Rủi ro an ninh thông tin sinh viên có thể gặp

Link khảo sát:

<https://docs.google.com/forms/d/e/1FAIpQLSfXfahowbJ-F_uuoA-KpIsmZ9fk6hEQjKEN3Q5qLn-resZF_Q/viewform?usp=dialog>

- Lừa đảo qua email (Phishing): Sinh viên có thể nhận được email giả mạo từ kẻ xấu, yêu cầu cung cấp thông tin cá nhân như mật khẩu, tài khoản ngân hàng hoặc thông tin đăng nhập hệ thống trường học.

- Sử dụng mạng Wi-Fi công cộng không an toàn: Khi sử dụng Wi-Fi công cộng tại các quán cà phê, thư viện, hay trong khuôn viên trường, sinh viên có thể bị tấn công bởi hacker thông qua các phương thức như "Man-in-the-middle", làm lộ thông tin cá nhân.

- Tấn công malware và ransomware: Sinh viên có thể vô tình tải về phần mềm độc hại hoặc ransomware qua các website không đáng tin cậy hoặc email đính kèm. Điều này có thể gây hư hại cho dữ liệu và hệ thống của họ.

- Mất cắp dữ liệu qua thiết bị di động: Khi sinh viên mất điện thoại hoặc laptop, nếu không có các biện pháp bảo mật như mã hóa dữ liệu, mật khẩu mạnh, hoặc xác thực hai yếu tố, các dữ liệu cá nhân quan trọng có thể bị lộ.

- Lộ thông tin qua mạng xã hội: Sinh viên đôi khi chia sẻ quá nhiều thông tin cá nhân trên các nền tảng mạng xã hội mà không nhận thức được rủi ro. Điều này có thể tạo cơ hội cho kẻ xấu đánh cắp thông tin hoặc thực hiện các cuộc tấn công xã hội

# Sơ đồ tư duy các rủi ro an ninh mạng

