụ: Spyrix Free Keylogger, KidLogger.