**Bước 1: Ngắt kết nối và cô lập máy tính (Quan trọng nhất)**

1. **Ngắt Internet ngay lập tức:** Tháo dây mạng LAN hoặc tắt Wi-Fi. Việc này sẽ ngăn chặn Ransomware tiếp tục gửi khóa mã hóa và ngăn chặn các loại malware khác lây lan sang các thiết bị khác trong cùng mạng lưới của bạn.
2. **Tắt máy (Hard Shut Down):** Giữ nút nguồn để tắt máy tính hoàn toàn. Đối với Ransomware, việc này có thể ngăn chặn quá trình mã hóa đang diễn ra.

**Bước 2: Quét và Loại bỏ Phần mềm độc hại**

1. **Khởi động vào Chế độ An toàn (Safe Mode):** Khởi động lại máy tính và vào **Safe Mode with Networking** (hoặc chỉ Safe Mode nếu bạn muốn an toàn tuyệt đối). Chế độ này chỉ tải các chương trình cần thiết tối thiểu, giúp ngăn chặn malware chạy ngay khi khởi động.
2. **Sử dụng Phần mềm Diệt Virus:** Cài đặt hoặc chạy một phần mềm chống malware uy tín (ví dụ: **Malwarebytes**, **Windows Defender Offline**, hoặc Kaspersky) đã được cập nhật. Thực hiện **quét toàn bộ hệ thống** (Full System Scan) để tìm và loại bỏ cả Adware, Cryptojacker và các tập tin Ransomware.

**Bước 3: Xử lý file bị mã hóa (.locked)**

* **Tuyệt đối không trả tiền chuộc:** Không có gì đảm bảo rằng tin tặc sẽ cung cấp khóa giải mã sau khi bạn trả tiền.
* **Tìm kiếm công cụ giải mã:** Truy cập các trang web của các hãng bảo mật lớn (như ESET, Kaspersky, Avast) từ một máy tính an toàn khác. Họ thường phát hành **công cụ giải mã miễn phí (Decryption Tools)** cho các biến thể Ransomware đã biết.
* **Khôi phục từ bản sao lưu:** Cách xử lý hiệu quả nhất là xóa sạch hệ thống bị nhiễm và **khôi phục dữ liệu từ bản sao lưu (backup) gần nhất** mà bạn đã tạo trước khi bị tấn công. Nếu không có bản sao lưu, dữ liệu có thể đã bị mất vĩnh viễn.

**Bước 4: Dọn dẹp Trình duyệt và Cập nhật Bảo mật**

1. **Reset trình duyệt:** Vào phần cài đặt của Chrome/Firefox/Edge và chọn **Khôi phục cài đặt gốc** (Reset settings) để loại bỏ các extension và cài đặt độc hại do Adware/Browser Hijacker chèn vào.
2. **Cập nhật hệ thống:** Sau khi chắc chắn đã loại bỏ malware, hãy chạy **cập nhật hệ điều hành** và tất cả các phần mềm (đặc biệt là trình duyệt và phần mềm diệt virus) để vá các lỗ hổng bảo mật.