**1. Cách kiểm tra link mà không cần nhấn trực tiếp:**  
Khi nhận được đường link rút gọn như [**https://bit.ly/3xyzABC**](https://bit.ly/3xyzABC), bạn **không nên bấm vào ngay**, mà có thể kiểm tra trước bằng cách **xem trước địa chỉ gốc** (URL thật) để biết trang web sẽ dẫn đến đâu. Có thể thực hiện bằng cách:

* Dán link vào **các công cụ kiểm tra an toàn trực tuyến**.
* Dùng **trang mở rộng (add-on)** hoặc **chức năng preview** của dịch vụ rút gọn.
* **Di chuột qua liên kết** (trên máy tính) để xem URL đích hiển thị ở góc màn hình.

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

|  |  |
| --- | --- |
| **Cách kiểm tra** | **Mô tả và cách sử dụng** |
| **Trang mở rộng link trực tuyến (ví dụ: CheckShortURL.com, GetLinkInfo.com)** | Dán link rút gọn vào, hệ thống sẽ hiển thị URL thật, tiêu đề và mô tả trang đích. |
| **Công cụ kiểm tra độ an toàn (ví dụ: VirusTotal.com, Google Safe Browsing)** | Phân tích liên kết để phát hiện trang web độc hại, lừa đảo hoặc có mã độc. |
| **Tính năng “Preview” của dịch vụ rút gọn** | Ví dụ: với Bit.ly, thêm dấu “+” sau link (https://bit.ly/3xyzABC+) để xem trước địa chỉ gốc mà không truy cập. |

**3. Giải thích vì sao link rút gọn thường được dùng trong lừa đảo:**

* **Che giấu địa chỉ thật:** Tin tặc sử dụng link rút gọn để ẩn tên miền gốc, khiến người dùng không nhận ra trang web giả mạo (ví dụ: trang đăng nhập giả của ngân hàng, Facebook...).
* **Tạo cảm giác tin cậy hoặc ngắn gọn:** Người dùng dễ nhầm link rút gọn là đường dẫn hợp lệ, đặc biệt khi xuất hiện trong email hoặc tin nhắn trông chuyên nghiệp.
* **Khó nhận diện bằng trực giác:** Vì phần đuôi link là chuỗi ký tự ngẫu nhiên, người dùng khó đoán nội dung hoặc nguồn gốc của trang.