## 1. Các loại phần mềm độc hại có thể tương ứng

• Adware (Phần mềm quảng cáo): Thường gây ra việc xuất hiện nhiều cửa sổ quảng cáo, redirect trình duyệt. Có thể được cài kèm cùng phần mềm miễn phí.

• Ransomware (Mã độc tống tiền): Đổi tên hoặc mã hóa file rồi thêm phần đuôi như .locked, yêu cầu tiền chuộc để giải mã. Đây là dấu hiệu rõ ràng của ransomware.

• Trojan/Backdoor (Ngựa thành Troy / Cửa hậu): Cho phép kẻ tấn công truy cập từ xa, làm máy chạy nặng, mở các kết nối đến server điều khiển, hoặc cài thêm phần mềm khác.

## 2. Các bước xử lý ngay khi phát hiện (ưu tiên theo thứ tự)

1. Ngắt kết nối mạng ngay lập tức (rút cáp mạng hoặc tắt Wi‑Fi) để ngăn phần mềm độc hại giao tiếp với server điều khiển hoặc lan sang thiết bị khác.

2. Không tắt máy đột ngột nếu nghi ngờ ransomware vừa mã hóa file — việc tắt/ngắt điện có thể giúp bảo tồn trạng thái hiện tại để phục hồi bằng chuyên gia, nhưng trong nhiều trường hợp an toàn hơn vẫn là ngắt mạng ngay và dùng chế độ Safe Mode để xử lý.

3. Chạy quét toàn bộ hệ thống bằng phần mềm chống virus/malware uy tín (khi ở chế độ Safe Mode nếu cần). Có thể dùng Malwarebytes, Windows Defender, Kaspersky, Bitdefender,...

4. Dùng công cụ chuyên dụng để gỡ adware/ad-supported programs nếu thấy quảng cáo nhiều (ví dụ: AdwCleaner).

5. Nếu phát hiện ransomware (file đổi đuôi .locked): không trả tiền chuộc vội; ghi nhận thông tin, chụp màn hình, tham khảo các dịch vụ giải mã và báo cáo cơ quan có thẩm quyền.

6. Phục hồi từ bản sao lưu sạch (backup) nếu có — trước khi phục hồi, đảm bảo hệ thống hiện tại đã được làm sạch hoàn toàn.

7. Cân nhắc khôi phục cài đặt gốc hoặc cài lại hệ điều hành nếu không thể loại bỏ triệt để phần mềm độc hại.

8. Thay đổi mật khẩu các tài khoản quan trọng (email, ngân hàng, mạng xã hội) từ một thiết bị an toàn khác.

9. Cập nhật hệ điều hành và phần mềm, vá lỗi bảo mật và bật tường lửa.

10. Theo dõi giao dịch tài chính và cảnh giác với các hành vi đáng ngờ; nếu cần, báo ngân hàng để tạm khóa/giám sát.

## 3. Lưu ý phòng ngừa sau khi xử lý

• Luôn giữ bản sao lưu định kỳ và lưu trữ offline hoặc trên dịch vụ đám mây đáng tin cậy với phiên bản hóa.

• Không tải phần mềm từ nguồn không rõ, kiểm tra chữ ký/nhà phát hành, đọc quyền truy cập khi cài đặt.

• Kích hoạt cập nhật tự động cho hệ điều hành và chương trình chống virus.

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

• Kích hoạt xác thực hai yếu tố (2FA) cho các tài khoản quan trọng.