# BÀI 9: AN TOÀN TRÊN KHÔNG GIAN MẠNG

## 1. MỘT SỐ NGUY CƠ TRÊN MẠNG

**Không gian mạng tiềm ẩn nhiều rủi ro:**

- Tin giả và tin phản văn hoá: thông tin sai sự thật, nội dung bạo lực hoặc lệch lạc.
- Lừa đảo trên mạng: giả mạo danh tính cá nhân để lừa tiền hoặc tài sản. Lộ thông tin cá nhân: bị đánh cắp thông tin quan trọng dẫn đến việc bị mạo danh hoặc mất tiền.
- Bắt nạt trên không gian mạng: bị lăng mạ, đe dọa, tống tiền, bôi nhọ danh dự ảnh hưởng tâm lí nặng nề.
- Nghiện mạng: dành quá nhiều thời gian cho mạng và trò chơi điện tử làm hại sức khỏe.

**Biện pháp phòng tránh:**

- Chỉ truy cập các website tin cậy, không tin theo các thông tin xấu, tin giả.
- Bảo vệ thông tin cá nhân: không chia sẻ ở nơi công cộng, cảnh giác mạng wifi công cộng.
- Chỉ kết bạn với người quen biết, không dễ dãi kết bạn.
- Khi bị bắt nạt: không đôi co, lưu bằng chứng và chia sẻ với cha mẹ, thầy cô hoặc báo công an. Không sử dụng Internet quá nhiều.

## 2. PHẦN MỀM ĐỘC HẠI

Phần mềm độc hại (malware) là các phần mềm được tạo ra với ý đồ xấu, gây hại cho thiết bị và người dùng.

### a) Tìm hiểu về virus, trojan, worm và cơ chế hoạt động

- Virus: không phải phần mềm hoàn chỉnh, là đoạn mã độc gắn vào tệp/phần mềm khác để lây lan.
- Worm (sâu máy tính): phần mềm hoàn chỉnh, lợi dụng lỗ hổng hệ điều hành hoặc lừa người dùng tải về để tự lây lan.
- Trojan: phần mềm nội gián để đánh cắp dữ liệu hoặc chiếm quyền kiểm soát (gồm Spyware, Keylogger, Backdoor, Rootkit).

### b) Tác hại của phần mềm độc hại

- Gây khó chịu, hỏng hệ điều hành và các ứng dụng.
- Đánh cắp hoặc mã hoá dữ liệu tống tiền (ví dụ sâu WannaCry).
- Chiếm quyền điều khiển máy tính, tạo mạng máy tính ngầm tấn công từ chối dịch vụ (DOS).

**c) Phòng chống phần mềm độc hại**

- Cẩn trọng khi sao chép tệp từ USB, ổ cứng ngoài hoặc tải về từ mạng.
- Không mở các liên kết lạ, đáng ngờ trong thư điện tử hoặc tin nhắn.
- Bảo mật thông tin tài khoản và mật khẩu.
- Sử dụng các phần mềm diệt virus và phần mềm độc hại.