# Bảo mật thông tin cá nhân trên mạng xã hội

## 1. Tình huống ví dụ

Bài đăng giả định trên Facebook:

**“Hôm nay sinh nhật mình, 08/09/2002. Ai tặng quà thì tới số nhà 123, đường Lê Lợi nhé.”**

## 2. Các thông tin nhạy cảm đã bị lộ

Trong bài đăng này, có ít nhất **3 thông tin cá nhân quan trọng** đã bị công khai:

* **Ngày sinh**: 08/09/2002.
* **Địa chỉ nhà riêng**: Số 123, đường Lê Lợi.
* **Họ tên thật** (nếu đăng từ tài khoản thật).
* **Tổng cộng:** 2–3 thông tin nhạy cảm bị lộ có thể bị khai thác để nhận dạng hoặc giả mạo danh tính.

## 3. Cách tin tặc có thể lợi dụng thông tin này

* **Đoán mật khẩu hoặc trả lời câu hỏi bảo mật:** Tin tặc có thể dùng ngày sinh, họ tên để khôi phục hoặc chiếm đoạt tài khoản.
* **Lừa đảo hoặc tiếp cận trực tiếp:** Địa chỉ nhà có thể bị lợi dụng để gửi thư rác, giả danh giao hàng hoặc thực hiện hành vi xấu.
* **Giả mạo danh tính:** Kết hợp thông tin công khai khác (ảnh, bạn bè, nơi làm việc) để tạo hồ sơ giả nhằm lừa đảo người quen hoặc đồng nghiệp của nạn nhân.

## 4. Ba cách bảo mật thông tin cá nhân khi dùng mạng xã hội

1. **Không công khai thông tin nhạy cảm** như ngày sinh, địa chỉ, số điện thoại, số CCCD, hoặc giấy tờ cá nhân.
2. **Thiết lập quyền riêng tư** cho bài đăng, chỉ chia sẻ với bạn bè hoặc nhóm đáng tin cậy.
3. **Sử dụng mật khẩu mạnh và bật xác thực hai yếu tố (2FA)** để bảo vệ tài khoản khỏi bị truy cập trái phép.

## 5. Kết luận

Việc chia sẻ quá nhiều thông tin cá nhân trên mạng xã hội có thể dẫn đến **rủi ro về bảo mật, lừa đảo hoặc đánh cắp danh tính**.  
Người dùng cần **cân nhắc kỹ nội dung đăng tải**, **thiết lập quyền riêng tư phù hợp**, và **nâng cao ý thức bảo vệ thông tin cá nhân** trong môi trường số.