

Kỹ năng An toàn thông tin cá nhân và cách nhận diện

Trong thời đại số hóa, việc bảo vệ thông tin cá nhân và nhận diện các mối đe dọa an ninh mạng là kỹ năng thiết yếu. Chương này sẽ trang bị cho bạn kiến thức về phòng tránh lừa đảo, xâm hại và nhận diện các hình thức tấn công phổ biến trong môi trường giáo dục. Chúng ta sẽ khám phá các chiến lược hiệu quả để tạo ra một không gian học tập an toàn và lành mạnh cho tất cả mọi người.



by **Hoan Le**



Phòng tránh lừa đảo trong giáo dục

1

Email giả mạo

Cảnh giác với email yêu cầu cập nhật thông tin tài khoản hoặc đăng nhập hệ thống quản lý học sinh.

2

Cuộc gọi lừa đảo

Đề phòng cuộc gọi giả danh cơ quan chức năng yêu cầu chuyển tiền giải quyết vấn đề học vụ.

3

Hợp đồng giả mạo

Kiểm tra kỹ lưỡng các hợp đồng từ nhà tài trợ hay đối tác giáo dục để tránh bị lừa đảo tài chính.



Biện pháp bảo vệ thông tin

1

Tập huấn an ninh mạng

Tổ chức các buổi tập huấn về an ninh mạng cho giáo viên và cán bộ quản lý.

2

Chính sách bảo mật

Xây dựng chính sách bảo mật thông tin chi tiết và rõ ràng cho toàn trường.

3

Hệ thống phản hồi

Thiết lập hệ thống phản hồi và xử lý sự cố nhanh chóng khi phát hiện vấn đề.

Nhận biết email lừa đảo

Địa chỉ email đáng ngờ

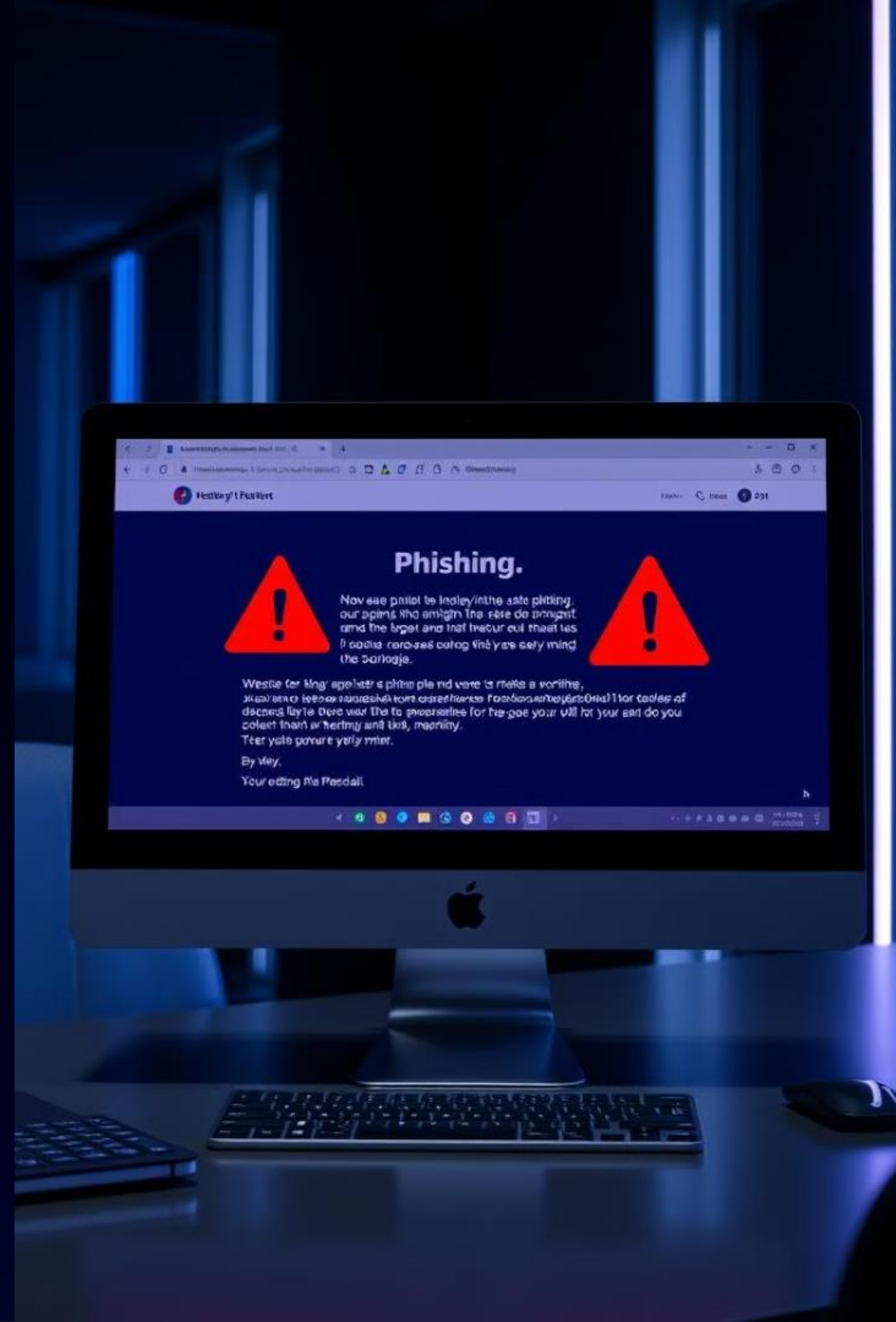
Kiểm tra kỹ địa chỉ email người gửi, tìm sự thay đổi nhỏ so với địa chỉ chính thức.

Ngôn ngữ không chính thức

Chú ý đến việc sử dụng ngôn ngữ không chuyên nghiệp hoặc có nhiều lỗi chính tả.

Yêu cầu khẩn cấp

Đề phòng các yêu cầu gấp gáp hoặc đe dọa không hợp lý về việc cung cấp thông tin.



Lừa đảo qua điện thoại và mạng xã hội



Vishing

Cảnh giác với cuộc gọi giả mạo yêu cầu thông tin đăng nhập hoặc thông tin cá nhân để "cập nhật hồ sơ".



Mạng xã hội

Đề phòng tài khoản giả mạo hoặc trang giả nhằm lừa đảo thông tin cá nhân hoặc phát tán phần mềm độc hại.



Xác minh danh tính

Luôn xác minh danh tính người liên hệ trước khi cung cấp bất kỳ thông tin nhạy cảm nào.

Giả mạo cơ hội đào tạo và học bổng

1

Nhận diện lời mời đáng ngờ

Cảnh giác với thông báo giả mạo về cơ hội đào tạo hoặc học bổng hấp dẫn nhưng thiếu thông tin chi tiết.

2

Kiểm tra yêu cầu thanh toán

Đề phòng yêu cầu nộp "phí đặt cọc" hoặc "phí quản lý" qua các phương thức không an toàn.

3

Xác minh nguồn gốc

Luôn xác minh tính xác thực của cơ hội thông qua các kênh chính thức của tổ chức giáo dục.



Dấu hiệu cảnh báo lừa đảo



Yêu cầu chuyển tiền

Cảnh giác với yêu cầu chuyển tiền hoặc cung cấp thông tin tài chính không mong đợi.



Liên hệ lạ

Đề phòng thông báo hoặc yêu cầu từ các tài khoản hoặc số điện thoại không quen thuộc.



Đổi mật khẩu

Kiểm tra kỹ các yêu cầu đổi mật khẩu đến từ các trang web không chính thức hoặc không an toàn.



Quà tặng đáng ngờ

Nghi ngờ các lời đề nghị về việc đầu tư tài chính hoặc nhận quà từ các nguồn không rõ ràng.



Thực hành tốt nhất để phòng chống lừa đảo

1

Đào tạo nhân viên

Tổ chức các buổi tập huấn về an ninh mạng để nâng cao nhận thức cho giáo viên và cán bộ quản lý.

2

Cập nhật bảo mật

Thực hiện các biện pháp bảo mật như cài đặt phần mềm chống virus và tường lửa, cập nhật thường xuyên.

3

Xác thực đa yếu tố

Sử dụng hệ thống xác thực đa yếu tố để bảo vệ các tài khoản trực tuyến quan trọng.

4

Quản lý mật khẩu

Khuyến khích việc sử dụng mật khẩu mạnh và thay đổi mật khẩu định kỳ cho tất cả tài khoản.



Phòng tránh quấy rối tinh thần

Nhận biết dấu hiệu

Chú ý đến thái độ không thích hợp, bình luận xúc phạm hoặc miệt thị trong môi trường học đường.

Giám sát trực tuyến

Theo dõi và xử lý các thông điệp hoặc hình ảnh không mong muốn gửi qua email hoặc mạng xã hội.

Hỗ trợ tâm lý

Cung cấp hỗ trợ tâm lý cho nạn nhân và tạo môi trường an toàn để báo cáo các vụ việc.

Đối phó với bắt nạt trực tuyến



Giáo dục

Giáo dục học sinh về cách sử dụng trách nhiệm các phương tiện truyền thông số và tác hại của bắt nạt trực tuyến. Điều này bao gồm việc dạy cho họ cách nhận biết các dấu hiệu của bắt nạt trực tuyến, cách báo cáo các trường hợp bắt nạt và cách bảo vệ bản thân khỏi bị bắt nạt.



Chính sách rõ ràng

Xây dựng và thực thi chính sách nghiêm ngặt về bắt nạt trực tuyến trong trường học. Chính sách này cần xác định rõ ràng các hành vi bị xem là bắt nạt trực tuyến, các hình thức kỷ luật đối với những học sinh có hành vi bắt nạt và các quyền lợi của nạn nhân.



Hỗ trợ nạn nhân

Phát triển các chương trình hỗ trợ tâm lý và can thiệp kịp thời cho nạn nhân của bắt nạt trực tuyến. Nạn nhân cần được hỗ trợ để xử lý cảm xúc, tìm kiếm sự giúp đỡ từ chuyên gia và xây dựng lại sự tự tin.

Bảo vệ thông tin cá nhân

1 Mật khẩu mạnh

Sử dụng mật khẩu phức tạp và duy nhất cho mỗi tài khoản, thay đổi định kỳ.

2 Hạn chế chia sẻ

Không chia sẻ thông tin qua các kênh không an toàn và hạn chế cung cấp thông tin cá nhân trực tuyến.

3 Cập nhật bảo mật

Thường xuyên cập nhật phần mềm và hệ điều hành để đảm bảo các lỗ hổng bảo mật được vá.

4 Giám sát truy cập

Kiểm soát quyền truy cập vào dữ liệu nhạy cảm và theo dõi các hoạt động đáng ngờ.



Chính sách và thủ tục an toàn thông tin

1

Xây dựng chính sách

Phát triển chính sách rõ ràng về việc sử dụng mạng nội bộ và internet trong trường học.

2

Đào tạo nhân viên

Tổ chức các buổi đào tạo định kỳ về an toàn thông tin cho tất cả nhân viên và giáo viên.

3

Quy trình ứng phó

Thiết lập quy trình ứng phó với các sự cố xâm hại và vi phạm an ninh mạng.

4

Đánh giá và cập nhật

Thường xuyên đánh giá và cập nhật chính sách để đối phó với các mối đe dọa mới.





Khuyến khích báo cáo sự cố

Hệ thống báo cáo ẩn danh

Thiết lập hệ thống cho phép học sinh và nhân viên báo cáo các hành vi đáng ngờ một cách ẩn danh.

Đảm bảo bảo mật

Cam kết bảo mật thông tin người báo cáo để tạo môi trường an toàn cho việc chia sẻ.

Phản hồi nhanh chóng

Xử lý và phản hồi các báo cáo một cách nhanh chóng và hiệu quả để xây dựng lòng tin.

Quản lý an toàn mạng xã hội

1

Cài đặt riêng tư

Hướng dẫn cách sử dụng cài đặt riêng tư trên các nền tảng mạng xã hội phổ biến.

2

Chia sẻ có trách nhiệm

Giáo dục về việc chia sẻ thông tin và hình ảnh một cách có trách nhiệm trên mạng xã hội.

3

Nhận diện rủi ro

Trang bị kỹ năng nhận diện các mối đe dọa và hành vi đáng ngờ trên mạng xã hội.

4

Xây dựng hình ảnh tích cực

Khuyến khích việc xây dựng hình ảnh trực tuyến tích cực và chuyên nghiệp.



Phân biệt thông tin chính xác và sai lệch



Kiểm tra nguồn

Hướng dẫn học sinh và nhân viên cách xác minh độ tin cậy của nguồn thông tin. Cần kiểm tra xem nguồn thông tin có uy tín, độc lập và khách quan hay không. Học sinh cũng nên chú ý đến ngày đăng tải và xem xét liệu thông tin có được cập nhật thường xuyên hay không.



Đối chiếu thông tin

Khuyến khích học sinh và nhân viên so sánh thông tin từ nhiều nguồn khác nhau. Việc đối chiếu thông tin từ nhiều nguồn tin đáng tin cậy giúp học sinh và nhân viên có cái nhìn tổng quan hơn và xác định được tính chính xác của thông tin.



Tư duy phản biện

Phát triển kỹ năng tư duy phản biện cho học sinh và nhân viên để đánh giá thông tin một cách khách quan và toàn diện. Học sinh cần đặt câu hỏi về mục đích của thông tin, xem xét liệu có bất kỳ sai sót hoặc thiên vị nào trong thông tin hay không, và suy nghĩ về những ảnh hưởng tiềm ẩn của thông tin đó.