**THỰC HÀNH NHẬN DIỆN LỪA ĐẢO & NGUY CƠ ONLINE / PRACTICE REPORT – PHISHING & ONLINE THREATS**

## I. 5 EMAIL MẪU (GIẢ LẬP) / 5 SAMPLE EMAILS (FICTIONAL)

**Email 1: Khóa tài khoản trong 24h – Xác minh ngay / Account locked in 24h - Verify now**

From: support@goog1e-security.com

To: anhb2505821@student.ctu.edu.vn

Body:

Kính gửi người dùng, Tài khoản của bạn sẽ bị khóa trong 24 giờ nếu không xác minh. Vui lòng truy cập: http://secure-verify.example/login để nhập thông tin OTP.

**Email 2: Biên lai học phí học kỳ / Tuition receipt - semester**

From: finance@cantho-university.edu.vn

To: anhb2505821@student.ctu.edu.vn

Body:

Kính gửi sinh viên, đính kèm biên lai học phí của học kỳ này. Vui lòng kiểm tra file đính kèm PDF để xem chi tiết.

**Email 3: Thông báo trúng thưởng quà tặng / You won a prize!**

From: promo@lucky-event.example

To: anhb2505821@student.ctu.edu.vn

Body:

Chúc mừng! Bạn đã trúng quà. Nhấn vào liên kết rút gọn để nhập thông tin nhận quà: http://bit.ly/win-prize-example

**Email 4: Yêu cầu cập nhật thông tin sinh viên / Update student record**

From: admin@ctu.edu.vn

To: anhb2505821@student.ctu.edu.vn

Body:

Vui lòng cập nhật thông tin tại portal chính thức: https://portal.cantho.edu.vn/profile. (Lưu ý: email này thật, kiểm tra token bên trong portal để xác nhận).

**Email 5: File kết quả thi – download\_now.exe**

From: noreply@examresults.example

To: anhb2505821@student.ctu.edu.vn

Body:

Kết quả thi đã được cập nhật. Tải file đính kèm để xem kết quả: download\_now.exe

## II. PHÂN TÍCH EMAIL & KẾT LUẬN / ANALYSIS & CONCLUSIONS

|  |  |  |  |
| --- | --- | --- | --- |
| Email ID | Thật/Giả (Real/Fake) | Dấu hiệu nghi ngờ / Suspicious signs | Kết luận & Hành động / Conclusion & Action |
| Email 1 | Giả / Fake | Tên miền gửi giả mạo (ví dụ support@goog1e-security.com có ký tự giống Google nhưng không phải), chứa liên kết HTTP (không phải HTTPS) dẫn tới miền lạ (secure-verify.example), ngôn từ tạo cảm giác khẩn cấp yêu cầu nhập OTP. | Lừa đảo (phishing). Không bấm vào link, không nhập OTP hay thông tin cá nhân; báo cáo cho bộ phận CNTT/giảng viên và xóa email |
| Email 2 | Thật / Real | (Không thấy dấu hiệu bất thường rõ rệt) Gửi từ miền chính thức của trường (ví dụ finance@cantho-university.edu.vn), định dạng trang trọng và đính kèm file PDF. | Có khả năng hợp lệ. Mở file đính kèm trong môi trường an toàn (ví dụ trên máy có phần mềm diệt virus) hoặc xác minh trực tiếp qua cổng thông tin trường (không bấm link trong email nếu có). |
| Email 3 | Giả / Fake | Người gửi không rõ ràng (địa chỉ quảng cáo), thông báo trúng thưởng bất ngờ; chứa link rút gọn (ví dụ bit.ly) làm che giấu đích đến. | Lừa đảo / có nguy cơ chứa mã độc. Không bấm vào link, không cung cấp thông tin cá nhân; báo cáo và xóa email. |
| Email 4 | Thật / Real | Gửi từ miền chính thức của trường (ví dụ admin@ctu.edu.vn) và liên kết dẫn tới trang portal chính thức với HTTPS. (Nếu có token hoặc yêu cầu đăng nhập, cần kiểm tra kỹ.) | Có khả năng hợp lệ. Truy cập trực tiếp vào trang portal bằng cách gõ địa chỉ trong trình duyệt (không bấm link trong email) để cập nhật; nếu có nghi ngờ, xác minh với phòng hành chính/trường. |
| Email 5 | Giả / Fake | File đính kèm là tệp thực thi (.exe) — hiếm khi trường gửi file .exe; tên miền gửi lạ/không rõ. | Có nguy cơ chứa mã độc. Không tải hay mở tệp .exe; xóa email và chạy quét virus trên thiết bị nếu đã nhỡ tải/khởi chạy. |

## III. QUY TRÌNH PHÂN TÍCH ĐÃ THỰC HIỆN / STEPS PERFORMED

1. Nhóm phân công: mỗi thành viên đọc 1 email và ghi lại các dấu hiệu đáng ngờ.  
2. Thảo luận trong 15 phút: so sánh dấu hiệu giữa các email.  
3. Kiểm tra link (mô phỏng): dán link vào VirusTotal / Google Safe Browsing để kiểm tra.  
4. Kết luận: đánh dấu email thật/giả và đề xuất hành động.  
5. Viết báo cáo và chuẩn bị thông báo nội bộ nếu phát hiện phishing.

## IV. 5 DẤU HIỆU NHẬN BIẾT EMAIL/WEBSITE LỪA ĐẢO / TOP 5 SIGNS OF PHISHING

1. Sender domain giả mạo hoặc gần giống domain thật (typosquatting).  
2. Ngôn ngữ khẩn cấp hoặc đe dọa (thời hạn 24h, khóa tài khoản).  
3. Link rút gọn hoặc link text khác URL (hover to check real URL).  
4. Đính kèm file thực thi (.exe, .scr) hoặc file lạ.  
5. Yêu cầu cung cấp thông tin nhạy cảm (mật khẩu, OTP, mã số thẻ).

## V. KHUYẾN NGHỊ & HÀNH ĐỘNG / RECOMMENDATIONS & ACTIONS

1. Luôn kiểm tra tên miền trước khi nhấp và không cung cấp OTP cho bất kỳ ai.  
2. Sử dụng VirusTotal/Google Safe Browsing để kiểm tra link nghi ngờ.  
3. Nếu nhận email khả nghi, báo cáo cho bộ phận CNTT hoặc giảng viên.  
4. Tổ chức buổi hướng dẫn ngắn cho lớp về cách báo cáo phishing.

Báo cáo được xây dựng dưới sự hướng dẫn của AI Chatgpt