**1. Định nghĩa:** Xác thực hai lớp (2FA – Two-Factor Authentication) là cơ chế bảo mật yêu cầu người dùng cung cấp **hai yếu tố xác minh** khi đăng nhập: mật khẩu và một mã xác thực thứ hai (ví dụ: mã OTP, thông báo điện thoại, hoặc khóa bảo mật). Nó giúp tăng cường bảo vệ tài khoản khỏi bị truy cập trái phép ngay cả khi mật khẩu bị lộ.

**2. Ba lợi ích khi bật 2FA:**

1. **Tăng mức độ bảo mật**, ngăn kẻ xấu đăng nhập dù có mật khẩu.
2. **Nhận cảnh báo đăng nhập lạ**, giúp phát hiện sớm nguy cơ bị xâm nhập.
3. **Bảo vệ thông tin cá nhân và dữ liệu quan trọng** trên email, mạng xã hội.

**3. Ví dụ bật 2FA trên Gmail (Google):**

1. Đăng nhập vào tài khoản Google → vào **Quản lý tài khoản (Google Account)**.
2. Chọn mục **Bảo mật (Security)** → bật **Xác minh 2 bước (2-Step Verification)**.
3. Chọn phương thức xác thực: nhận mã qua **SMS**, **ứng dụng Google Authenticator**, hoặc **khóa bảo mật**.
4. Xác nhận thiết bị và hoàn tất thiết lập — từ nay khi đăng nhập, bạn phải nhập thêm mã xác thực ngoài mật khẩu.