

K7. D. B2. ỨNG XỬ TRÁNH RỦI RO TRÊN MẠNG

ỦY BAN NHÂN DÂN PHƯỜNG TÂN MỸ

Trường: THCS Phạm Hữu Lầu

Tổ: Công nghệ - Tin học - Nghệ thuật

Giáo viên: Vũ Nguyễn Hoàng Anh

Khối: 7

Năm học: 2025-2026





Giới thiệu bài học

Một học sinh nhận tin nhắn lạ và cảm thấy lo lắng.

Mạng là công cụ hữu ích nhưng cũng tiềm ẩn rủi ro.

Mục tiêu hôm nay: hiểu tác hại, biết cách ứng xử và biết tìm sự giúp đỡ.



Nội dung bài học



1. Tác hại của nghiện Internet
2. Nhận biết thông tin không phù hợp
3. Ứng xử khi gặp nội dung xấu
4. Ứng xử khi bị bắt nạt trên mạng
5. Khi nào và cách nhờ người lớn giúp đỡ
6. Ví dụ truy cập không hợp lệ và biện pháp phòng tránh
7. Bảo mật thông tin cá nhân và thiết lập quyền riêng tư
8. Đánh giá nguồn thông tin và thái độ số an toàn

1. Tác hại của nghiện Internet



Dành quá nhiều thời gian cho mạng gây ảnh hưởng học tập và sức khỏe.

Hậu quả: mệt mỏi, giảm tập trung, ảnh hưởng giấc ngủ và quan hệ xã hội.

Dấu hiệu: bỏ bữa, lén dùng thiết bị, sa sút điểm số.

Ví dụ minh họa: em A chơi game đến khuya và vắng tiết học sáng hôm sau.



2. Nhận biết thông tin không phù hợp



Các loại nội dung không phù hợp: bạo lực, khiêu dâm, ngôn từ thù hận, thông tin độc hại.

Dấu hiệu nhận biết: ngôn từ kích động, hình ảnh gây sốc, yêu cầu chia sẻ thông tin cá nhân.

Tại sao phải tránh: có thể gây tổn thương tinh thần và pháp lý.

Ví dụ: đường link mời xem video 'độc' có nội dung người lớn.



3. Ứng xử khi gặp nội dung xấu



Ngừng tương tác ngay: không nhấp, không chia sẻ, không trả lời.

Ghi lại bằng chứng: chụp màn hình (nếu an toàn) và lưu ngay giờ.

Sử dụng tính năng báo cáo và chặn trên nền tảng.

Nếu cảm thấy bị đe dọa: thông báo cho người lớn hoặc giáo viên ngay lập tức.



4. Ứng xử khi bị bắt nạt trên mạng (cyberbullying)



Hành động có thể gặp: tin nhắn xúc phạm, bị lôi kéo vào nhóm bêu xấu, bị chia sẻ ảnh riêng tư.

Cách xử lý: giữ bình tĩnh, không trả đũa, lưu bằng chứng, chặn kẻ bắt nạt.

Tìm người lớn tin cậy: phụ huynh, giáo viên, cán bộ tư vấn.



5. Khi nào cần nhờ người lớn giúp đỡ



Nếu có đe dọa về thân thể, hình ảnh riêng tư bị phát tán, hoặc cảm thấy sợ hãi.

Khi sự việc lặp lại hoặc ảnh hưởng đến tâm lý, học tập. Người lớn có thể hỗ trợ thu thập bằng chứng và liên hệ nhà trường, công an.

Ví dụ: báo cho phụ huynh và giáo viên khi nhận được tin đe dọa.



6. Ví dụ truy cập không hợp lệ và biện pháp phòng tránh

Truy cập trang web lậu, tải phần mềm bẻ khoá hoặc mở đường link lạ.

Hậu quả: nhiễm mã độc, mất dữ liệu, đánh cắp thông tin cá nhân.

Ví dụ minh họa: một bạn tải phần mềm lậu và bị mất tài khoản học tập.

Cách phòng: chỉ tải từ nguồn tin cậy, không chia sẻ mật khẩu.



7. Bảo mật thông tin cá nhân và thiết lập quyền riêng tư

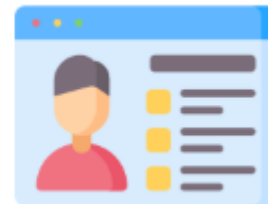


Không chia sẻ mật khẩu, địa chỉ, số điện thoại hoặc ảnh riêng tư với người lạ.

Sử dụng cài đặt quyền riêng tư trên mạng xã hội: giới hạn người nhìn thấy bài viết.

Sử dụng mật khẩu mạnh và không dùng cùng mật khẩu cho nhiều tài khoản.

Kiểm tra cài đặt quyền riêng tư ít nhất 6 tháng một lần.



8. Đánh giá nguồn thông tin và thái độ số an toàn



Kiểm tra nguồn: tin từ ai, có đáng tin không, có dấu hiệu giả mạo không.

Không chia sẻ thông tin chưa kiểm chứng hoặc gây hoang mang.

Thái độ số: tôn trọng, lịch sự, không lan truyền tin xấu.

Ví dụ: so sánh tin chính thống và tin giả trên mạng xã hội.



Tóm tắt bài học



Mạng mang lại lợi ích nhưng có rủi ro nếu không cẩn trọng.

Nhận biết nội dung xấu và hành vi bất nạt trên mạng.

Ứng xử: dừng, lưu bằng chứng, chặn, báo cáo và nhờ người lớn.

Bảo vệ thông tin cá nhân và kiểm tra nguồn tin trước khi chia sẻ.



?

