**1. Thông tin nhạy cảm đã bị lộ**

Thông tin nhạy cảm bao gồm:

**-** Ngày sinh cụ thể: 08/09/2002

- Địa chỉ nhà (một phần đầy đủ): Số nhà 123, đường Lê Lợi

- Thông tin cá nhân được xác nhận công khai: Hôm nay là sinh nhật → xác định ngày hiện tại, khớp với ngày sinh

=> Tổng cộng có ít nhất 2–3 thông tin nhạy cảm bị lộ, đủ để xác định danh tính cá nhân.

**2. Tin tặc có thể lợi dụng thông tin này như thế nào?**

Các nguy cơ tiềm ẩn:

**-** Xác thực danh tính giả mạo:

+ Ngày sinh thường được dùng làm câu hỏi bảo mật hoặc xác thực tài khoản ngân hàng, email, dịch vụ online.

+ Tin tặc có thể dùng thông tin này để khôi phục mật khẩu, chiếm quyền tài khoản.

- Tấn công xã hội (social engineering):

+ Dựa vào ngày sinh và địa chỉ, tin tặc có thể giả làm bạn bè/giao hàng/nhân viên dịch vụ để lừa người thân hoặc chính chủ nhân.

+ Tạo các email/sms lừa đảo đúng thời điểm sinh nhật để dẫn dụ bấm vào link độc hại.

- Định vị cá nhân trong đời thực:

+ Biết địa chỉ + thời điểm cụ thể bạn có thể ở nhà, kẻ xấu có thể theo dõi, tiếp cận, gây nguy hiểm.

**3. Ba cách bảo mật thông tin cá nhân khi dùng mạng xã hội**

- Hạn chế chia sẻ thông tin cá nhân công khai

+ Không nên đăng công khai ngày sinh, địa chỉ nhà, số điện thoại, trường học, nơi làm việc...

+ Nếu cần chia sẻ, hãy chọn chế độ **"Bạn bè"** hoặc **"Chỉ mình tôi"** thay vì **"Công khai"**.

- Sử dụng cài đặt quyền riêng tư hợp lý

+ Thường xuyên kiểm tra phần **“Quyền riêng tư”** của tài khoản.

+ Giới hạn người có thể xem bài đăng, tìm kiếm bạn qua email/số điện thoại.

- Không đăng bài theo thời gian thực về vị trí

+ Tránh gắn thẻ địa điểm hoặc thông báo bạn đang **ở đâu/làm gì** tại thời điểm thực.

+ Nếu muốn chia sẻ, hãy đăng sau khi bạn đã rời khỏi nơi đó.