**Cách kiểm tra nhanh (không nhấp):**

1. **Di chuột / chuột phải → Copy link address** rồi dán vào một nơi an toàn (notepad) để xem toàn bộ chuỗi.
2. **Xem trước (preview) cho Bit.ly:** thêm dấu + vào cuối link (ví dụ https://bit.ly/3xyzABC+) — trang preview của Bitly sẽ hiển thị URL đích mà không chuyển hướng.
3. **Dùng công cụ mở rộng (unshorten) / quét URL:** dán link vào một trong các dịch vụ bên dưới để biết đích thật và kiểm tra an toàn.

**Ít nhất 3 công cụ / cách kiểm tra link rút gọn:**

* **CheckShortURL (checkshorturl.com)** — hiện đích thật, hiển thị trang tiêu đề và ảnh chụp nhanh của trang đích.
* **VirusTotal (virustotal.com)** — dán link để quét bằng nhiều engine antivirus và xem lịch sử báo cáo (tốt để phát hiện malware/phishing).
* **Unshorten.It / Unshorten.me / ExpandURL** — các dịch vụ chuyên mở rút gọn và hiển thị URL đích cùng snapshot.
* **URLVoid / Sucuri SiteCheck** — kiểm tra độ tin cậy của domain đích, danh sách đen, malware.
* **Dùng dòng lệnh (cho người biết kỹ thuật):** curl -I -L "https://bit.ly/3xyzABC" hoặc curl -s -o /dev/null -w "%{url\_effective}\n" "https://bit.ly/3xyzABC" để theo dõi header/redirect và thấy URL cuối cùng mà không tải trang thực tế.
* **Google Safe Browsing / Transparency Report** — dán URL vào công cụ của Google để kiểm tra báo cáo an toàn.

**Lý do link rút gọn thường được dùng trong lừa đảo:**

1. **Che giấu domain đích:** người nhận không thấy tên miền thật (ví dụ bank-login.example.com) nên khó phân biệt trang giả mạo.
2. **Qua mặt bộ lọc / hiển thị ngắn gọn:** nhiều hệ thống lọc/cảnh báo có thể khó nhận diện chuỗi rút gọn, khiến liên kết độc hại dễ gửi qua email/nhắn tin.
3. **Tạo cảm giác đáng tin/click nhanh:** link ngắn trông “sạch”, dễ kích thích người dùng click vội; kẻ tấn công còn có thể theo dõi số click để đánh giá chiến dịch lừa đảo.