# Phân loại an toàn / không an toàn cho các địa chỉ website

## 1. Giải thích nhanh (nếu cần)

Một website được xem là **“an toàn”** nếu sử dụng giao **thức bảo mật (HTTPS)**, có địa chỉ **tên miền rõ ràng, uy tín** và **không chứa các yếu tố lừa đảo (phishing, nội dung giả mạo).** Nếu website sử dụng HTTP không **mã hóa, tên miền bất thường hoặc giả mạo dựa vào thương hiệu nổi tiếng,** thì có nguy cơ **không an toàn**.

## 2. Bảng phân loại và giải thích

| **Địa chỉ website** | **Phân loại** | **Giải thích (ít nhất 2 lý do)** |
| --- | --- | --- |
| [https://www.vietcombank.com.vn](https://www.vietcombank.com.vn?utm_source=chatgpt.com" \t "_new) | An toàn | 1. Sử dụng HTTPS và tên miền chính thức của ngân hàng Vietcombank, có chứng chỉ bảo mật SSL.  2. Tổ chức, thương hiệu lớn nên khả năng trở thành trang giả mạo giảm nếu đăng nhập từ link chính. |
| [http://secure-vietcombank-login.com](http://secure-vietcombank-login.com" \t "_new) | Không an toàn | 1. Dùng HTTP không mã hóa, thông tin truyền đi dễ bị nghe lén (sniffing).  2. Tên miền có chứa từ “secure-vietcombank-login” nhưng không phải tên miền chính thức của ngân hàng — rất có thể là trang phishing giả mạo để đánh cắp thông tin đăng nhập. |
| [https://facebook.com](https://facebook.com?utm_source=chatgpt.com" \t "_new) | An toàn | 1. Dùng HTTPS, mã hóa dữ liệu giữa trình duyệt và máy chủ.  2. Tên miền chính xác “facebook.com” — thương hiệu lớn, độ uy tín cao, ít khả năng bị giả mạo nếu bạn truy cập đúng địa chỉ. |
| [http://free-gift-now.info](http://free-gift-now.info" \t "_new) | Không an toàn | 1. Dùng HTTP — không mã hóa, dễ bị can thiệp hoặc nghe trộm dữ liệu.  2. Tên miền lạ, chứa cụm “free-gift-now” thường dùng trong chiêu trò lừa tặng quà miễn phí để dụ người dùng click vào, khả năng chứa mã độc hoặc lừa đảo cao. |

## 3. Ghi chú cho việc sử dụng và cảnh giác

1. Khi truy cập trang web liên quan đến ngân hàng, tài chính hoặc thông tin cá nhân quan trọng, **luôn kiểm tra giao thức HTTPS và biểu tượng ổ khóa** trên thanh địa chỉ.
2. Kiểm tra **tên miền kỹ càng — nếu tên miền dài, lạ hoặc chứa từ bổ sung giống thương hiệu nổi tiếng thì rất có khả năng là giả mạo.**
3. **Tránh nhấp vào các liên kết từ email, tin nhắn không rõ nguồn nếu chứa đường dẫn đến trang đăng nhập ngân hàng hay nơi bạn nhập mật khẩu.**