**1. Cách kiểm tra link mà không cần nhấn trực tiếp:**

Có thể sử dụng các công cụ mở rộng link hoặc kiểm tra độ an toàn trực tuyến. Những công cụ này giúp bạn **xem đích đến thật sự** và kiểm tra xem trang đó có chứa mã độc hoặc lừa đảo không.

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

|  |  |
| --- | --- |
| Cách/công cụ | Mô tả |
| CheckShort URL | Dán link rút gọn vào trang này để **xem URL gốc,** tiêu đề trang, và hình ảnh trước khi truy cập. Hỗ trợ nhiều dịch vụ rút gọn như Bit.ly, TinyURL. |
| Visual Total | Công cụ kiểm tra **độ an toàn của liên kết** thông qua hơn 60 dịch vụ bảo mật. Dán link vào và xem kết quả phân tích (malware, phishing). |
| Xem trước link trên Bit.ly | Thêm dấu + vào sau link để xem trước, ví dụ: https://bit.ly/3xyzABC+. Bit.ly sẽ hiển thị trang đích mà không tự động chuyển hướng. |

**3. Tại sao link rút gọn thường được dùng trong lừa đảo?**

- **Che giấu địa chỉ thật:**Link rút gọn làm mờ đi URL gốc, khiến người dùng **không biết rõ trang web sẽ dẫn đến đâu** (có thể là trang giả mạo, chứa mã độc…).

- **Tạo cảm giác tin cậy/ngắn gọn:** Những link ngắn gọn nhìn có vẻ "gọn gàng", dễ chia sẻ, dễ bấm — tạo tâm lý chủ quan, nhất là trên mạng xã hội hoặc email.

- **Khó bị phát hiện bởi công cụ lọc spam/phishing:** Một số bộ lọc email có thể bỏ qua link rút gọn nếu không kiểm tra kỹ nội dung đằng sau, tạo cơ hội cho kẻ xấu.