**BÁO CÁO THỰC HÀNH**   
**Nhận diện lừa đảo & nguy cơ online — Tiết 3 (Cá nhân)**

**1) 5 email mẫu (tóm tắt phân loại)**  
- Mẫu A (Giả - Ngân hàng): support@vietbank-security.com — link rút gọn bit.ly — Dấu hiệu: domain lạ, khẩn cấp.  
- Mẫu B (Thật - Shopee): no-reply@shopee.vn — link HTTPS chuẩn — Dấu hiệu: đáng tin.  
- Mẫu C (Giả - Trúng thưởng): lucky@prize.events — yêu cầu phí, domain lạ.  
- Mẫu D (Thật - Giảng viên): letruong@truongdh.edu.vn — link meet.google.com — đáng tin.  
- Mẫu E (Giả - Microsoft): security@microsoffice.com — file .zip đính kèm, domain sai.

**2) Kiểm tra link (tóm tắt hướng dẫn)**  
- VirusTotal: dán URL vào tab URL → nếu nhiều engine báo malicious → không truy cập.  
- Google Safe Browsing (Transparency Report): dán URL → nếu báo Unsafe → không truy cập.  
- Kiểm tra header (SPF/DKIM) nếu có thể.

**3) 5 dấu hiệu nhận biết email/wedsite lừa đảo**  
1. Domain/email bất thường (sai chính tả hoặc domain gần giống).   
2. Nội dung gây áp lực/khẩn cấp.  
3. Yêu cầu cung cấp thông tin nhạy (mật khẩu, OTP, thẻ).  
4. Link rút gọn hoặc file đính kèm lạ (.zip/.exe).  
5. Lỗi chính tả, logo kém, thiếu thông tin liên hệ.

**4) Hành động đề xuất**- Không click link lạ, không mở file đính kèm nghi ngờ.  
- Quét URL bằng VirusTotal & kiểm tra Google Safe Browsing.  
- Bật 2FA, đổi mật khẩu nếu đã cung cấp thông tin, báo cáo cho IT.