**Phân Tích và Kiểm Tra Tính An Toàn của Đường Link Rút Gọn**

Bạn nhận được đường link trong email: **https://bit.ly/3xyzABC**

**1. Cách kiểm tra liên kết mà không nhấp trực tiếp**

Để kiểm tra đích đến thực sự của một liên kết rút gọn mà không nhấn trực tiếp (hạn chế rủi ro dính mã độc hoặc trang lừa đảo), bạn cần sử dụng các công cụ giải mã (unshortener) hoặc các tiện ích mở rộng của trình duyệt.

**2. 3 Công cụ hoặc cách thức giúp kiểm tra link rút gọn**

| STT | Công cụ/Cách thức | Cách thức hoạt động và mục đích |
| --- | --- | --- |
| **1** | **Trang web Unshortener** | Các trang web chuyên dụng như **CheckShortURL**, **Unshorten.It**, hoặc **WhereGoes.com** cho phép bạn dán liên kết rút gọn vào và nó sẽ hiển thị **URL đích cuối cùng** (Final URL), giúp bạn biết trang web đó là gì trước khi truy cập. |
| **2** | **Xem trước trong Thanh Trạng thái (Hover)** | Nếu liên kết không bị rút gọn quá sâu, hãy **di chuột qua liên kết** (nhưng không nhấp chuột) trong giao diện email hoặc trên trình duyệt. URL đích đến thường sẽ hiển thị ở góc dưới cùng bên trái hoặc bên phải của cửa sổ trình duyệt/ứng dụng. |
| **3** | **Trang web quét mã độc/an toàn** | Sử dụng các dịch vụ uy tín như **Google Transparency Report** (Kiểm tra trạng thái trang web an toàn) hoặc **Virustotal** để dán URL đích (sau khi đã giải mã). Các công cụ này sẽ quét liên kết đích xem có bị liệt vào danh sách đen (Blacklist) vì chứa mã độc hay lừa đảo (phishing) hay không. |

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

Liên kết rút gọn (như bit.ly, tinyurl, goo.gl trước đây) thường được tin tặc sử dụng trong các cuộc tấn công lừa đảo (phishing) vì những lý do chính sau:

1. **Che giấu URL độc hại:** Mục đích chính là để **giấu đi địa chỉ thực sự** của trang web lừa đảo. Người dùng chỉ thấy một chuỗi ký tự ngẫu nhiên, không thể nhận ra rằng nó dẫn đến một trang giả mạo hoặc chứa mã độc.
2. **Tăng độ tin cậy giả:** Trong email hoặc tin nhắn, một liên kết rút gọn trông **"sạch sẽ" và "ngắn gọn"** hơn nhiều so với một URL đầy đủ, dài và có thể chứa các dấu hiệu đáng ngờ, từ đó dễ dàng qua mặt sự cảnh giác của người dùng.