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

## Tình trạng máy

- 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.

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

Dưới đây là các loại phần mềm độc hại thường tương ứng với những dấu hiệu nêu trên:  
  
1. Ransomware  
- Triệu chứng: Các file bị mã hóa hoặc đổi tên (ví dụ đuôi .locked), xuất hiện yêu cầu tiền chuộc.  
- Hậu quả: Mất quyền truy cập vào dữ liệu; có thể yêu cầu trả tiền để lấy khóa giải mã.  
  
2. Adware (phần mềm quảng cáo) / Browser Hijacker  
- Triệu chứng: Xuất hiện nhiều cửa sổ quảng cáo, trình duyệt mở tab lạ, home page/thay đổi tìm kiếm mặc định.  
- Hậu quả: Quấy rối người dùng, theo dõi hành vi, có thể dẫn tới trang chứa mã độc.  
  
3. Cryptominer (phần mềm đào tiền ảo trái phép) / Trojan / Rootkit  
- Triệu chứng: Máy chạy chậm bất thường, CPU/GPU sử dụng cao, quạt kêu to do tải nặng liên tục.  
- Hậu quả: Hiệu năng giảm, phần cứng nóng, có thể tạo cửa hậu cho tin tặc.  
  
Ngoài ra còn có: Worms (tự lan), Backdoor (cửa hậu), PUPs (Potentially Unwanted Programs).

## 2. Cách xử lý NGAY KHI phát hiện các dấu hiệu trên (HÀNH ĐỘNG KHẨN CẤP)

Thực hiện theo các bước dưới đây để giảm thiểu thiệt hại và ngăn chặn lây lan:  
  
1. Ngắt kết nối mạng ngay lập tức  
- Rút cáp mạng hoặc tắt Wi‑Fi để ngăn phần mềm độc hại gửi/nhận dữ liệu hoặc lây lan đến thiết bị khác.  
  
2. Không khởi chạy thêm chương trình hoặc mở file lạ  
- Tránh mở email, tệp đính kèm, hoặc liên kết khả nghi. Không trả tiền chuộc ngay lập tức.  
  
3. Ghi lại bằng chứng  
- Chụp ảnh màn hình thông báo mã độc, danh sách file bị đổi tên, và lưu log nếu có.  
  
4. Khởi động vào Safe Mode (Chế độ An toàn)  
- Trên Windows: vào Safe Mode with Networking (nếu cần cập nhật) hoặc Safe Mode không có mạng để quét.  
  
5. Chạy phần mềm chống mã độc uy tín  
- Chạy quét toàn bộ hệ thống bằng Windows Defender Offline / Malwarebytes / Kaspersky Rescue Disk.  
  
6. Gỡ phần mở rộng và chương trình khả nghi  
- Kiểm tra trình duyệt (extensions, homepage, search engine) và gỡ bỏ extension khả nghi.  
  
7. Cách ly thiết bị lưu trữ ngoài  
- Ngắt mọi USB/ổ cứng gắn ngoài khỏi máy để tránh lây nhiễm.  
  
8. Khôi phục từ bản sao lưu an toàn  
- Nếu có backup gần nhất, restore từ backup được lưu trước khi nhiễm. Kiểm tra backup trên thiết bị sạch trước khi khôi phục.  
  
9. Thay đổi mật khẩu từ thiết bị an toàn  
- Sau khi máy đã được làm sạch hoặc từ một máy khác an toàn, đổi mật khẩu các tài khoản quan trọng.  
  
10. Liên hệ chuyên gia hoặc cơ quan chức năng  
- Nếu là ransomware hoặc nghi ngờ bị tấn công nghiêm trọng, liên hệ dịch vụ IT chuyên nghiệp hoặc tố giác cơ quan an ninh mạng.

## 3. Bước phục hồi và phòng ngừa (sau khi xử lý khẩn cấp)

- Cài đặt lại hệ điều hành nếu không thể đảm bảo máy đã sạch hoàn toàn.  
- Cập nhật hệ điều hành và phần mềm (patchs bảo mật).  
- Cài phần mềm chống virus uy tín và bật cập nhật tự động.  
- Thiết lập sao lưu định kỳ (offline hoặc cloud có phiên bản hóa) và kiểm tra tính toàn vẹn backup.  
- Kích hoạt tường lửa, sử dụng tài khoản không phải admin cho hoạt động hàng ngày.  
- Kích hoạt xác thực hai yếu tố (2FA) cho tài khoản quan trọng.  
- Cẩn trọng khi tải phần mềm, tránh file/codec/crack từ nguồn không đáng tin cậy.

## Ghi chú quan trọng

- Không khuyến khích trả tiền chuộc: trả tiền không đảm bảo khôi phục và khuyến khích tội phạm.  
- Nếu dữ liệu quan trọng chưa có backup, cân nhắc nhờ dịch vụ phục hồi chuyên nghiệp.  
- Luôn thực hiện các bước cách ly và sao lưu trước khi thử biện pháp sửa chữa mạnh (ví dụ dùng công cụ 'wipe' hay cài lại hệ điều hành).