# Xử lý khi máy tính có dấu hiệu nhiễm phần mềm độc hại

Máy tính xuất hiện các hiện tượng: chạy chậm bất thường, quạt kêu to; xuất hiện nhiều cửa sổ quảng cáo lạ; các file bị đổi tên sang đuôi .locked; trình duyệt tự động mở tab lạ khi khởi động. Dưới đây là phân loại các loại phần mềm độc hại có thể gây ra và các biện pháp xử lý ngay lập tức.

## 1. Ít nhất 3 loại phần mềm độc hại tương ứng

* • Ransomware

Mô tả: Mã hóa file trên máy và đổi đuôi (ví dụ: .locked), yêu cầu tiền chuộc để giải mã.  
Dấu hiệu điển hình: File bị đổi đuôi, xuất hiện thông báo đòi tiền chuộc (ransom note).

* • Adware / PUP (Potentially Unwanted Program)

Mô tả: Phần mềm hiển thị quảng cáo, mở cửa sổ/tab quảng cáo liên tục, làm chậm trình duyệt.  
Dấu hiệu điển hình: Quảng cáo pop-up, thanh công cụ lạ trên trình duyệt, chuyển hướng nhiều lần.

* • Trojan / Backdoor

Mô tả: Chương trình giả danh phần mềm hợp pháp nhưng mở cửa hậu (backdoor) cho kẻ tấn công điều khiển, tải mã độc bổ sung.  
Dấu hiệu điển hình: Máy chạy chậm, quạt kêu to do quá tải CPU/IO, kết nối mạng bất thường, trình duyệt tự mở tab lạ.

## 2. Đề xuất cách xử lý ngay khi phát hiện các dấu hiệu trên

* • Ngắt kết nối mạng ngay lập tức

Rút cáp mạng hoặc tắt Wi‑Fi để ngăn kẻ tấn công tiếp tục truyền dữ liệu hoặc lan truyền mã độc sang máy khác trong mạng.

* • Không tắt/rút nguồn vội nếu nghi có ransomware nhưng ưu tiên cô lập

Nếu nghi ngờ ransomware, đôi khi tắt máy nhanh có hạn chế việc mã hóa tiếp tục — nhưng lưu ý điều này có thể gây mất dữ liệu; ưu tiên là cô lập (ngắt mạng) trước.

* • Chạy quét bằng phần mềm chống virus/anti‑malware uy tín

Sử dụng Windows Defender hoặc phần mềm bảo mật đáng tin cậy (Malwarebytes, Kaspersky, Bitdefender, v.v.) để quét và loại bỏ mã độc.

* • Khởi động vào Safe Mode hoặc môi trường cứu hộ (Rescue Environment)

Khởi động ở Safe Mode (Windows) hoặc dùng USB cứu hộ để quét khi mã độc ngăn không cho phần mềm bảo mật chạy ở chế độ bình thường.

* • Sao lưu dữ liệu quan trọng (nếu có thể và an toàn)

Sao chép file quan trọng sang ổ ngoài chưa bị mã hoá, nhưng tránh sao chép các file thực thi khả nghi. Nếu có ransomware, lưu bản sao phục vụ điều tra, sau đó sử dụng bản sao sạch để khôi phục.

* • Kiểm tra các tiến trình và ứng dụng khởi động

Dùng Task Manager (Windows) hoặc Activity Monitor (macOS) và công cụ msconfig/Task Scheduler để tìm tiến trình/ứng dụng lạ; gỡ cài đặt PUPs, tiện ích mở rộng trình duyệt khả nghi.

* • Đổi mật khẩu từ thiết bị an toàn

Sau khi máy sạch hoặc từ một thiết bị an toàn, thay đổi mật khẩu tài khoản quan trọng (email, ngân hàng). Không đổi mật khẩu trên máy bị nghi nhiễm.

* • Khôi phục từ bản sao lưu sạch hoặc cài lại hệ điều hành nếu cần

Nếu hệ thống bị xâm phạm nặng (ransomware, backdoor), khôi phục từ backup đáng tin cậy hoặc cài lại hệ điều hành để đảm bảo an toàn.

* • Không trả tiền chuộc tự động (khuyến nghị)

Trả tiền chuộc không đảm bảo sẽ lấy lại dữ liệu và khuyến khích tội phạm; liên hệ chuyên gia, cơ quan chức năng nếu cần.

* • Tìm trợ giúp chuyên nghiệp

Nếu không tự tin xử lý, mang máy đến trung tâm sửa chữa uy tín hoặc chuyên gia an ninh mạng để xử lý và phục hồi dữ liệu.

## 3. Lưu ý phòng ngừa

• Luôn cập nhật hệ điều hành và phần mềm, bật cập nhật tự động khi có thể.

• Không nhấp vào liên kết/đính kèm email lạ; kiểm tra nguồn trước khi mở.

• Sử dụng tài khoản người dùng không có quyền quản trị cho công việc hàng ngày để giảm rủi ro.

• Duy trì bản sao lưu định kỳ (offsite/hoặc offline) và kiểm tra tính toàn vẹn của backup.

Kết luận: Những dấu hiệu mô tả (quảng cáo lạ, file .locked, tab tự mở, máy chậm/quạt kêu) là các chỉ dấu rõ ràng máy có thể đã bị nhiễm mã độc. Hãy cô lập ngay thiết bị, quét bằng phần mềm đáng tin cậy, sao lưu dữ liệu quan trọng và liên hệ chuyên gia nếu cần.