



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

Kỹ năng an toàn thông tin cá nhân và cách nhận diện trong môi trường mạng là một khía cạnh quan trọng đối với giáo viên và cán bộ quản lý trong các cơ sở giáo dục. Trong thế giới ngày nay, mạng internet trở thành một phần không thể thiếu trong cuộc sống và công việc, nhưng cũng đi kèm với các rủi ro và nguy cơ về an toàn thông tin cá nhân. Chương này sẽ tìm hiểu các khía cạnh quan trọng về kỹ năng an toàn thông tin cá nhân và cách nhận diện, đặc biệt dành cho giáo viên và cán bộ quản lý trong lĩnh vực giáo dục.



by Hoan Le

Hiểu biết về các rủi ro trực tuyến



1

Xâm nhập mạng

Kẻ tấn công có thể xâm nhập vào hệ thống mạng của trường học, gây mất dữ liệu hoặc đe dọa an ninh thông tin.

2

Lừa đảo trực tuyến

Các chiêu trò lừa đảo như giả mạo email để đánh cắp thông tin đăng nhập hoặc tài chính.

3

Quấy rối mạng

Hành vi quấy rối, bắt nạt trực tuyến có thể gây tổn hại tinh thần cho học sinh và giáo viên.

4

Virus máy tính

Phần mềm độc hại có thể lây nhiễm và phá hoại hệ thống máy tính của trường học.



Bảo vệ thông tin cá nhân

Tạo mật khẩu mạnh

Sử dụng mật khẩu dài, phức tạp và độc đáo cho từng tài khoản.

Không chia sẻ mật khẩu

Tuyệt đối không chia sẻ mật khẩu với người khác, kể cả đồng nghiệp.

Xác thực hai yếu tố

Bật tính năng xác thực hai yếu tố khi có thể để tăng cường bảo mật.

Hạn chế chia sẻ thông tin

Cẩn trọng khi chia sẻ thông tin cá nhân trên mạng xã hội và các trang web.



Phát triển ý thức an toàn trực tuyến

1

Đọc và kiểm tra thông tin

Phát triển thói quen đọc kỹ và xác minh thông tin trước khi tin tưởng hoặc chia sẻ.

2

Đánh giá nguồn thông tin

Học cách đánh giá độ tin cậy của các nguồn thông tin trực tuyến.

3

Nhận biết tin giả

Rèn luyện khả năng phân biệt tin tức thật và tin tức giả mạo.

4

Cảnh giác với các mối đe dọa

Luôn duy trì sự cảnh giác với các mối đe dọa an ninh mạng tiềm ẩn.

Giảng dạy về an toàn trực tuyến cho học sinh



Bảo vệ thông tin cá nhân

Hướng dẫn học sinh cách bảo vệ thông tin cá nhân trên mạng, bao gồm việc sử dụng mật khẩu mạnh và hạn chế chia sẻ thông tin nhạy cảm.



Nhận diện mối nguy hiểm

Dạy học sinh cách nhận biết các mối nguy hiểm trực tuyến như lừa đảo, quấy rối và nội dung không phù hợp.



Ứng phó với tình huống

Cung cấp hướng dẫn cụ thể về cách ứng phó khi gặp các tình huống nguy hiểm trực tuyến, bao gồm việc báo cáo và tìm kiếm sự giúp đỡ.

Sử dụng phần mềm an toàn và công cụ kiểm tra



Phần mềm diệt virus

Cài đặt và cập nhật thường xuyên phần mềm diệt virus để bảo vệ máy tính khỏi mã độc.



Tường lửa

Sử dụng tường lửa để kiểm soát lưu lượng mạng và ngăn chặn truy cập trái phép.



Công cụ kiểm tra danh tính

Sử dụng các công cụ kiểm tra danh tính trực tuyến để xác minh tính xác thực của người dùng và trang web.



Cập nhật phần mềm

Thường xuyên cập nhật hệ điều hành và các ứng dụng để vá lỗ hổng bảo mật.



Phản ứng trước các tình huống nguy hiểm

1

Nhận diện mối đe dọa

Học cách nhận biết các dấu hiệu của tấn công mạng hoặc vi phạm bảo mật.

2

Hành động nhanh chóng

Thực hiện các bước cần thiết để ngăn chặn hoặc hạn chế thiệt hại, như thay đổi mật khẩu hoặc ngắt kết nối mạng.

3

Báo cáo sự cố

Thông báo cho người có trách nhiệm trong tổ chức và các cơ quan chức năng nếu cần thiết.

4

Tìm kiếm hỗ trợ

Liên hệ với chuyên gia IT hoặc bộ phận hỗ trợ kỹ thuật để được giúp đỡ.



Cập nhật kiến thức về an toàn thông tin

1

Tham gia khóa đào tạo

Tham gia các khóa học và hội thảo về an toàn thông tin để nâng cao kiến thức.

2

Theo dõi tin tức

Cập nhật thường xuyên về các mối đe dọa mới và phương pháp bảo mật mới nhất.

3

Chia sẻ kiến thức

Trao đổi thông tin và kinh nghiệm với đồng nghiệp để cùng nâng cao nhận thức.

4

Thực hành liên tục

Áp dụng kiến thức mới vào thực tế để duy trì và cải thiện kỹ năng an toàn thông tin.





Xây dựng chính sách an toàn thông tin

Đề xuất biện pháp

Tham gia vào quá trình đề xuất các biện pháp bảo mật phù hợp với môi trường giáo dục, bao gồm các chính sách về mật khẩu, quyền truy cập, sử dụng Wi-Fi, bảo mật thiết bị di động, và các biện pháp phòng chống tấn công mạng.

Quy định sử dụng internet

Xây dựng quy định rõ ràng về việc sử dụng internet và thiết bị trực tuyến trong trường học, bao gồm các quy định về truy cập mạng xã hội, sử dụng email, tải xuống tài liệu, và việc chia sẻ thông tin cá nhân.

Hướng dẫn an toàn

Cung cấp hướng dẫn chi tiết về an toàn thông tin cho nhân viên và học sinh, bao gồm cách nhận diện các mối đe dọa trực tuyến, xử lý email đáng ngờ, bảo vệ danh tiếng trực tuyến, và các biện pháp bảo mật thông tin cá nhân.

Cập nhật chính sách

Thường xuyên rà soát và cập nhật chính sách để đáp ứng với các thách thức mới, bao gồm các công nghệ mới, các loại hình tấn công mới, và các thay đổi trong luật pháp liên quan đến bảo mật thông tin.

Quản lý mật khẩu và quyền truy cập

1

Tạo mật khẩu mạnh

Sử dụng mật khẩu dài, phức tạp và độc đáo cho từng tài khoản.

2

Sử dụng trình quản lý mật khẩu

Áp dụng công cụ quản lý mật khẩu để lưu trữ và tạo mật khẩu an toàn.

3

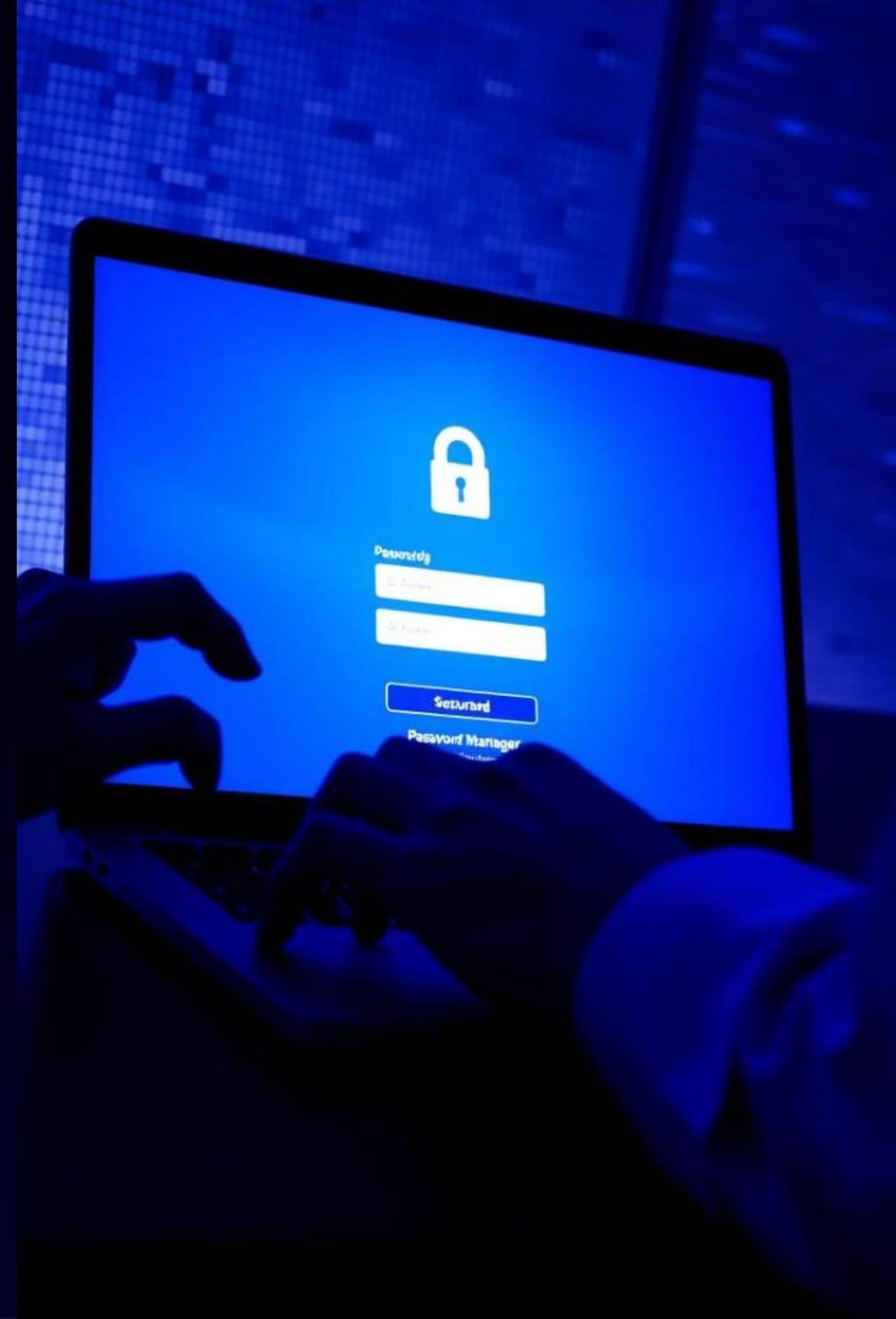
Xác thực đa yếu tố

Bật tính năng xác thực đa yếu tố cho các tài khoản quan trọng.

4

Phân quyền truy cập

Thiết lập và quản lý quyền truy cập dựa trên vai trò và trách nhiệm của từng người dùng.



Bảo vệ dữ liệu học sinh



Mã hóa dữ liệu

Sử dụng các phương pháp mã hóa để bảo vệ thông tin cá nhân và học tập của học sinh.



Quyền truy cập hạn chế

Giới hạn quyền truy cập vào dữ liệu học sinh chỉ cho những người có thẩm quyền.



Sao lưu dữ liệu

Thực hiện sao lưu dữ liệu định kỳ để phòng tránh mất mát thông tin quan trọng.

An toàn khi sử dụng Wi-Fi công cộng



1

Sử dụng VPN

Kết nối thông qua mạng riêng ảo (VPN) khi sử dụng Wi-Fi công cộng để mã hóa dữ liệu.

2

Tránh giao dịch nhạy cảm

Không thực hiện các giao dịch tài chính hoặc truy cập thông tin nhạy cảm trên mạng Wi-Fi công cộng.

3

Tắt chia sẻ file

Vô hiệu hóa tính năng chia sẻ file trên thiết bị khi kết nối với mạng công cộng.

4

Xác minh mạng

Đảm bảo kết nối với mạng Wi-Fi chính thức, tránh các mạng giả mạo.





Bảo mật thiết bị di động



Khóa màn hình

Sử dụng mã PIN, mật khẩu hoặc sinh trắc học để bảo vệ thiết bị.



Cập nhật phần mềm

Luôn cập nhật hệ điều hành và ứng dụng lên phiên bản mới nhất.



Cài đặt ứng dụng an toàn

Chỉ tải ứng dụng từ các nguồn chính thức và đáng tin cậy.



Theo dõi từ xa

Bật tính năng định vị và xóa dữ liệu từ xa để bảo vệ thông tin khi thiết bị bị mất.

Xử lý email đáng ngờ

1

Kiểm tra người gửi

Xác minh địa chỉ email của người gửi để đảm bảo tính xác thực.

2

Cẩn trọng với tệp đính kèm

Không mở tệp đính kèm từ nguồn không xác định hoặc đáng ngờ.

3

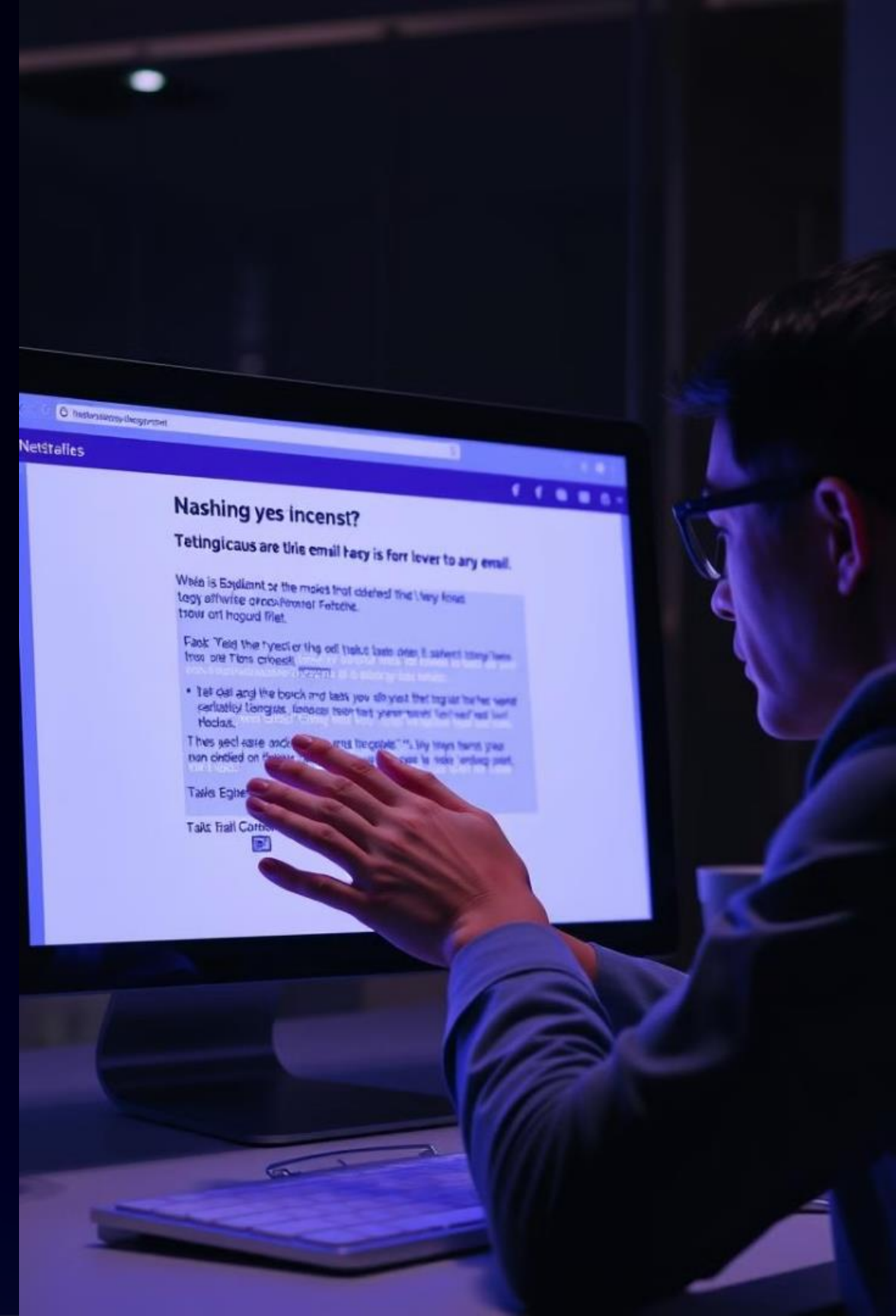
Xác minh liên kết

Kiểm tra URL của các liên kết trước khi nhấp vào bằng cách di chuột qua chúng.

4

Báo cáo email đáng ngờ

Thông báo cho bộ phận IT hoặc quản trị hệ thống về các email có dấu hiệu lừa đảo.



Bảo vệ danh tiếng trực tuyến



Kiểm soát nội dung chia sẻ

Cẩn trọng với thông tin và hình ảnh được đăng tải trên mạng xã hội và các nền tảng trực tuyến.



Thiết lập quyền riêng tư

Điều chỉnh cài đặt quyền riêng tư trên các tài khoản mạng xã hội để kiểm soát người có thể xem thông tin của bạn.



Theo dõi dấu chân số

Thường xuyên tìm kiếm tên của bạn trên internet để kiểm tra thông tin xuất hiện về bạn.



Xây dựng hình ảnh chuyên nghiệp

Tạo và duy trì một hình ảnh trực tuyến tích cực và chuyên nghiệp, phù hợp với vai trò giáo dục của bạn.