**5 Dấu hiệu nhận biết Email/Website lừa đảo**

**1. Địa chỉ Email/Tên miền không chính thức (Giả mạo)**

Kẻ lừa đảo thường giả mạo các tổ chức, công ty uy tín (ngân hàng, mạng xã hội, cơ quan nhà nước) bằng cách sử dụng địa chỉ email hoặc tên miền có chứa lỗi chính tả, thêm/bớt ký tự hoặc sử dụng tên miền phụ/đuôi lạ.

* **Dấu hiệu:**
  + **Email:** Địa chỉ email người gửi không khớp với tên miền chính thức của tổ chức (ví dụ: gửi từ @gmail.com, @hotmail.com thay vì tên miền công ty như @tencongty.com). Hoặc tên miền bị sai lệch tinh vi (ví dụ: support@paypall.com thay vì support@paypal.com).
  + **Website:** Đường link (URL) có lỗi chính tả hoặc thêm các ký tự/tên miền lạ (ví dụ: vietcombanker.com, shopeepv.com, dien-may-xanh.net).
* **Ví dụ:**
  + **Email lừa đảo:** Nhận được email từ người gửi là "Ngân hàng ACB" nhưng địa chỉ email lại là acb-thongbao@gmail.com hoặc hotro@acbvip.com.
  + **Website lừa đảo:** Bạn nhấp vào một liên kết trông giống như https://www.google.com/, nhưng khi kiểm tra thanh địa chỉ, nó lại là https://www.gooogle.info/dangnhap.php.

**2. Nội dung tạo cảm giác khẩn cấp, sợ hãi hoặc hấp dẫn quá mức**

Những kẻ lừa đảo lợi dụng cảm xúc để khiến bạn hành động thiếu suy nghĩ (hoảng sợ, tò mò, tham lam).

* **Dấu hiệu:**
  + Thông báo **khẩn cấp** về việc tài khoản bị khóa, thẻ tín dụng bị xâm nhập, nợ tiền, hoặc cần hành động ngay lập tức để tránh hậu quả nghiêm trọng.
  + Đưa ra các lời hứa hẹn **hấp dẫn quá mức** như trúng thưởng số tiền lớn, nhận quà tặng giá trị, hoặc cơ hội làm giàu nhanh chóng.
* **Ví dụ:**
  + **Email lừa đảo:** Tiêu đề "CẢNH BÁO: Tài khoản Ngân hàng của bạn sẽ bị đình chỉ trong 24 giờ! **Nhấp vào đây ngay** để xác thực."
  + **Website lừa đảo:** Một trang web hiển thị thông báo bật lên: "Chúc mừng! Bạn là khách hàng thứ 1.000.000 và đã **trúng thưởng một chiếc iPhone mới**. Hãy nhập thông tin nhận thưởng!"

**3. Yêu cầu cung cấp thông tin cá nhân/nhạy cảm**

Các tổ chức uy tín (ngân hàng, dịch vụ trực tuyến) **hầu như không bao giờ** gửi email yêu cầu bạn nhấp vào liên kết để nhập lại mật khẩu, số thẻ tín dụng, mã số bí mật (PIN/OTP), hoặc các thông tin cá nhân nhạy cảm khác.

* **Dấu hiệu:**
  + Email hoặc website giả mạo có biểu mẫu yêu cầu bạn nhập **tên đăng nhập, mật khẩu, số CMND/CCCD, hoặc thông tin thẻ ngân hàng** để "xác minh", "cập nhật" hoặc "lấy lại quyền truy cập".
* **Ví dụ:**
  + **Email lừa đảo:** "Chúng tôi đang cập nhật hệ thống bảo mật. Vui lòng nhấp vào liên kết dưới đây để **đăng nhập và xác nhận lại mật khẩu** của bạn."
  + **Website lừa đảo:** Một trang đăng nhập giả mạo có giao diện giống hệt ngân hàng của bạn, yêu cầu bạn nhập **tên đăng nhập và mật khẩu** để "mở khóa tài khoản".

**4. Liên kết (Link) đáng ngờ**

Đây là dấu hiệu quan trọng nhất. Liên kết trong email lừa đảo thường dẫn bạn đến một trang web giả mạo để lấy cắp thông tin.

* **Dấu hiệu:**
  + Khi **di chuột** (không nhấp) lên đường link trong email, địa chỉ URL hiển thị ở góc màn hình khác hoàn toàn so với mô tả của liên kết hoặc khác với tên miền chính thức của tổ chức.
  + Website không bắt đầu bằng **https://** (chữ "s" thể hiện kết nối an toàn) hoặc không có biểu tượng ổ khóa bên cạnh địa chỉ.
* **Ví dụ:**
  + **Email lừa đảo:** Văn bản hiển thị là "Nhấp vào đây để đến trang chủ **Facebook**", nhưng khi di chuột, đường link thực tế lại là http://fb.dangnhaptaikhoan.xyz/.
  + **Website lừa đảo:** Trang web có giao diện giống Cổng Dịch vụ công Quốc gia nhưng đường link lại là https://dichvucong.dancuso.com.

**5. Lỗi ngữ pháp, chính tả, cách xưng hô chung chung**

Email lừa đảo, đặc biệt là email gửi hàng loạt, thường được dịch hoặc viết vội vàng nên mắc nhiều lỗi chính tả, ngữ pháp hoặc sử dụng cách xưng hô không cá nhân hóa.

* **Dấu hiệu:**
  + Nội dung email có các lỗi viết hoa, dấu câu, hoặc cú pháp câu thiếu tự nhiên.
  + Cách chào hỏi chung chung như: "Kính gửi Chủ tài khoản," "Gửi Thành viên thân mến," hoặc không đề cập đến tên của bạn. (Trong khi các công ty hợp pháp thường chào bạn bằng tên).
* **Ví dụ:**
  + **Email lừa đảo:** "Thân gửi **Khách Hàng**. **Tai Khoản** của bạn đã bị ***Khóa***. Chúng tôi cần **Xác minh Thong Tin** của bạn ngay lập Tức." (Nhiều lỗi chính tả, ngữ pháp).
  + **Website lừa đảo:** Các phần nội dung trên website có câu chữ lủng củng, sử dụng phông chữ không đồng nhất, hoặc hình ảnh có chất lượng thấp.

**Điều quan trọng nhất:** Luôn kiểm tra kỹ lưỡng địa chỉ người gửi và đường link trước khi nhấp vào. Nếu nghi ngờ, hãy truy cập trực tiếp trang web chính thức (bằng cách gõ địa chỉ vào trình duyệt) thay vì nhấp vào liên kết trong email.  
  
Nguồn tham khảo:

[***Google Gemini***](https://gemini.google.com/)*, prompt: Dấu hiệu nhận biết Email/Website lừa đảo*

[***7 Cách để nhận biết một email lừa đảo và email giả - vnetwork***](https://www.vnetwork.vn/news/7-cach-de-nhan-biet-mot-email-lua-dao/)

[***Cách nhận biết email lừa đảo và website không an toàn – bộ khoa học và công nghệ Việt Nam***](https://mst.gov.vn/cach-nhan-biet-email-lua-dao-va-website-khong-an-toan-197142763.htm)

[***Bộ Công an hướng dẫn cách nhận diện website lừa đảo – báo điện tử Chính Phủ***](https://baochinhphu.vn/bo-cong-an-huong-dan-cach-nhan-dien-website-lua-dao-102250124133511758.htm)