



BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG
TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

Google

Cẩm nang

Chung tay phòng, chống



Mục lục

01

Toàn cảnh tình hình lừa đảo trực tuyến tại Việt Nam.

Các hình thức lừa đảo trực tuyến phổ biến và biện pháp phòng, chống.

02

03

An toàn hơn khỏi lừa đảo trực tuyến cùng các giải pháp từ Google.

Bắt bài lừa đảo online

04

05

Lời kết

Giới thiệu

Internet từ lâu đã trở thành một phần không thể thiếu trong đời sống hàng ngày, từ công việc, học tập đến giải trí và giao tiếp. Tuy nhiên, song hành với những tiện ích vượt trội là sự gia tăng nhanh chóng của các thủ đoạn lừa đảo trên không gian mạng.

Đặc biệt, chúng ngày càng tinh vi và khó nhận diện hơn, gây thiệt hại nghiêm trọng về cả tài sản lẫn tinh thần của người dân. Theo báo cáo, có đến **70% người Việt Nam cho biết họ đã từng tiếp nhận ít nhất một cuộc gọi hoặc tin nhắn lừa đảo mỗi tháng(*)**: một con số đáng báo động, cho thấy mức độ phổ biến và nguy hiểm của loại tội phạm này.

Cẩm nang “Chung tay phòng, chống lừa đảo Online” là một tài liệu phối hợp giữa **Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công An** và **Google**, nhằm trang bị cho người dân những kiến thức và kỹ năng cần thiết để nhận diện, phòng tránh, và phản ứng đúng trước các hình thức lừa đảo trực tuyến phổ biến hiện nay.

Cuốn cẩm nang được phát hành trong khuôn khổ chiến dịch truyền thông cộng đồng “**Lừa đảo Online - Chung tay phòng, chống!**” và được sử dụng trong các hoạt động truyền thông, tập huấn và tuyên truyền tại địa phương - góp phần nâng cao nhận thức và tạo dựng một môi trường mạng an toàn, lành mạnh và văn minh cho tất cả mọi người thuộc mọi lứa tuổi.

(*) Nguồn: Global Anti-Scam Alliance, 2023



99+



01



**Toàn cảnh tình hình
lừa đảo trực tuyến
tại Việt Nam**

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của công nghệ thông tin và thanh toán điện tử, Việt Nam đã chứng kiến sự bùng nổ trong hoạt động giao dịch trực tuyến, kết nối số và sử dụng các nền tảng mạng xã hội.



Tính đến 5/2025, dân số Việt Nam là hơn 101 triệu người. Trong đó, có hơn **78,4 triệu người sử dụng Internet chiếm khoảng 80% dân số**; hơn **72 triệu người sử dụng mạng xã hội**; tổng cộng gần **170 triệu kết nối di động tại Việt Nam, tương đương khoảng 170% dân số**.

Tuy nhiên, chính sự phổ biến này cũng tạo điều kiện để các đối tượng xấu lợi dụng, triển khai hàng loạt phương thức lừa đảo với thủ đoạn ngày càng tinh vi, có tổ chức và mang tính xuyên quốc gia.

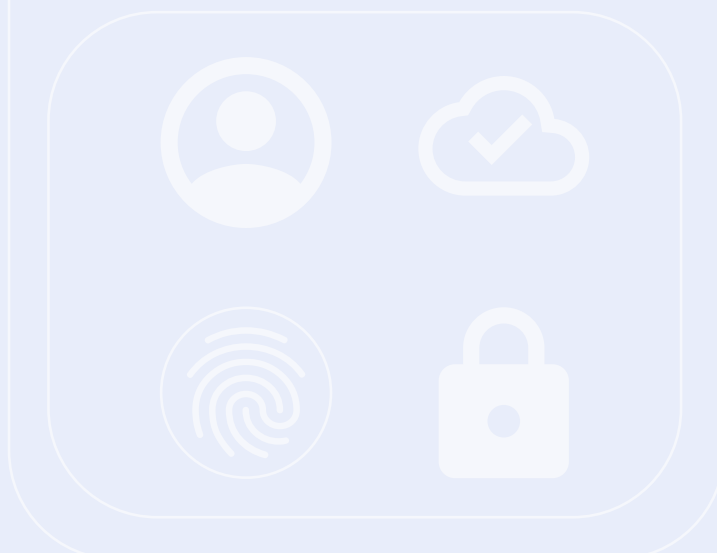
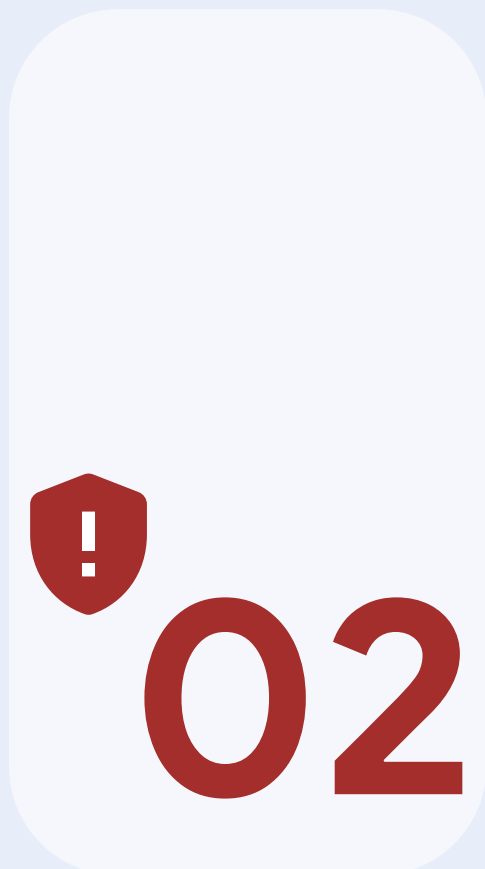
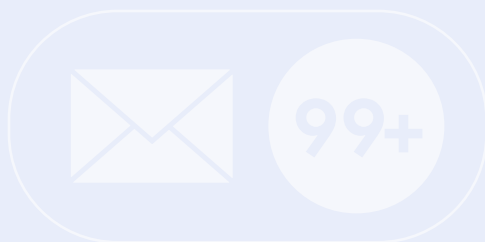
Theo thống kê, trong năm 2024, các cơ quan chức năng đã phát hiện hơn **6.000 vụ việc liên quan đến lừa đảo công nghệ cao, với tổng số thiệt hại lên đến hơn 12.000 tỷ đồng**. Riêng từ giữa tháng 2 đến cuối tháng 5/2025, hàng trăm vụ việc được tiếp nhận và điều tra, gây thiệt hại gần 1.000 tỷ đồng. Đáng chú ý, theo thống kê trên cổng Cảnh báo an toàn thông tin (Bộ Thông tin và Truyền thông), chỉ trong vòng 4 tuần từ 14/10 đến 10/11/2024, đã có gần 18.000 lượt phản ánh của người dân về các hành vi lừa đảo trực tuyến.



✉ *****

Thực trạng này cho thấy loại hình tội phạm lừa đảo qua mạng đang không ngừng gia tăng cả về quy mô và mức độ tinh vi. Nhiều đối tượng hoạt động theo mô hình “làng nghề” hoặc “tập đoàn lừa đảo”, chủ yếu điều hành từ nước ngoài như Campuchia, Lào, Philippines... đặc biệt tập trung tại các “đặc khu kinh tế” với thời hạn thuê đất lên tới 99 năm - gây không ít khó khăn cho công tác điều tra, truy bắt và xử lý hình sự.

Trước thực trạng phức tạp và nguy hiểm này, việc nâng cao nhận thức, tăng cường kỹ năng tự bảo vệ khi tham gia không gian mạng là vô cùng cấp thiết. Mỗi người dân cần chủ động tiếp cận các nguồn thông tin chính thống, cảnh trọng trong từng thao tác trực tuyến và luôn cảnh giác với các dấu hiệu bất thường – góp phần xây dựng một môi trường số an toàn, lành mạnh và văn minh.



**Các hình thức lừa đảo
trực tuyến phổ biến và
biện pháp phòng, chống**

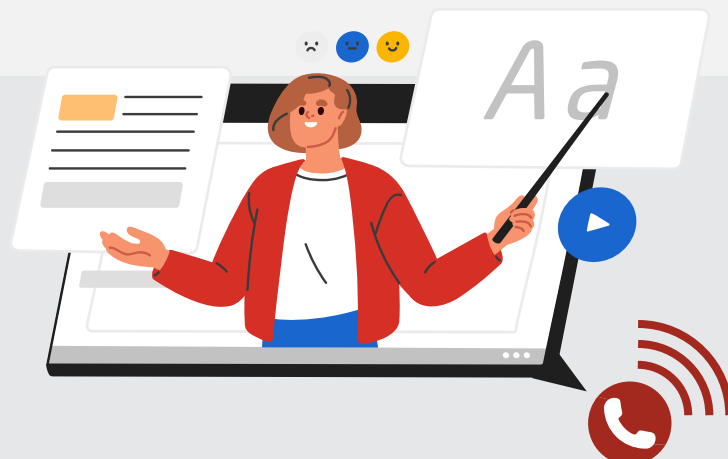


Lừa đảo mạo danh cơ sở giáo dục

Phương thức, thủ đoạn

Giả danh nhân viên cơ sở giáo dục gọi điện cho sinh viên hoặc phụ huynh, thông báo về việc đủ điều kiện nhận học bổng du học nước ngoài, hoàn tiền học phí hoặc khi phụ huynh liên hệ đăng ký cho con tham gia Trại hè thuộc các trường Công an, Quân đội.

Chúng yêu cầu nạn nhân khi muốn cho con tham gia trại hè thì phải thực hiện “nhiệm vụ online” hoặc khi đăng ký học bổng, hoàn tiền học phí thì phải có bằng chứng để chứng minh tài chính hoặc đặt cọc ngay lập tức để “đảm bảo” học bổng, ép buộc nạn nhân chuyển tiền gấp hoặc nhấp vào các liên kết độc hại để đánh cắp thông tin chi tiết ngân hàng và mã xác thực một lần (OTP).





Lừa đảo mạo danh cơ sở giáo dục

Kịch bản dẫn dắt

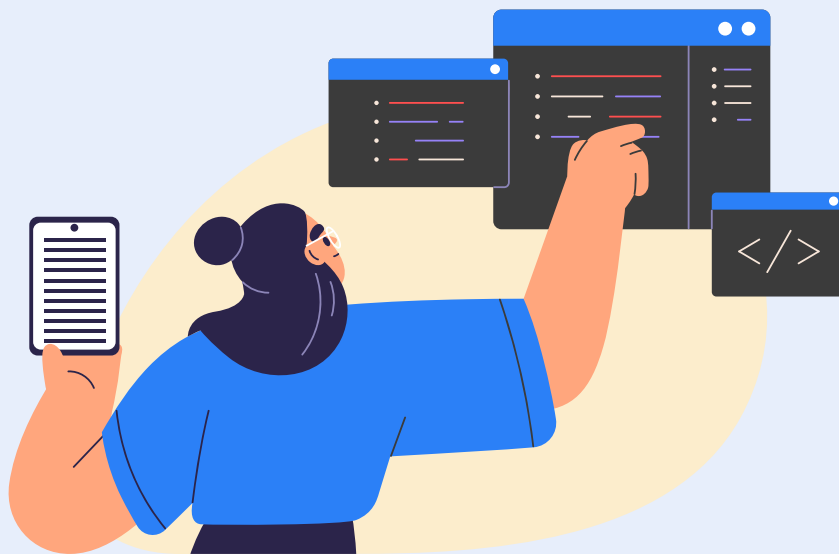
- 1. Giảng bầy bằng giấy tờ “rất thật”:** Kẻ gian tạo thông báo học bổng với logo, con dấu giống trường thật để tạo sự tin tưởng.
- 2. Tiếp cận nạn nhân qua email, tin nhắn, điện thoại:** Giả làm nhân viên trường, liên hệ với phụ huynh hoặc sinh viên, nói rằng “đã đủ điều kiện nhận học bổng”.
- 3. Tạo áp lực thời gian:** Yêu cầu nộp giấy tờ chứng minh tài chính hoặc chuyển cọc gấp để không “mất suất”.
- 4. Chuyển hướng sang liên kết độc hại:** Gửi đường liên kết giả, dụ nạn nhân điền thông tin ngân hàng và mã OTP để đánh cắp thông tin.
- 5. Ngụy trang bằng trang web và trang mạng xã hội giả:** Tất cả tương tác đều diễn ra qua các kênh trông có vẻ rất uy tín, hợp pháp nhưng thực chất là giả mạo.



Lừa đảo mạo danh cơ sở giáo dục

Cách phòng, chống

- ° Xác minh tất cả các đề nghị học bổng trực tiếp với các kênh chính thức của trường.
- ° Cảnh giác với các yêu cầu thanh toán gấp hoặc chứng minh tiền gửi được gửi qua các kênh không chính thức.
- ° Không nhấp vào bất kỳ đường liên kết nào để cung cấp thông tin cá nhân hoặc tài chính cho các liên hệ chưa được xác minh.
- ° Báo cáo bất kỳ hoạt động đáng ngờ nào cho trường và cơ quan thực thi pháp luật.





Lừa đảo thu hồi vốn treo!

Phương thức, thủ đoạn

Giả danh các cán bộ thuộc lực lượng công an, hội luật sư cam kết sẽ thu hồi lại tiền của người dân đã bị lừa đảo qua mạng.

Chúng tạo các tài khoản, trang web, ứng dụng và tài liệu giả mạo để lấy lòng tin. Sau đó lấy nhiều lý do để yêu cầu người dân chuyển khoản với số tiền lớn nhằm thực hiện hành vi chiếm đoạt tài sản.

Kịch bản dẫn dắt

- 1. Dựng vở bọc chuyên nghiệp:** Lập các trang mạng xã hội, trang web, tài khoản mạng xã hội mạo danh cơ quan Công an, công ty luật, văn phòng luật sư... đăng bài quảng cáo "tiếp nhận hồ sơ", "thu hồi tiền treo", "lấy lại tiền bị lừa" với cam kết uy tín chỉ thu phí khi xử lý thành công.
- 2. Khai thác tâm lý tiếc tiền:** Nhắm đến người từng là nạn nhân lừa đảo, lợi dụng mong muốn lấy lại tiền để tiếp tục lừa đảo lần hai.



Lừa đảo thu hồi vốn treo!

Kịch bản dẫn dắt

3. Tăng độ tin tưởng qua hình ảnh và truyền thông giả: Sử dụng ảnh, video, phát biểu cắt ghép từ cán bộ, luật sư hoặc đơn vị có thật để tạo lòng tin. Chạy quảng cáo và tạo bình luận ảo để nội dung hiện liên tục trên mạng xã hội.

4. Dụ người dân chủ động liên hệ: Khi người dân nhắn tin hoặc gọi, kẻ gian yêu cầu cung cấp thông tin cá nhân, vụ việc, rồi hướng dẫn cài ứng dụng nhắn tin để tiện liên lạc.

5. Giăng bẫy nhiều lớp: Gửi tài liệu giả (đã được “xử lý hồ sơ”), sau đó viện cớ thiếu giấy tờ, lỗi hệ thống... để tiếp tục yêu cầu chuyển thêm tiền, chiếm đoạt tài sản.



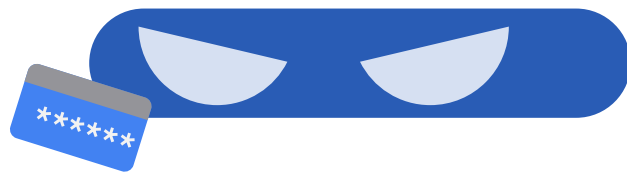


Lừa đảo thu hồi vốn treo

Cách phòng, chống

- ° Hiện nay, Bộ Công an và các đơn vị liên quan không phối hợp, ủy quyền cho bất cứ đơn vị nào để hướng dẫn, nhận hồ sơ của người dân về các vụ việc lừa đảo, chiếm đoạt tài sản qua các mạng xã hội. Khi có vụ việc liên quan đến lừa đảo chiếm đoạt tài sản qua mạng, người dân cần trực tiếp đến các cơ quan Công an để trình báo.
- ° Tuyệt đối không nghe theo, không liên hệ với các trang web, trang mạng xã hội, tài khoản mạng xã hội quảng cáo dịch vụ "tiếp nhận hồ sơ", "hỗ trợ lấy lại tiền bị treo", "thu hồi tiền lừa đảo"... trên không gian mạng
- ° Không chuyển tiền cho các đối tượng trên để được hướng dẫn, hoàn thiện hồ sơ thu hồi vốn treo.





Lừa đảo thanh toán dịch vụ



Phương thức, thủ đoạn

Giả danh nhân viên công ty điện lực, công ty cấp thoát nước, công ty viễn thông, internet để gọi điện, nhắn tin yêu cầu thanh toán tiền dịch vụ định kỳ, hoặc cập nhật thông tin.

Chúng yêu cầu nạn nhân cài ứng dụng giả mạo, sau đó đánh cắp thông tin cá nhân, tài khoản ngân hàng để chiếm đoạt tài sản.





Lừa đảo thanh toán dịch vụ

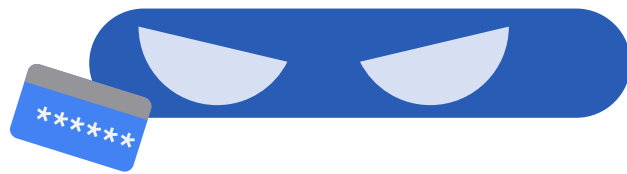
Kịch bản dẫn dắt

1. Gọi từ số lạ, nói chuyện khẩn cấp: Dùng sim rác gọi điện, tự xưng là nhân viên điện, nước. Thông báo tiền dịch vụ định kỳ chưa đóng và dọa sẽ cắt điện/nước nếu không thanh toán ngay lập tức.

2. Ép cập nhật thông tin “quản lý nhà nước”: Yêu cầu cập nhật thông tin cá nhân qua một ứng dụng được nói là “quản lý khách hàng toàn quốc”, thực chất đây là ứng dụng giả mạo.

3. Dụ dỗ cài ứng dụng giả mạo và giữ liên lạc liên tục: Hướng dẫn cài đặt ứng dụng, rồi liên tục giữ liên lạc để “hướng dẫn từng bước”, khiến người dân mất cảnh giác.

4. Lợi dụng để lấy thông tin ngân hàng: Trong lúc “hướng dẫn”, đối tượng yêu cầu nhập thông tin tài khoản, mật khẩu, mã OTP và ảnh chân dung. Sau đó âm thầm truy cập và rút sạch tài khoản nạn nhân.



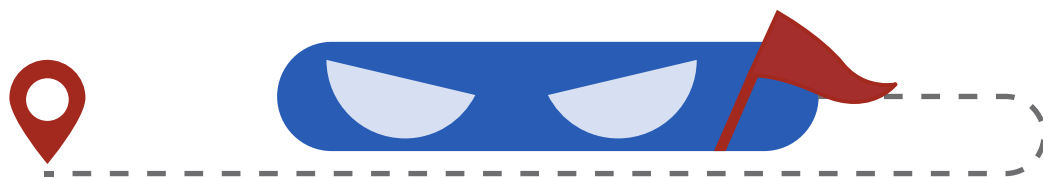
Lừa đảo thanh toán dịch vụ

Cách phòng, chống



- ° Chỉ tải và cài đặt ứng dụng từ các nguồn chính thống; không cài đặt ứng dụng theo sự hướng dẫn của người lạ liên hệ qua điện thoại, mạng xã hội.
- ° Không cung cấp thông tin tài khoản ngân hàng, mật khẩu, mã OTP qua điện thoại, mạng xã hội, hoặc cho bất kỳ cá nhân nào không rõ danh tính.
- ° Không nhấn vào các đường liên kết lạ do người khác gửi qua tin nhắn, email, mạng xã hội. Nếu đã vô tình “nhấn” vào, phải thoát ngay và không thực hiện bất kỳ thao tác cài đặt ứng dụng nào từ các liên kết lạ đó.
- ° Khi nhận được cuộc gọi nghi ngờ giả danh nhân viên cơ quan nhà nước để lừa đảo, phải lập tức liên hệ ngân hàng để khóa tài khoản, đồng thời gọi điện hoặc đến trình báo tại cơ quan Công an nơi gần nhất để được hướng dẫn xử lý theo quy định.





Lừa đảo mua bán và du lịch trực tuyến !

Phương thức, thủ đoạn

Giả danh người bán và đại lý du lịch hợp pháp bằng cách tạo các trang web và trang mạng xã hội giả mạo, đưa ra các ưu đãi hấp dẫn để dụ dỗ nạn nhân đặt cọc.

Sau khi nhận tiền đặt cọc, chúng gửi email hoặc tin nhắn thông báo lỗi chuyển khoản và yêu cầu thanh toán thêm, sau đó chặn liên lạc và chiếm đoạt tiền.





Lừa đảo mua bán và du lịch trực tuyến

Kịch bản dẫn dắt

1. Tạo trang mạng xã hội mạo danh địa điểm du lịch nổi tiếng: Lập trang mạng xã hội có giao diện giống trang chính thức của khách sạn, khu du lịch, nghỉ dưỡng. Chạy quảng cáo, tặng tương tác, dùng số điện thoại đường dây nóng giả và bình luận “ảo” để tạo lòng tin.

2. Chào giá ưu đãi để cho khách chủ động liên hệ: Đăng các chương trình khuyến mãi hấp dẫn. Người dùng tưởng thật nên nhắn tin, gọi điện để đặt phòng.

3. Yêu cầu chuyển tiền đặt cọc: Sau khi tư vấn, đối tượng yêu cầu người dùng chuyển khoản đặt cọc vào tài khoản cá nhân.

4. Báo chuyển sai nội dung sau đó yêu cầu chuyển lại: Sau khi nhận cọc, chúng giả vờ báo chuyển sai nội dung, rồi yêu cầu chuyển thêm để “kế toán xác minh” và “hoàn lại sau”.

5. Chặn liên lạc, chiếm đoạt toàn bộ tiền: Khi đã nhận nhiều lần chuyển tiền, đối tượng xóa tin nhắn, chặn liên hệ hoặc xóa trang mạng xã hội giả đi.



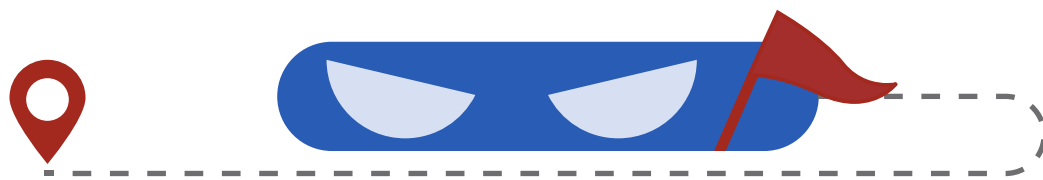
Lừa đảo mua bán và du lịch trực tuyến

Cách phòng, chống



- Kiểm tra kỹ địa chỉ trang web, các trang web tin cậy thường có chứng chỉ bảo mật (biểu tượng khóa ở góc trên bên trái của trình duyệt) và có địa chỉ rõ ràng. Cần tránh những trang web có tên miền lạ hoặc không có chứng nhận bảo mật.
- Tham khảo ý kiến của những người đã từng lưu trú tại khách sạn bạn muốn đặt, hoặc các trang đặt phòng uy tín thường có những đánh giá chi tiết của du khách trước đó.
- Chủ động liên hệ trực tiếp với khách sạn trước khi thanh toán thông qua các thông tin liên hệ trên trang chính thức như số điện thoại đường dây nóng hoặc gửi email trực tiếp để xác minh thông tin về phòng và dịch vụ. Có thể thông qua bạn bè, người thân đang sinh sống tại các khu vực dự kiến du lịch để lấy thông tin liên hệ với khách sạn, nhà nghỉ chính xác nhất.



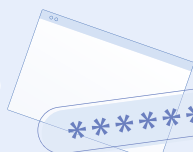


Lừa đảo mua bán và du lịch trực tuyến

Cách phòng, chống

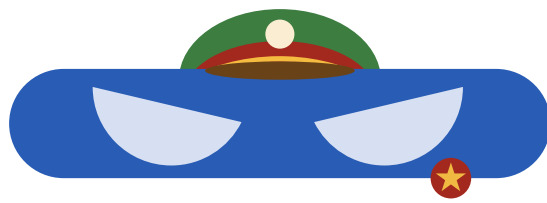


- ° Không làm theo các yêu cầu, hướng dẫn chuyển tiền cho các đối tượng vì những lý do như sai cú pháp nhắn tin hay bị treo tiền trên hệ thống,...
- ° Tuyệt đối không tải xuống các ứng dụng lạ hay nhấn vào các đường liên kết không xác định từ bên thứ ba.
- ° Chỉ nên đặt phòng qua các nền tảng uy tín để giúp bảo vệ quyền lợi của khách hàng, vì các nền tảng này thường có hệ thống bảo vệ thanh toán và các chính sách hoàn tiền nếu có xảy ra sự cố.









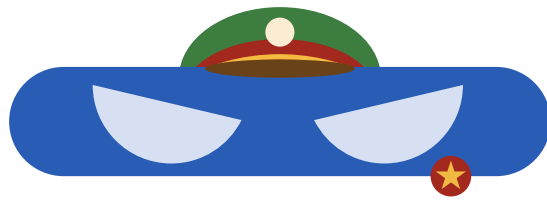
Lừa đảo mạo danh cán bộ Công An, Viện Kiểm Sát, Tòa án

Phương thức, thủ đoạn

Giả danh các cán bộ thuộc cơ quan Công an, Viện Kiểm Sát, Tòa án gọi điện đe dọa nạn nhân liên quan đến vụ việc đang điều tra (rửa tiền, buôn bán trái phép chất ma túy,...).

Chúng yêu cầu nạn nhân chứng minh sự minh bạch bằng cách chuyển tiền hoặc tải các ứng dụng giả mạo, cung cấp các thông tin đăng nhập tài khoản ngân hàng, mã OTP.





Lừa đảo mạo danh cán bộ Công An, Viện Kiểm Sát, Tòa án

Kịch bản dẫn dắt

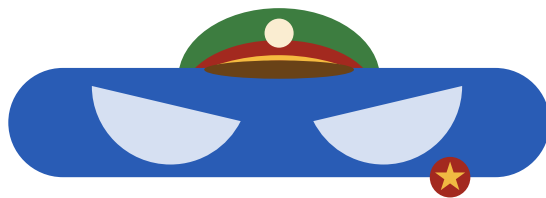
1. Gọi điện tự xưng cán bộ cơ quan chức năng:

Kẻ gian dùng số lạ gọi điện hoặc nhắn tin, nói rằng nạn nhân liên quan đến các vụ án nghiêm trọng như ma túy, bắt cóc, rửa tiền, hoặc bị lợi dụng thuê bao để chống phá Nhà nước.

2. Tung “lệnh bắt” giả để đe dọa: Chúng giả mạo các văn bản như lệnh bắt, phong tỏa tài sản, cắt thuê bao... và gửi qua mạng xã hội để khiến nạn nhân hoang mang, mất bình tĩnh.

3. Yêu cầu hợp tác chứng minh vô tội: Kẻ lừa đảo yêu cầu nạn nhân mở tài khoản ngân hàng mới, đăng ký dịch vụ ngân hàng điện tử, rồi cung cấp toàn bộ thông tin đăng nhập, mã OTP, thậm chí rút sổ tiết kiệm và vay tiền gửi vào tài khoản mới mở.

4. Chiếm đoạt tiền sau khi chuyển khoản: Sau khi nạn nhân chuyển tiền vào tài khoản mới mở mang tên mình, đối tượng chiếm quyền truy cập và rút toàn bộ số tiền sang tài khoản khác.

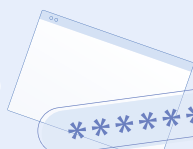


Lừa đảo mạo danh cán bộ Công An, Viện Kiểm Sát, Tòa án

Cách phòng, chống



- ° Không sợ hãi, mất bình tĩnh trước các cuộc gọi lạ, trao đổi với người thân, bạn bè khi phát hiện dấu hiệu lừa đảo.
- ° Không thực hiện theo hướng dẫn của đối tượng, tuyệt đối không chuyển tiền, cung cấp mã OTP, thông tin cá nhân cho chúng.
- ° Lực lượng Công An, Viện Kiểm Sát, Tòa Án không làm việc qua điện thoại, không có các hành vi gọi điện đe dọa, dọa nạt người dân.
- ° Liên hệ, trình báo với cơ quan chức năng để được hướng dẫn, xử lý khi phát hiện vụ việc có dấu hiệu giả danh cơ quan chức năng để thực hiện lừa đảo.

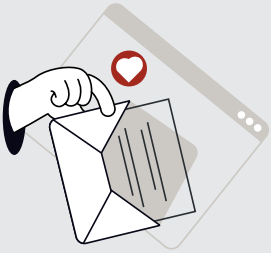








Lừa đảo tình cảm trực lợi tài chính



Phương thức, thủ đoạn

Giả danh các cá nhân có ngoại hình đẹp, tạo dựng lòng tin thông qua tin nhắn trên mạng xã hội, luôn lấy lý do để không gặp mặt trực tiếp, sau đó lừa nạn nhân tham gia vào các ứng dụng, trang web cờ bạc hoặc đầu tư giả mạo.

Chúng cho nạn nhân thắng nhỏ và rút tiền về để tạo lòng tin, rồi thúc giục nạp thêm để gia tăng lợi nhuận. Khi số tiền đủ lớn, chúng sẽ lấy lý do để khóa tài khoản, yêu cầu nạp thêm tiền để mở khóa tài khoản hoặc hứa hẹn cho rút tiền nhằm chiếm đoạt toàn bộ tài sản và cắt đứt liên lạc.





Lừa đảo tình cảm trực lợi tài chính

Kịch bản dẫn dắt

1. Tạo tài khoản giả mạo người thành đạt, ngoại hình tốt: Kẻ gian lập các tài khoản mạng xã hội với ngoại hình đẹp, giả làm bác sĩ, kỹ sư, chuyên gia sống ở nước ngoài. Họ thường xuyên đăng ảnh du lịch, khoe cuộc sống sang chảnh để tạo niềm tin.

2. Tìm hiểu và nhắm đến nạn nhân dễ tổn thương: Chúng nhắm vào phụ nữ độc thân, hay chia sẻ chuyện cá nhân, gia đình trên mạng. Sau đó kết bạn, nhắn tin xã giao, trò chuyện mỗi ngày để xây dựng lòng tin.

3. Gợi mở cơ hội “đầu tư hộ”: Khi đã thân thiết, chúng sẽ giới thiệu về việc đang có cơ hội đầu tư “đánh chắc chắn thắng” từ hệ thống cá cược hoặc đầu tư trực tuyến – rồi nhờ nạn nhân chơi hộ vì “bận công việc”.



Lừa đảo tình cảm trực lợi tài chính



Kịch bản dẫn dắt

4. Dụ nạn nhân nạp tiền vào hệ thống: Ban đầu tài khoản thắng liên tục, rút được tiền nên nạn nhân tin tưởng. Sau đó, chúng dụ nạn nhân tiếp tục nạp thêm tiền để chiếm đoạt nhiều tiền hơn.

5. Khóa tài khoản, yêu cầu nạp thêm rồi biến mất: Đến lúc số tiền đủ lớn, chúng giả vờ khóa tài khoản hoặc nói cần nạp thêm để xử lý hồ sơ, rồi cắt liên lạc hoàn toàn và chiếm đoạt toàn bộ số tiền của nạn nhân.



Lừa đảo tình cảm trực lợi tài chính

Cách phòng, chống



- ° Hạn chế trao đổi với các cá nhân chưa rõ danh tính trên không gian mạng, đặc biệt là các tài khoản có ngoại hình đẹp sau đó kết bạn với tài khoản cá nhân của mình để tâm sự riêng tư.
- ° Tuyệt đối không tin tưởng vào các thông tin do các đối tượng này cung cấp (như hình ảnh gia đình, vé máy bay, CCCD...) do các thông tin này hầu hết có thể làm giả, sao chép trên không gian mạng.
- ° Hạn chế đăng tải các hình có chứa thông tin cá nhân, công việc, gia đình lên các mạng xã hội hoặc thiết lập chế độ chỉ cho phép bạn bè bình luận, tương tác để hạn chế việc tội phạm lợi dụng các hình ảnh này để thực hiện hành vi lừa đảo.
- ° Trường hợp nghi vấn các đối tượng thực hiện hành vi lừa đảo chiếm đoạt tài sản, nạn nhân cần báo ngay cho cơ quan Công an gần nhất để được hỗ trợ, xử lý kịp thời. Tuyệt đối không chuyển tiền cho các đối tượng tự nhận là Công an, luật sư ... để thu hồi số tiền đã mất.







Lừa đảo đầu tư trên nền tảng giả mạo



Phương thức, thủ đoạn

Giả danh nhân viên của các sàn thương mại điện tử, sàn đầu tư ngoại hối, tiền ảo, tài chính quốc tế gọi điện thoại cho nạn nhân kêu gọi đầu tư lợi nhuận cao.

Chúng sử dụng các trang web, nền tảng giả mạo và hội nhóm mạng xã hội để thao túng nạn nhân đầu tư, chỉnh sửa lệnh cho nạn nhân dễ dàng thắng những khoản đầu tư nhỏ, khi nạn nhân đầu tư khoản tiền lớn thì chúng sẽ đánh cháy tài khoản hoặc đánh sập sàn.



Lừa đảo đầu tư trên nền tảng giả mạo

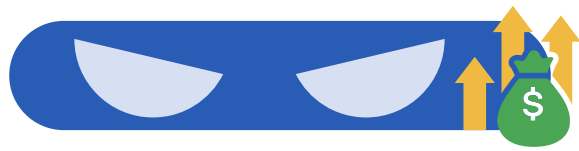
Kịch bản dẫn dắt

1. Gọi từ số không chính chủ, mạo danh nhân viên sàn uy tín: Kẻ gian gọi điện cho nạn nhân, giới thiệu những cơ hội đầu tư tài chính có lãi suất cao.

2. Thêm vào nhóm chat có “chuyên gia” và “nhà đầu tư cò mối”: Trong nhóm, “chuyên gia” giới thiệu mã đầu tư; “nhà đầu tư” thì bình luận sôi nổi khoe đã mua và đang có lãi, nhằm tạo dựng hiệu ứng tin tưởng.

3. Nạp thử, trúng thật: Ban đầu, hệ thống cho nạn nhân rút lời để tạo cảm giác yên tâm. Sau đó dụ nạp thêm tiền để sinh lợi lớn hơn.

4. Nạp thêm để mở khoá tài khoản: Khi số tiền đủ lớn, chúng sẽ báo tài khoản có lỗi, yêu cầu nạp thêm để mở khoá. Cuối cùng, kẻ gian chặn liên lạc, đánh sập hệ thống và chiếm toàn bộ số tiền.



Lừa đảo đầu tư trên nền tảng giả mạo

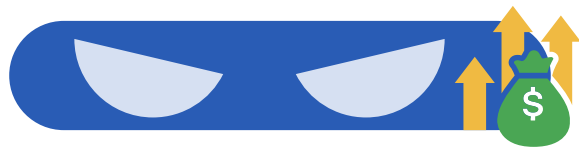
Cách phòng, chống



- Cảnh giác khi tham gia đầu tư chứng khoán, đa cấp, tiền ảo... trên các sàn giao dịch trực tuyến không rõ ràng, có dấu hiệu giả mạo hoặc không được công bố thông tin minh bạch.
- Chỉ đầu tư vào các sàn giao dịch đã được cơ quan quản lý nhà nước cấp phép hoạt động. Cần kiểm tra rõ ràng về pháp lý, địa chỉ thật, và tính xác thực của sàn trước khi đầu tư. Ưu tiên đến trực tiếp văn phòng của sàn giao dịch để được tư vấn, xác minh thông tin và tránh rủi ro khi thực hiện đầu tư qua các kênh trực tuyến không kiểm chứng.







Lừa đảo đầu tư trên nền tảng giả mạo

Cách phòng, chống

- ° Không chia sẻ thông tin cá nhân và không làm theo hướng dẫn của người lạ trên mạng xã hội khi chưa xác minh rõ danh tính và lai lịch của họ.
- ° Tìm hiểu thông tin về các hình thức lừa đảo qua mạng khi có dấu hiệu nghi ngờ bị lừa; chủ động hỏi ý kiến từ người thân, bạn bè có kinh nghiệm để được hỗ trợ kịp thời.
- ° Trình báo ngay với cơ quan Công an nơi gần nhất khi phát hiện dấu hiệu bị lừa đảo; đồng thời liên hệ với ngân hàng chủ quản để khóa tài khoản hoặc đề nghị hỗ trợ xử lý giao dịch.





99+



03



**An toàn hơn khỏi lừa
đảo trực tuyến cùng
các giải pháp từ
Google**



Tại Google, chúng tôi bảo vệ người dùng trên không gian mạng bằng cách tích hợp sẵn các tính năng “bảo mật mặc định” trong mọi sản phẩm, mang đến khả năng bảo vệ tự động và cảnh báo kịp thời.



Các sản phẩm được thiết kế để bảo vệ người dùng



Bằng cách ứng dụng trí tuệ nhân tạo (AI) tiên tiến, Google chủ động phát hiện, ngăn chặn và loại bỏ các nội dung lừa đảo, góp phần xây dựng một không gian mạng an toàn và tin cậy hơn trên các nền tảng của mình, dựa trên ba nguyên tắc sau:



Bảo mật mặc định: Người dùng được bảo vệ tự động ngay khi sử dụng sản phẩm, mà không cần thực hiện bất kỳ bước cài đặt phức tạp nào.



Bảo vệ quyền riêng tư: Quyền riêng tư luôn là ưu tiên hàng đầu. Mọi sản phẩm của chúng tôi đều được phát triển với cơ chế bảo mật tích hợp, giúp người dùng toàn quyền kiểm soát thông tin cá nhân ngay từ ban đầu.

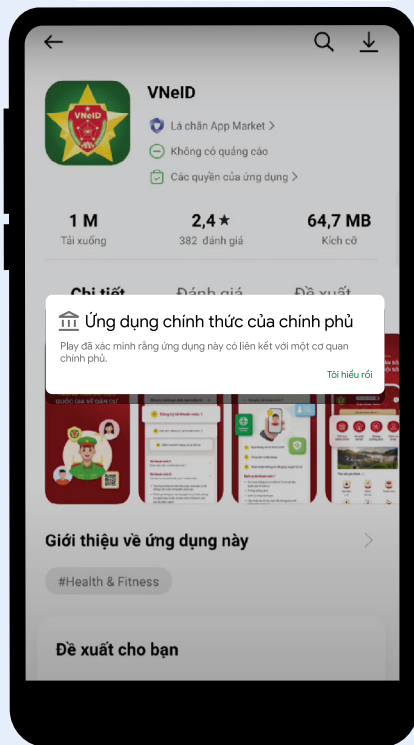


Nắm quyền kiểm soát: Người dùng luôn giữ quyền làm chủ dữ liệu của mình. Chúng tôi cung cấp đầy đủ công cụ và thông tin minh bạch để bạn dễ dàng điều chỉnh cài đặt quyền riêng tư và bảo mật theo nhu cầu cá nhân.





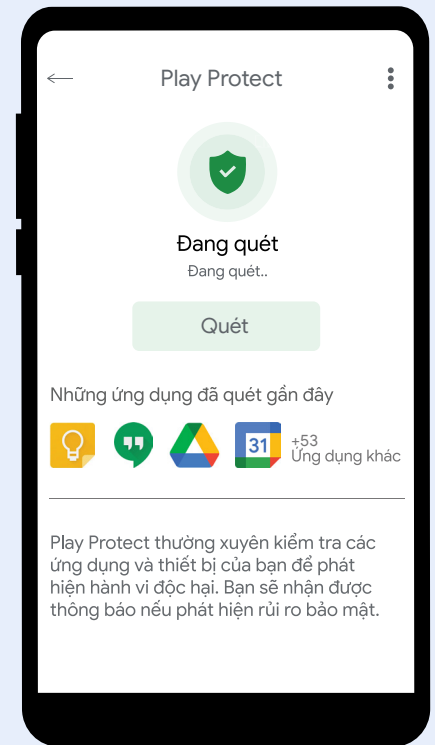
Xác thực ứng dụng Chính phủ: Nhận diện ứng dụng Chính Phủ hợp pháp



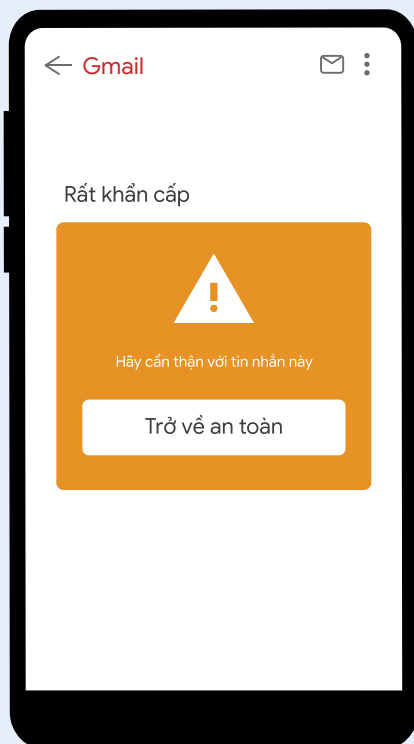
Duyệt web an toàn: Phát hiện và ngăn chặn trang web lừa đảo



Google Play Protect: Quét các ứng dụng độc hại



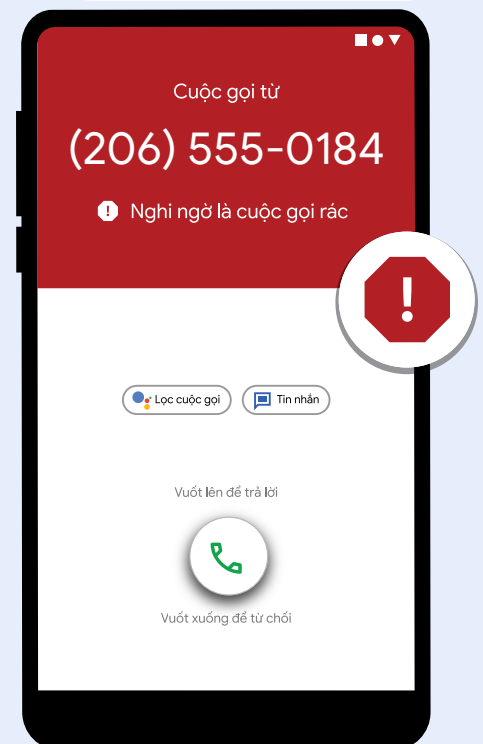
Gmail: Ngăn chặn thư rác, hành vi lừa đảo



Google Tin Nhắn: Nhận cảnh báo về tin nhắn đáng ngờ



Google Điện Thoại: Xác minh danh tính người gọi và chặn cuộc gọi làm phiền





Các sản phẩm được thiết kế để bảo vệ người dùng



Xác thực ứng dụng Chính Phủ

Nhận diện ứng dụng Chính Phủ hợp pháp

"Xác thực ứng dụng Chính phủ" của Google là gì và nó hoạt động như thế nào?

° Từ tháng 12/2024, Việt Nam là quốc gia đầu tiên hợp tác với Google để triển khai tính năng **"Xác thực ứng dụng Chính phủ" trên Google Play** - với hơn 110* ứng dụng thuộc các cơ quan nhà nước đã được gắn nhãn xác thực.

° Tính năng này giúp người dùng Việt Nam dễ dàng nhận diện và phân biệt các ứng dụng hợp pháp của Chính phủ với các ứng dụng giả mạo, lừa đảo. Khi một ứng dụng Chính phủ đã được xác minh, **Google Play** sẽ hiển thị một biểu tượng đặc biệt (ví dụ: **"Government"** hoặc **"Chính phủ"**) để người dùng dễ dàng nhận biết.

(*) Cập nhật 7/2025







Các sản phẩm được thiết kế để bảo vệ người dùng



Duyệt web an toàn

Phát hiện và ngăn chặn trang web lừa đảo

Tính năng Duyệt web an toàn của Google là gì và có thể bảo vệ người dùng như thế nào?

- ° **Duyệt web an toàn** của Google là một công cụ bảo mật tích hợp được thiết kế để giúp bảo vệ người dùng khỏi các trang web nguy hiểm và lừa đảo.
- ° Khi bạn truy cập một trang web hoặc sắp tải xuống một tệp, **Duyệt web an toàn** của Google sẽ tự động kiểm tra xem nội dung đó có nằm trong danh sách các trang web độc hại, lừa đảo hoặc chứa phần mềm độc hại đã biết hay không. Nếu phát hiện ra bất kỳ mối nguy hiểm nào, hệ thống sẽ hiển thị cảnh báo. Cảnh báo này sẽ cung cấp cho bạn tùy chọn để "Quay lại trang an toàn" chỉ với một cú nhấp, để tránh truy cập trang web hoặc tải xuống tệp độc hại.



Theo thông tin của Google, tính năng **Duyệt web an toàn** đã và đang bảo vệ bao nhiêu thiết bị?

Theo báo cáo nội bộ từ Google, tính năng **Duyệt web an toàn** hiện tự động bảo vệ hơn 5 tỷ thiết bị trên toàn thế giới.



Tính năng **Duyệt web an toàn** có được chia sẻ với các trình duyệt khác không?

Có, Google cung cấp tính năng **Duyệt web an toàn** miễn phí cho các trình duyệt và công ty Internet khác, và nó được triển khai trên nhiều trình duyệt cạnh tranh như Firefox và Safari, trên các nền tảng bao gồm iOS và Android.





Các sản phẩm được thiết kế để bảo vệ người dùng



Google Play Protect

Quét các ứng dụng độc hại

Google Play Protect là gì và cách nó bảo vệ thiết bị Android?

- ° Đây là công cụ quét các ứng dụng trên thiết bị Android để tìm kiếm mối nguy hại. Công cụ này luôn kiểm tra các ứng dụng tải từ cửa hàng **Google Play**, và cả những ứng dụng tải từ bên ngoài, giữ cho thiết bị người dùng luôn an toàn khỏi phần mềm độc hại và các phần mềm không mong muốn.
- ° Tại Việt Nam, **Google Play Protect** đã ngăn chặn hơn 4,5 triệu lượt cài đặt ứng dụng có dấu hiệu độc hại trên 1 triệu thiết bị Android.





Các sản phẩm được thiết kế để bảo vệ người dùng



Gmail

Ngăn chặn thư rác, hành vi lừa đảo

Gmail sẽ bảo vệ người dùng khỏi thư rác, phần mềm độc hại và lừa đảo qua mạng như thế nào?

Gmail được biết đến với hiệu quả cao trong việc bảo vệ người dùng khỏi thư rác và các cuộc tấn công lừa đảo nhờ khả năng sàng lọc nội dung được tăng cường bởi AI.

Gmail tự động chặn hơn 99,9% thư rác, lừa đảo và phần mềm độc hại, bảo vệ hơn 2,5 tỷ hộp thư mỗi ngày.



Gmail có những biện pháp bảo vệ nào chống lại các email không được xác thực hoặc gửi hàng loạt?

° Kể từ năm 2023, **Gmail** đã bắt buộc tất cả các email gửi đến địa chỉ **Gmail** phải có một hình thức xác thực nào đó. Quy định này đã mang lại hiệu quả đáng kể, giúp giảm 65% số lượng tin nhắn không xác thực mà người dùng **Gmail** nhận được. Việc này giúp ngăn chặn các email giả mạo hoặc lừa đảo mạo danh các tổ chức hoặc cá nhân đáng tin cậy.

° Từ đầu năm 2024, **Gmail** cũng đã áp dụng các yêu cầu nghiêm ngặt hơn đối với những người gửi email hàng loạt (gửi hơn 5.000 email mỗi ngày). Theo đó, họ phải:

- **Xác thực email của mình:** Đảm bảo tính hợp lệ và nguồn gốc rõ ràng của email.
- **Cho phép hủy đăng ký dễ dàng:** Cung cấp tùy chọn hủy nhận email chỉ bằng một cú nhấp chuột, giúp người dùng dễ dàng kiểm soát hộp thư đến của mình.
- **Duy trì tỷ lệ báo cáo thư rác thấp:** Những người gửi này phải đảm bảo các email của họ ít bị người dùng đánh dấu là thư rác.





Các sản phẩm được thiết kế để bảo vệ người dùng



Google Điện Thoại

Xác minh danh tính người gọi và chặn cuộc gọi làm phiền

Ứng dụng Google Điện thoại bảo vệ tôi khỏi các cuộc gọi lừa đảo như thế nào?

Ứng dụng **Google Điện thoại** (Phone by Google) tích hợp tính năng xác định ID người gọi, bảo vệ chống cuộc gọi rác và tính năng **Sàng lọc cuộc gọi** (Call Screen) để giúp bảo vệ người dùng khỏi lừa đảo. Tính năng này chặn các cuộc gọi nguy hiểm và cảnh báo bạn về những cuộc gọi đáng ngờ.





Các sản phẩm được thiết kế để bảo vệ người dùng



Google Tin Nhắn

Nhận cảnh báo về tin nhắn đáng ngờ

Google Tin nhắn bảo vệ người dùng khỏi thư rác và lừa đảo qua mạng như thế nào?

Google Tin nhắn mang đến khả năng bảo vệ tích hợp chống lại thư rác và các chiêu trò lừa đảo. Tính năng này giúp giữ an toàn cho bạn bằng cách:

- **Cảnh báo và lọc tự động:** **Google Tin nhắn** sẽ tự động cảnh báo bạn về các tin nhắn đáng ngờ và lọc chúng ra khỏi hộp thư chính. Đồng thời, nó cũng nhận diện và chặn các đường liên kết (link) không an toàn được đính kèm.
- **Phát hiện thông minh bằng AI:** Dịch vụ này sử dụng **Trí tuệ nhân tạo (AI)** để liên tục phát hiện các tin nhắn khả nghi. AI sẽ đánh giá độ tin cậy của người gửi, tìm kiếm các mẫu tin nhắn lừa đảo đã biết và nhận diện các đường liên kết nguy hiểm, từ đó bảo vệ bạn một cách chủ động.







99+



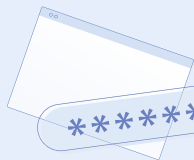
04



**Bắt bài lừa đảo
online**



BẮT BÀI LỪA ĐẢO ONLINE



Tình huống 1

Một số điện thoại lạ gọi đến và tự xưng là nhân viên của một sàn chứng khoán lớn và uy tín.



Chào bạn! Mình đang có một cơ hội đầu tư lợi nhuận cao, mỗi tháng cam kết lời từ 15% đến 20% và gần như không có rủi ro. Tham gia ngay nhé!

Là thật

hay

lừa đảo?



Tình huống 2

Bạn nhận được cuộc gọi từ một nhân viên công ty chứng khoán bạn từng mở tài khoản.



Công ty Chứng khoán ABC
0123 456 789

Tôi là A, là nhân viên công ty chứng khoán ABC.
Số tài khoản chứng khoán của bạn là 0123456, mời bạn đến văn phòng của chúng tôi để được tư vấn đầu tư trực tiếp tại: Số 2, Phố XXX, Quận YYY, TP Hà Nội.

Là thật

hay

lừa đảo?



Tình huống 3

Vừa bị lừa một khoản lớn qua mạng, khi tìm cách lấy lại tiền, bạn tìm thấy các trang web chuyên nghiệp,...



Tình huống 4

Một người lạ có ngoại hình thu hút gửi lời mời kết bạn qua mạng xã hội. Sau vài ngày nhắn tin tâm sự, họ chia sẻ...



Lời kết



Lừa đảo trực tuyến đang ngày càng tinh vi và khó lường hơn. Vì thế, bạn cần nâng cao hiểu biết, cập nhật kiến thức cho chính mình và người thân. Bắt đầu từ những bước đơn giản như sau:

- 1 Cảnh giác với người lạ chủ động kết bạn, liên hệ, đặc biệt qua các ứng dụng hẹn hò hoặc mạng xã hội.
- 2 Không cung cấp, chia sẻ thông tin cá nhân (CMND/CCCD, tài khoản ngân hàng, mã OTP...) dưới bất kỳ hình thức nào.
- 3 Cẩn trọng khi nhấp vào đường liên kết lạ, không tải ứng dụng không rõ nguồn gốc từ người chưa xác minh danh tính.
- 4 Không làm theo hướng dẫn như đăng nhập, xác minh, chuyển tiền từ bất kỳ người lạ nào trên mạng.
- 5 Cài đặt các công cụ bảo mật, nhận diện lừa đảo để tránh bị chiếm quyền truy cập.
- 6 Khi nghi ngờ có dấu hiệu lừa đảo, hãy liên hệ cơ quan công an gần nhất để được hỗ trợ và xử lý kịp thời.









Bên cạnh đó, hãy theo dõi ngay các kênh chính thống của **Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an** trên mạng xã hội để cập nhật thông tin, thủ đoạn của tội phạm sử dụng công nghệ cao, tội phạm lừa đảo trực tuyến hiệu quả nhất.



<https://www.youtube.com/@pctpluadaotructuyen>



<https://www.facebook.com/csched.gov.vn>



tiktok.com/@csched.gov.vn





BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG
TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

Google

Hy vọng những nội dung trong **Cẩm nang**
CHUNG TAY PHÒNG, CHỐNG LỪA ĐẢO ONLINE
sẽ trở thành công cụ hữu ích, giúp bạn sử dụng Internet
một cách an toàn hơn.



Đáp án thử thách “**Bắt bài lừa đảo online**”

Tình huống 1



Là lừa đảo

Là kẻ lừa đảo giả danh tư vấn đầu tư

Bắt bài

Gọi từ số lạ, không xác minh được danh tính người gọi.

Ưu đãi quá tốt đến mức khó tin: Cam kết lợi nhuận cao, rủi ro thấp là chiêu trò thường thấy trong các mô hình đầu tư ảo.



Bí kíp phòng, chống



Google Điện Thoại

Hỗ trợ bạn xác minh danh tính người gọi, cảnh báo nếu số có dấu hiệu lừa đảo, và chặn cuộc gọi quấy rối từ số không chính chủ.

Tình huống 2



Là thật

Bắt bài

Cuộc gọi đến từ đầu số chính chủ, hiển thị thương hiệu rõ ràng.

Nhân viên xác minh kỹ thông tin và không yêu cầu bạn chuyển tiền hay cung cấp OTP qua điện thoại.

Hẹn tư vấn trực tiếp tại địa điểm chính thức của công ty.



Bí kíp phòng, chống



Google Điện Thoại

Hỗ trợ bạn xác minh danh tính người gọi, cảnh báo nếu số có dấu hiệu lừa đảo, và chặn cuộc gọi quấy rối từ số không chính chủ.



Đáp án thử thách “**Bắt bài lừa đảo online**”

Tình huống 3



Là lừa đảo

Là kẻ lừa đảo giả mạo đơn vị hỗ trợ thu hồi tiền lừa đảo

Bắt bài

Đường liên kết lạ, không chính thống.

Cơ quan Công An và Viện Kiểm Sát không ủy quyền cho bên thứ ba.

Bí kíp phòng, chống



Duyệt web an toàn

Giúp phát hiện và ngăn chặn trang web lừa đảo.

Tình huống 4



Là lừa đảo

Là kẻ lừa đảo lợi dụng tình cảm để trục lợi tài chính

Bắt bài

Cẩn thận với cá nhân có ảnh đẹp, lý lịch “hoàn hảo” tiếp cận trò chuyện.

Cảnh giác các liên kết lạ gửi từ người gửi chưa xác minh lai lịch trên không gian mạng.

Bí kíp phòng, chống



Duyệt web an toàn

Giúp phát hiện và ngăn chặn trang web lừa đảo.



BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG
TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

Google

Lừa đảo online



✓ Chung tay phòng, chống