Báo cáo tiết 3: Thực hành nhận diện lừa đảo & nguy cơ online

5 Dấu Hiệu Nhận Biết Email/Website Lừa Đảo

**1. Yêu Cầu Khẩn Cấp hoặc Đe Dọa:**

* Tin nhắn tạo ra cảm giác sợ hãi hoặc cực kỳ khẩn cấp để bạn hành động ngay lập tức, không kịp suy nghĩ.
* Ví dụ:

"Tài khoản của bạn sẽ bị khóa trong 24 giờ nếu không xác minh ngay!"

"Có một giao dịch đáng ngờ, hãy xác nhận thông tin ngay lập tức!"

"Bạn đã trúng thưởng, hãy nhanh chóng cung cấp thông tin để nhận quà!"

**2. Yêu Cầu Thông Tin Cá Nhân Nhạy Cảm:**

* Một tổ chức hợp pháp (ngân hàng, Facebook, Apple...) gần như không bao giờ yêu cầu bạn cung cấp thông tin nhạy cảm qua email hoặc tin nhắn.
* Thông tin bị yêu cầu:

1. Mật khẩu
2. Số CMND/CCCD
3. Số thẻ tín dụng và mã CVV
4. Mã PIN

**3. Địa Chỉ Email, Link hoặc Website Giả Mạo:**

* Kẻ lừa đảo dùng các địa chỉ gần giống với thật để đánh lừa.
* Cách kiểm tra:
  + Với email: Kiểm tra kỹ địa chỉ người gửi. Ví dụ, email giả mạo Apple có thể gửi từ apple-support@gmail.com thay vì tên miền chính thức @apple.com.
  + Với link: Di chuột (không click):vào liên kết để xem địa chỉ thật. Một liên kết giả mạo có thể trông như http://dang-nhap-facebook.xyz thay vì https://www.facebook.com.
  + Với website: Kiểm tra kỹ thanh địa chỉ trình duyệt. Website giả thường dùng tên miền gần giống (vd: paypa1.com với số "1" thay chữ "l", hoặc amaz0n.com với số "0").

**4. Lỗi Ngữ Pháp và Chính Tả:**

* Các email/website lừa đảo thường chứa nhiều lỗi chính tả, ngữ pháp kỳ lạ và cách dùng từ thiếu chuyên nghiệp.
* Ví dụ: "Xin chào quý khãch. Tài khoản của bạn có nguy cơ bị khóa. Vui lòng cập nhât thông tin ngay de tiếp tục sử dụng dịch vụ."

**5. Lời Chào Chung Chung và Giao Diện Bất Thường:**

* Lời chào: Email thường bắt đầu bằng "Kính gửi Quý khách hàng" hoặc "Thưa Ông/Bà" thay vì dùng tên thật của bạn.
* Giao diện: Website giả mạo có thể có logo mờ nhạt, hình ảnh chất lượng thấp, bố cục lộn xộn hoặc các nút bấm không hoạt động. Dù trông có vẻ giống thật, nhưng nó sẽ có cảm giác "sai sai".