# Kiểm tra link rút gọn

## 1) Nếu muốn kiểm tra mà không nhấn trực tiếp, bạn có thể làm thế nào?

1. Xem trước (preview) liên kết mà không click:  
- Di chuột lên liên kết (hover) để xem URL đầy đủ.  
- Sao chép địa chỉ liên kết và dán vào nơi an toàn để kiểm tra.  
  
2. Mở liên kết đã rút gọn trong công cụ unshortener để biết đích đến thực sự.  
  
3. Sử dụng dịch vụ kiểm tra URL (như VirusTotal) để quét.  
  
4. Dùng lệnh dòng (curl -I -L) để xem header/redirect mà không tải nội dung.  
  
5. Sử dụng môi trường an toàn (sandbox, máy ảo) nếu buộc phải mở link.

## 2) Ít nhất 3 công cụ hoặc cách thức giúp kiểm tra link rút gọn

1. CheckShortURL (checkshorturl.com): Hiển thị URL đích và thông tin meta.  
2. Unshorten.It (unshorten.it): Giải mã link rút gọn và mô tả ngắn.  
3. VirusTotal (virustotal.com): Quét URL bằng nhiều bộ phát hiện.  
4. URLVoid, Sucuri: Phân tích rủi ro và blacklist.  
5. Với bit.ly có thể thêm dấu cộng (+) để xem thông tin preview.

## 3) Tại sao link rút gọn thường được dùng trong lừa đảo?

1. Che giấu đích đến thực sự, khiến người dùng không biết trang web thật.  
2. Link ngắn gọn, dễ gây tin tưởng.  
3. Có thể né tránh một số bộ lọc URL.  
4. Dễ tạo và thay đổi đích nhanh chóng.  
5. Tin tặc tận dụng công cụ thống kê để tối ưu chiến dịch lừa đảo.

## 4) Lời khuyên an toàn khi nhận link rút gọn qua email

- Không click trực tiếp vào email khả nghi.  
- Sao chép và kiểm tra bằng unshortener hoặc VirusTotal.  
- Không nhập thông tin nhạy cảm ở trang đích lạ.  
- Kiểm tra địa chỉ email người gửi.  
- Bật xác thực hai yếu tố (2FA) cho tài khoản quan trọng.

## 5) Kết luận ngắn gọn

Link rút gọn tiện lợi nhưng tiềm ẩn nguy cơ bị lợi dụng trong lừa đảo. Hãy luôn kiểm tra bằng công cụ unshortener, trình quét URL và cẩn trọng với email từ người lạ.