**1. Cách kiểm tra mà không nhấn trực tiếp:**  
Không bấm vào link. Thay vào đó, **dùng công cụ kiểm tra hoặc dịch vụ mở rộng liên kết** để xem đường dẫn thật và độ an toàn của trang web.

**2. Ba công cụ hoặc cách thức kiểm tra link rút gọn:**

1. **Trang mở rộng link:**
   * https://checkshorturl.com
   * https://unshorten.it  
     👉 Giúp hiển thị **địa chỉ thật** mà link rút gọn trỏ tới.
2. **Dùng công cụ kiểm tra độ an toàn của website:**
   * https://virustotal.com
   * https://safebrowsing.google.com  
     👉 Phân tích xem trang đích có chứa **mã độc hoặc nội dung lừa đảo** không.
3. **Dò trước bằng cách di chuột (hover)** lên liên kết (không bấm) để xem **URL thật** hiển thị ở góc trình duyệt.

**3. Giải thích:**  
Link rút gọn thường được dùng trong **lừa đảo (phishing)** vì:

* Nó **che giấu địa chỉ thật**, khiến người dùng **không biết trang có đáng tin cậy không**.
* Tin tặc dễ **dụ người dùng nhấp vào** bằng các liên kết ngắn gọn, trông “vô hại” nhưng dẫn tới **trang giả mạo hoặc chứa mã độc**.