## 3 Công cụ/Cách thức Giúp Kiểm tra Link Rút gọn

**Sử dụng Trình giải mã URL Trực tuyến:**

Các dịch vụ như **checkshorturl.com** hoặc **unshorten.it** cho phép bạn dán link rút gọn vào. Các công cụ này sẽ phân tích và hiển thị URL đích thực cũng như kiểm tra độ an toàn của nó.

**Thêm dấu + vào cuối URL (áp dụng cho Bitly):**

Đối với nhiều dịch vụ rút gọn phổ biến như Bitly, bạn có thể thêm ký tự dấu cộng (+) vào cuối link để xem thông tin thống kê và URL đầy đủ.

**Ví dụ:** Thay vì nhấn vào https://bit.ly/3xyzABC, bạn truy cập https://bit.ly/3xyzABC\*\*+\*\*. (Lưu ý: Cách này không hoạt động với mọi dịch vụ).

**Sử dụng Tiện ích mở rộng Trình duyệt (Browser Extensions):**

Cài đặt các tiện ích mở rộng như **LinkPeel** hoặc **Unshorten** (tùy thuộc vào trình duyệt). Các tiện ích này tự động hiển thị URL đích đầy đủ khi bạn di chuột qua đường link rút gọn, không cần phải sao chép và dán.

## Giải thích tại sao Link Rút gọn thường được dùng trong Lừa đảo

Link rút gọn thường được tin tặc sử dụng trong các cuộc tấn công lừa đảo (phishing) vì những lý do sau:

**Che giấu Danh tính URL Đích:** Mục đích chính của link rút gọn là ẩn URL dài và phức tạp. Kẻ lừa đảo lợi dụng điều này để **giấu đi các trang web độc hại** có tên miền đáng ngờ hoặc tên miền giả mạo (ví dụ: một trang web giả ngân hàng).

**Vượt qua Bộ lọc Email:** Các bộ lọc thư rác và bảo mật đôi khi dễ dàng phát hiện các URL độc hại đã biết. Link rút gọn, với cấu trúc đơn giản và phổ biến (như bit.ly), thường **dễ dàng vượt qua các bộ lọc** này.

**Tạo cảm giác "Đáng tin cậy":** Người dùng có xu hướng ít nghi ngờ các link rút gọn ngắn gọn, chuyên nghiệp hơn so với một URL dài và phức tạp có chứa các từ khóa lạ.