# Bài làm: Phân tích dấu hiệu và xử lý khi máy tính nhiễm phần mềm độc hại

## Tình huống

Máy tính xuất hiện các hiện tượng sau:  
- Máy chạy chậm bất thường, quạt kêu to.  
- Xuất hiện nhiều cửa sổ quảng cáo lạ.  
- Các file trong máy bị đổi tên sang đuôi .locked.  
- Trình duyệt tự động mở tab lạ khi khởi động.

## I. Ba (hoặc nhiều hơn) loại phần mềm độc hại tương ứng

Dưới đây là các loại phần mềm độc hại có khả năng gây ra các hiện tượng nêu trên:

1. Ransomware

- Triệu chứng điển hình: file bị mã hóa và đổi đuôi (ví dụ .locked), yêu cầu tiền chuộc để giải mã.

- Tác hại: mất quyền truy cập vào dữ liệu, rủi ro mất dữ liệu vĩnh viễn nếu không có bản sao lưu.

1.2. Adware (phần mềm quảng cáo)

- Triệu chứng: xuất hiện nhiều cửa sổ quảng cáo, trình duyệt mở tab lạ hoặc chuyển hướng quảng cáo.

- Tác hại: làm chậm máy, gây phiền nhiễu, và có thể dẫn đến trang chứa mã độc.

1.3. Trojan / Backdoor

- Triệu chứng: máy chạy chậm do tiến trình ẩn; kẻ tấn công có thể điều khiển hoặc cài thêm phần mềm.

- Tác hại: lộ thông tin nhạy cảm, cài đặt ransomware hoặc phần mềm gián điệp.

1.4. Cryptominer (trình khai thác tiền ảo bất hợp pháp)

- Triệu chứng: CPU/GPU sử dụng cao liên tục, quạt kêu to, máy nóng và chậm.

## II. Cách xử lý ngay khi phát hiện các dấu hiệu

Khi phát hiện các triệu chứng trên, hãy thực hiện các bước sau theo thứ tự ưu tiên:

2.1. Ngắt kết nối mạng ngay lập tức (rút cáp Ethernet hoặc tắt Wi‑Fi) để hạn chế việc lây lan hoặc liên lạc với máy chủ điều khiển.

2.2. Tắt máy hoặc đưa vào chế độ offline nếu nghi ngờ ransomware đang hoạt động (nhưng nếu đang mã hóa file, tắt nguồn có thể là lựa chọn tốt để ngăn tiến trình tiếp tục).

2.3. Khởi động vào Safe Mode (Chế độ an toàn) để giảm thiểu tiến trình độc hại tự khởi động.

2.4. Chạy quét toàn bộ bằng phần mềm diệt virus/anti-malware uy tín (ví dụ: Malwarebytes, Windows Defender) và cách ly/xóa các mục phát hiện.

2.5. Kiểm tra tiến trình và các chương trình khởi động bằng Task Manager / msconfig / Autoruns để phát hiện mục lạ và tắt chúng.

2.6. Phục hồi dữ liệu từ bản sao lưu an toàn nếu có (không trả tiền chuộc nếu có thể).

2.7. Nếu nghiêm trọng (ransomware hoặc trojan backdoor), cân nhắc sao chép dữ liệu cần thiết, cài lại hệ điều hành sạch và khôi phục từ backup.

2.8. Đổi mật khẩu trên các tài khoản quan trọng (làm trên thiết bị an toàn khác) và bật xác thực hai yếu tố.

2.9. Cập nhật hệ điều hành, phần mềm và trình duyệt lên phiên bản mới nhất; kiểm tra và gỡ bỏ tiện ích mở rộng (extensions) lạ trên trình duyệt.

2.10. Nếu cần, nhờ chuyên gia CNTT hoặc dịch vụ xử lý sự cố bảo mật để phân tích sâu và khôi phục an toàn.

## Ghi chú an toàn

- Không mở file đính kèm hoặc nhấp link lạ. Kiểm tra email/sources cẩn thận.

- Giữ thói quen sao lưu định kỳ và lưu bản sao lưu offline hoặc trên dịch vụ đáng tin cậy.

- Luôn cập nhật phần mềm bảo mật và hệ điều hành để giảm lỗ hổng bị lợi dụng.