1. **Mở rộng link (preview) trước** — với bit.ly bạn có thể **thêm dấu + vào cuối** đường link (ví dụ <https://bit.ly/3xyzABC>+) để xem trang đích mà không tự động truy cập.
2. **Dán link vào dịch vụ mở rộng/kiểm tra** (không nhấp) như CheckShortURL, Unshorten.It hoặc unshorten.me để biết URL đích và thông tin phụ.
3. **Quét URL bằng dịch vụ an ninh** như VirusTotal hoặc PhishTank — dán link, dịch vụ sẽ báo nếu link có dấu hiệu độc hại hoặc đã bị báo cáo.
4. **Xem header (chỉ kiểm tra, không tải nội dung)** bằng lệnh HEAD/curl -I trên terminal để thấy header Location (nơi chuyển hướng) — ví dụ curl -I <https://bit.ly/3xyzABC>.
5. **Sao chép (copy) link rồi dán vào một trình soạn thảo văn bản** hoặc công cụ trực tuyến để bỏ trạng thái click-able, rồi kiểm tra an toàn như ở bước 2–3.

## **Ít nhất 3 công cụ / phương pháp cụ thể**

* **Bitly preview (+)** — cách nhanh để xem trang đích của bit.ly mà không truy cập.
* **CheckShortURL / Unshorten.It / unshorten.me** — các dịch vụ chuyên mở rộng link rút gọn và hiển thị URL đích.
* **VirusTotal (**[**https://www.virustotal.com**](https://www.virustotal.com)**)** — quét URL bằng nhiều engine để phát hiện phishing/malware.
* **PhishTank / URLVoid / Sucuri** — kiểm tra xem URL có bị báo cáo là phishing hoặc host mã độc hay không.
* **curl -I / wget --spider** — kiểm tra header HTTP để biết nơi redirect (dành cho người quen dùng dòng lệnh).

## **Tại sao link rút gọn thường được dùng trong lừa đảo**

1. **Che giấu URL thật:** Link rút gọn giấu tên miền đích, khiến nạn nhân không biết họ sẽ đến trang nào — dễ dùng để mạo danh ngân hàng, dịch vụ.
2. **Qua mặt bộ lọc và người dùng:** Nhiều hệ thống lọc hoặc người dùng đánh giá link bằng mắt thường; link rút gọn làm khó việc kiểm tra và tăng tỉ lệ click.
3. **Tạo cảm giác cấp bách / tò mò:** các nút “bit.ly/…”, “free-gift…”, quảng cáo khuyến mãi thường kích thích người dùng click ngay mà không kiểm tra kỹ.