**Bảng phân loại**

| **Website** | **An toàn / Không an toàn** | **Lý do** |
| --- | --- | --- |
| [https://www.vietcombank.com.vn](https://www.vietcombank.com.vn?utm_source=chatgpt.com) | An toàn | Sử dụng **HTTPS** mã hóa, tên miền chính thức của ngân hàng, có chứng chỉ SSL hợp lệ. |
| <http://secure-vietcombank-login.com> | Không an toàn | Dùng **HTTP** (không mã hóa), tên miền giả mạo (có chứa từ “secure-vietcombank-login”) có thể là trang phishing. |
| <https://facebook.com> | An toàn | Sử dụng **HTTPS**, tên miền chính thức của Facebook, chứng chỉ SSL hợp lệ. |
| <http://free-gift-now.info> | Không an toàn | Dùng HTTP không mã hóa, tên miền lạ, đuôi ".info" thường xuất hiện trong các trang giả mạo hoặc spam. |

**Giải thích chi tiết**

1. **Với các website an toàn**:
   * Sử dụng **HTTPS** (SSL/TLS) để mã hóa luồng dữ liệu giữa trình duyệt và máy chủ, giúp ngăn chặn việc dữ liệu bị nghe lén hoặc can thiệp.
   * Tên miền chuẩn xác, có độ tin cậy cao (ví dụ facebook.com, vietcombank.com.vn), có chứng chỉ SSL hợp lệ do các tổ chức tín nhiệm cấp.
2. **Với các website không an toàn**:
   * Dùng **HTTP** nên dữ liệu gửi đến không được mã hóa — tin tặc có thể dễ dàng chặn hoặc thay đổi nội dung.
   * Tên miền đáng ngờ hoặc giả mạo (có từ “secure”, “login”, “free-gift”…) là đặc điểm phổ biến của các trang phishing hoặc lừa đảo.
   * Ngoài ra, đuôi tên miền như “.info”, “.xyz” hay những tên miền mới thường được kẻ xấu lợi dụng để tạo trang lừa đảo vì chi phí đăng ký thấp.