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

## Tình huống

Máy tính xuất hiện các hiện tượng: máy 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.

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

1. **1) Ransomware**

* • Mô tả: Mã độc mã hóa file và đòi tiền chuộc; thường đổi đuôi file sang dạng như .locked, .crypt, .locked123.
* • Liên hệ với triệu chứng: Việc các file bị đổi đuôi sang .locked là điển hình của ransomware.

1. **2) Adware (phần mềm quảng cáo) / PUP (chương trình không mong muốn)**

* • Mô tả: Chèn quảng cáo, mở pop-up, làm chậm máy và ảnh hưởng trải nghiệm người dùng.
* • Liên hệ với triệu chứng: Xuất hiện nhiều cửa sổ quảng cáo lạ và tab trình duyệt tự mở là dấu hiệu điển hình.

1. **3) Cryptominer / Coinminer (phần mềm đào tiền ảo trái phép)**

* • Mô tả: Sử dụng CPU/GPU để đào tiền ảo dẫn đến sử dụng tài nguyên cao.
* • Liên hệ với triệu chứng: Máy chạy chậm, quạt kêu to do CPU/GPU hoạt động liên tục.

1. **4) Trojan / Backdoor (ngựa thành Troy, cửa hậu)**

* • Mô tả: Cho phép kẻ tấn công truy cập từ xa, cài thêm phần mềm độc hại khác hoặc đánh cắp dữ liệu.
* • Liên hệ với triệu chứng: Trình duyệt tự mở tab lạ hoặc máy thực hiện hành động bất thường có thể là do trojan/hacker điều khiển.

## 2. Các bước xử lý ngay khi phát hiện (ưu tiên làm ngay)

Ngắt kết nối Internet tức thì: rút dây mạng hoặc tắt Wi‑Fi để ngăn mã độc tải thêm module hoặc gửi dữ liệu ra ngoài.

Không tắt máy nguội (đang hoạt động) nếu nghi ngờ ransomware đã mã hóa — chụp lại ảnh màn hình, ghi chú thông báo tống tiền. Tuy nhiên nếu máy vẫn truy cập được và nguy cơ lây lan cao, cân nhắc tắt và khởi động vào Safe Mode.

Khởi động vào Safe Mode (Windows) hoặc chế độ an toàn tương ứng và quét bằng công cụ diệt malware uy tín (Windows Defender, Malwarebytes, Kaspersky Rescue Disk).

Dùng công cụ quét trực tuyến hoặc máy quét khởi động (bootable antivirus) nếu nghi ngờ hệ thống đã bị nhiễm nặng.

Nếu phát hiện ransomware (file đổi đuôi .locked): ngắt nguồn mạng, không trả tiền chuộc ngay, liên hệ chuyên gia bảo mật và kiểm tra bản sao lưu. Nếu có backup sạch — ưu tiên khôi phục từ backup.

Lưu giữ bằng chứng: chụp màn hình thông báo, lưu file log, tên file bị mã hóa để hỗ trợ phân tích và báo cáo cho cơ quan chức năng nếu cần.

Đổi mật khẩu: sau khi hệ thống an toàn, đổi mật khẩu các tài khoản quan trọng (email, ngân hàng) và kiểm tra truy cập bất thường.

Cập nhật hệ điều hành và phần mềm, gỡ bỏ chương trình khả nghi và xem xét cài lại hệ điều hành nếu không thể đảm bảo sạch hoàn toàn.

Kiểm tra các thiết bị khác trong mạng (NAS, điện thoại, máy khác) vì mã độc có thể lây lan.

Nếu cần, liên hệ dịch vụ phục hồi dữ liệu chuyên nghiệp — đặc biệt khi dữ liệu quan trọng và backup không có.

## 3. Lưu ý và phòng ngừa lâu dài

• Luôn giữ backup định kỳ (theo nguyên tắc 3-2-1: 3 bản, 2 loại lưu trữ, 1 bản offsite).

• Cài đặt phần mềm chống virus uy tín, bật cập nhật tự động và chỉ cài phần mềm từ nguồn tin cậy.

• Kỹ năng người dùng: không mở file đính kèm lạ, không click link nghi ngờ và kiểm tra chữ ký số/nguồn gốc email.

• Sử dụng tài khoản không có quyền admin cho công việc hàng ngày để giảm rủi ro khi mã độc chạy.

• Kích hoạt tính năng khôi phục (System Restore) và lưu key/backup mã hoá ở nơi an toàn nếu sử dụng mã hóa hợp pháp.