SỔ TAY HỌC TẬP

TÀI CHÍNH SỐ AN TOÀN

Sáu chủ đề giúp học sinh THPT nhận diện và ứng phó trước nguy cơ lừa đảo tài chính trực tuyến



Học liệu minh họa · Không yêu cầu tiền thật, mã OTP hoặc dữ liệu cá nhân

Năm 2026

Đọc sổ tay này như thế nào?

Mỗi chủ đề trình bày một tình huống gần gũi, ba điều cần nhớ và một câu hỏi tự kiểm tra. Khi gặp yêu cầu đáng ngờ, hãy ưu tiên dừng lại, tự kiểm chứng qua kênh chính thức và nhờ người đáng tin cậy hỗ trợ. Đây là tài liệu học tập, không có chức năng đánh giá hay xác nhận một giao dịch thật.

Mục lục

01. Lời mời kiếm tiền nhanh

02. Lợi nhuận bất thường

03. Đường dẫn và người gửi

04. Bảo vệ tài khoản

05. Hình ảnh và giọng nói giả mạo

06. Ứng phó và tìm trợ giúp

Quy trình Trạm SOS trong năm bước

1. Dừng giao dịch, không cung cấp thêm thông tin.
2. Kiểm chứng bằng kênh chính thức.
3. Lưu bằng chứng cần thiết và giữ kín dữ liệu riêng.
4. Báo người lớn, nhà trường hoặc đơn vị phù hợp.
5. Bảo vệ tài khoản theo hướng dẫn chính thức.

CHỦ ĐỀ 01 / 06

Lời mời kiếm tiền nhanh

Khi công việc bắt đầu bằng một khoản phí

Các tin tuyển cộng tác viên trực tuyến thường nhấn mạnh thời gian linh hoạt, thu nhập hấp dẫn và thủ tục đơn giản. Những chi tiết đó không đủ để đánh giá một công việc là thật hay giả. Dấu hiệu cần chú ý là yêu cầu chuyển tiền trước để kích hoạt nhiệm vụ, giữ chỗ, mở khóa đơn hàng hoặc được trả lương. Không nên gửi ảnh giấy tờ, số tài khoản hay mã xác thực cho tài khoản chưa được xác minh.

Hãy thử dừng lại để tìm địa chỉ tuyển dụng chính thức, xem thông tin pháp lý và hỏi người lớn đáng tin cậy. Nếu lời mời liên tục thúc giục phải chuyển tiền ngay, đó là lý do để tăng mức cảnh giác. Một công việc minh bạch phải cho phép người tìm việc đọc kỹ điều kiện và kiểm tra độc lập trước khi quyết định.

Ba điều cần nhớ

- Không nạp phí để được nhận việc hoặc làm nhiệm vụ.
- Xác minh đơn vị tuyển dụng qua kênh độc lập.
- Giữ kín giấy tờ và mã bảo vệ tài khoản.

TỰ KIỂM TRA

Vì sao yêu cầu nạp phí để nhận việc cần được kiểm chứng?

Gợi ý: Vì đây có thể là cách dẫn dụ chuyển tiền trước khi có công việc thực sự.

CHỦ ĐỀ 02 / 06

Lợi nhuận bất thường

Nhận ra lời hứa không tương xứng rủi ro

Một lời mời tài chính có thể sử dụng con số phần trăm rất cao, hình ảnh người nhận tiền hoặc nhận xét tích cực để tạo niềm tin. Tuy nhiên, lời cam kết “lợi nhuận chắc chắn” và “không có rủi ro” không phải bằng chứng đáng tin. Với học sinh, mục tiêu của bài học không phải thử đầu tư để kiểm tra, mà là biết phát hiện biểu hiện bất thường và tìm nguồn thông tin chính thức.

Khi thấy bạn bè định tham gia chương trình trên một trang lạ, hãy khuyên bạn không nạp tiền thử, không mời thêm người và không chia sẻ dữ liệu đăng nhập. Các bình luận trên mạng có thể được tạo hoặc sắp đặt. Cách xử lý có trách nhiệm là đọc kỹ nội dung, xác minh tổ chức qua kênh độc lập và tìm hỗ trợ từ người có chuyên môn.

Ba điều cần nhớ

- Lãi cao chắc chắn là dấu hiệu cần thận trọng.
- Không dùng tiền thật để thử một trang đáng ngờ.
- Không rủ bạn bè tham gia khi chưa rõ nguồn.

TỰ KIỂM TRA

Bạn nên nói gì khi một trang hứa lãi 20% mỗi tuần?

Gợi ý: Khuyên bạn tạm dừng và kiểm chứng tổ chức, không nạp tiền.

CHỦ ĐỀ 03 / 06

Đường dẫn và người gửi

Đừng quyết định chỉ vì logo quen

Đường dẫn giả mạo có thể gần giống địa chỉ một ngân hàng, ví điện tử hoặc sàn mua sắm. Logo đẹp và cách viết lịch sự không chứng minh người gửi là đại diện thật. Tin nhắn “tài khoản sẽ bị khóa trong năm phút” thường kết hợp yếu tố khẩn cấp để người nhận bỏ qua bước kiểm tra.

Khi cần xác minh, bạn nên tự mở ứng dụng chính thức đã cài đặt hoặc tự gõ địa chỉ website đã được biết trước. Không dùng số điện thoại hoặc đường dẫn nằm ngay trong thông điệp đáng ngờ làm nguồn xác thực duy nhất. Trường hợp có thể bị giả danh người quen, hãy liên lạc lại qua một kênh khác đã biết và chưa bị ảnh hưởng.

Ba điều cần nhớ

- Tự tìm kênh chính thức thay vì bấm đường dẫn lạ.
- Kiểm tra cả tên miền, không chỉ logo.
- Liên hệ người quen qua kênh thứ hai.

TỰ KIỂM TRA

Thấy logo ngân hàng trên tin nhắn có đủ để tin không?

Gợi ý: Không. Logo có thể bị sao chép, cần tự xác minh kênh chính thức.

CHỦ ĐỀ 04 / 06

Bảo vệ tài khoản

Mã xác thực là thông tin phải giữ kín

Mã OTP, mật khẩu và mã khôi phục có vai trò bảo vệ quyền truy cập. Người tự xưng hỗ trợ kỹ thuật hoặc nhân viên ngân hàng cũng không phải lý do để bạn đọc mã OTP cho họ. Một yêu cầu “gửi mã để tránh khóa tài khoản” đặc biệt đáng ngờ vì tạo áp lực đồng thời muốn lấy thông tin bảo vệ.

Nếu lỡ tiết lộ thông tin hoặc phát hiện hoạt động bất thường, hãy ngừng làm theo hướng dẫn của người lạ. Chủ động liên hệ nhà cung cấp dịch vụ hoặc ngân hàng qua kênh chính thức, đổi mật khẩu khi được hướng dẫn và báo người lớn đáng tin cậy. Đừng đăng ảnh chụp mã xác thực hay thông tin tài khoản vào nhóm công khai để nhờ giúp.

Ba điều cần nhớ

- Không tiết lộ OTP cho bất kỳ người tự nhận hỗ trợ.
- Không dùng liên kết lạ để đăng nhập.
- Tìm hỗ trợ chính thức ngay khi nghi bị chiếm tài khoản.

TỰ KIỂM TRA

Nếu đã gửi OTP cho người lạ, cần làm gì?

Gợi ý: Liên hệ ngay kênh hỗ trợ chính thức để bảo vệ tài khoản và báo người đáng tin.

CHỦ ĐỀ 05 / 06

Hình ảnh và giọng nói giả mạo

Thấy người quen trên màn hình chưa chắc là xác minh

Một tin nhắn có thể mang tên bạn thân, ảnh đại diện quen thuộc hoặc thậm chí đoạn video và giọng nói giống người thân. Công nghệ có thể tạo hoặc chỉnh sửa nội dung số khiến người xem nhầm lẫn. Vì thế, dấu hiệu quan trọng không chỉ nằm ở hình ảnh mà còn ở hành vi: người gửi yêu cầu chuyển tiền gấp, từ chối gọi lại hoặc né bước xác minh.

Khi nhận yêu cầu tiền bạc bất thường, hãy tạm dừng, gọi đến số liên hệ bạn đã biết từ trước hoặc hỏi trực tiếp khi có thể. Đừng cung cấp thêm dữ liệu cá nhân để "chứng minh" mình là người quen. Nếu không xác minh được, không thực hiện giao dịch và báo người có trách nhiệm hỗ trợ.

Ba điều cần nhớ

- Ảnh và giọng nói đều có thể bị giả mạo.
- Yêu cầu gấp không phải lý do bỏ qua xác minh.
- Liên hệ qua kênh đã biết độc lập.

TỰ KIỂM TRA

Gọi video giống người thân có đủ để chuyển tiền ngay không?

Gợi ý: Không. Cần xác minh độc lập qua kênh liên hệ đã biết.

CHỦ ĐỀ 06 / 06

Ứng phó và tìm trợ giúp

Quy trình Trạm SOS năm bước

Khi nghi gặp lừa đảo, việc quan trọng nhất là hạn chế thiệt hại và tìm đúng người hỗ trợ. Trước hết, dừng chuyển tiền hoặc gửi thêm thông tin. Thứ hai, kiểm chứng qua ứng dụng hoặc kênh chính thức. Thứ ba, giữ lại tin nhắn, thời gian và nội dung cần thiết ở nơi riêng tư. Thứ tư, báo người lớn, nhà trường, ngân hàng hoặc cơ quan có thẩm quyền phù hợp. Thứ năm, bảo vệ tài khoản theo hướng dẫn chính thức.

Bạn không cần tự đối chất với người nghi lừa đảo. Không công khai mã OTP, số tài khoản hoặc dữ liệu người khác để tìm giúp đỡ trên mạng. Nếu đã có chuyển tiền hoặc mất quyền truy cập, hãy nhanh chóng liên hệ đơn vị cung cấp dịch vụ hoặc tổ chức tài chính bằng kênh do chính bạn tìm kiếm. Các bài luyện trong website là tình huống giả định, không yêu cầu giao dịch thật.

Ba điều cần nhớ

- Dừng lại để tránh phát sinh thiệt hại.
- Giữ bằng chứng cần thiết mà không phát tán công khai.
- Báo người đáng tin và bảo vệ tài khoản qua kênh chính thức.

TỰ KIỂM TRA

Nêu ba hành động đầu tiên khi nghi gặp lừa đảo?

Gợi ý: Dừng giao dịch, tự kiểm chứng kênh chính thức, lưu bằng chứng cần thiết.

Tài liệu tham khảo

[1] Cục An toàn thông tin (2023). Cẩm nang nhận diện và phòng chống lừa đảo trực tuyến.

[2] Bộ Công an, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; Google (2025). Cẩm nang Chung tay phòng, chống lừa đảo online.

[3] Bộ Giáo dục và Đào tạo (2025). Thông tư 02/2025/TT-BGDĐT về Khung năng lực số cho người học.

[4] European Union/OECD (2023). Financial competence framework for children and youth in the European Union.

[5] OECD (2024). PISA 2022 Results (Volume IV): How Financially Smart Are Students?

Sổ tay được biên soạn để hỗ trợ học sinh thực hành và ôn tập theo bốn giải pháp của đề tài. Các tình huống đều mang tính giả định.