**TIỂU LUẬN AN TOÀN THÔNG TIN**

### ĐỀ TÀI 5: Social Engineering trong An toàn thông tin

#### I. Giới thiệu chung

**Social Engineering** (Kỹ thuật lừa đảo phi kỹ thuật) là hành vi khai thác yếu tố con người để đánh lừa, lấy cắp thông tin, hoặc tạo điều kiện cho tấn công mạng.

Không cần kỹ thuật cao, Social Engineering thường thành công nhờ sự thiếu cảnh giác, lòng tin, và thiếu kiến thức bảo mật của nạn nhân.

Đây là mắt xích yếu nhất trong chuỗi an toàn thông tin.

#### II. Các dạng tấn công Social Engineering phổ biến

|  |  |  |
| --- | --- | --- |
| **STT** | **Hình thức** | **Cách demo thực tế** |
| 1 | **Phishing** | Gửi email giả mạo có link Google Form yêu cầu nhập mật khẩu. |
| 2 | **Spear Phishing** | Gửi email có tên và chức vụ cụ thể người nhận, tăng tính thuyết phục. |
| 3 | **Whaling** | Gửi email giả mạo giám đốc yêu cầu chuyển khoản gấp. |
| 4 | **Pretexting** | Giả danh IT gửi email/chat yêu cầu xác nhận tài khoản. |
| 5 | **Reverse Social Engineering** | Tạo sự cố máy tính/ứng dụng, rồi tiếp cận với vai trò “hỗ trợ kỹ thuật”. |
| 6 | **Baiting** | Tạo file hấp dẫn (PDF/Excel/USB giả) có tiêu đề như “lương tháng”, “ảnh nóng”… |
| 7 | **Fake Login Page** (thay thế shoulder surfing) | Dẫn người dùng vào trang đăng nhập giả (demo offline, không ghi dữ liệu thật). |
| 8 | **QR Code Phishing (Quishing)** | Tạo mã QR dẫn tới form giả mạo – người dùng scan và nhập thông tin. |
| 9 | **Chat giả mạo nội bộ** | Dùng công cụ chat giả lập nội bộ (ví dụ Notepad, ảnh), giả danh phòng ban hỗ trợ. |
| 10 | **Fake Tech Support Call Script** (thay thế vishing) | Viết kịch bản hoặc ghi âm cuộc gọi hỗ trợ giả yêu cầu người dùng thao tác. |
| 11 | **Fake Notification Popup** | Tạo popup giả trên máy ảo: “Hệ thống cần xác thực tài khoản” → dẫn đến form. |
| 12 | **Email Spoofing Demo** | Sử dụng email giống it-support@domain.co để lừa người dùng. |

#### III. Tình huống thực tế

**Vụ CEO Fraud:** Hacker giả danh giám đốc gửi email yêu cầu kế toán chuyển tiền gấp → mất hàng trăm nghìn USD.

**Giả danh IT nội bộ:** Hacker gọi điện, giả danh bộ phận kỹ thuật, yêu cầu cung cấp mật khẩu để "nâng cấp hệ thống" → chiếm đoạt hệ thống.

**Tình huống mô phỏng:**

Nhân viên A nhận email từ địa chỉ giả it-support@xyz-corp.co, yêu cầu xác nhận tài khoản qua Google Form.

Nhân viên A nhập email, mật khẩu và OTP.

Hacker đăng nhập vào hệ thống, lấy dữ liệu khách hàng → tiếp tục lừa đảo.

#### IV. Biện pháp phòng chống

**Giáo dục & nâng cao nhận thức:**

Tập huấn định kỳ, mô phỏng tấn công phishing.

**Chính sách nội bộ:**

Quy định không cung cấp thông tin qua email, xác minh 2 bước với các giao dịch quan trọng.

**Kiểm thử định kỳ:**

Tổ chức kiểm tra phản ứng của nhân viên với email giả lập.

**Công nghệ hỗ trợ:**

Sử dụng xác thực 2 lớp (2FA), bộ lọc thư rác/phishing, hệ thống phát hiện truy cập bất thườg.

#### V. Kết luận

Social Engineering không đòi hỏi kỹ thuật cao nhưng cực kỳ nguy hiểm nếu người dùng mất cảnh giác.

Con người là điểm yếu quan trọng – cần kết hợp đào tạo, quy trình, công nghệ để đảm bảo an toàn thông tin.

### PHỤ LỤC LAB MÔ PHỎNG: TẤN CÔNG & PHÒNG THỦ SOCIAL ENGINEERING

#### 🎯 Mục tiêu

Mô phỏng một cuộc tấn công phishing qua email.

Ghi nhận hành vi người dùng và cách phản ứng/phòng vệ.

#### 🧪 A. Mô phỏng tấn công

**Tạo email giả:**

Địa chỉ: it.support.xyzcorp@gmail.com

Tiêu đề: [Cảnh báo] Xác nhận tài khoản bảo mật

Nội dung: yêu cầu truy cập biểu mẫu để tránh bị khóa tài khoản.

**Tạo Google Form:**

Gồm các trường: Email, mật khẩu, OTP (giả lập).

Giao diện giống biểu mẫu thật.

**Gửi và ghi nhận:**

Gửi cho người đóng vai nạn nhân trong nhóm.

Ghi nhận hành vi: người nhận có mở link không, có nhập thông tin không (dùng dữ liệu giả).

**Hình minh họa chụp lại:**

Email phishing

Giao diện biểu mẫu

Sơ đồ luồng tấn công: Hacker → Email → Người dùng → Nhập thông tin → Bị xâm nhập

#### B. Mô phỏng phòng thủ

**Phản ứng từ hệ thống:**

Gmail/Google Workspace cảnh báo địa chỉ gửi đáng ngờ.

Cảnh báo khi biểu mẫu đòi hỏi thông tin nhạy cảm.

**Phản ứng từ người dùng:**

Kiểm tra domain người gửi

Không nhập dữ liệu nếu thấy nghi ngờ.

Báo ngay với phòng CNTT.

**Hình ảnh minh họa:**

Giao diện cảnh báo email đáng ngờ

Hộp thoại chặn truy cập form lạ