

EXIMBANK



CẨM NANG NHẬN DIỆN & PHÒNG CHỐNG LỪA ĐẢO TRỰC TUYẾN



I. Các thủ đoạn lừa đảo



1. Giả danh cơ quan nhà nước
2. Giả danh ngân hàng, ví điện tử
3. Giả nhân viên dịch vụ điện/nước/viễn thông
4. Giả danh trường học, giáo viên
5. Giả hỗ trợ hoàn tiền, xử lý giao dịch lỗi.....
6. Hack tài khoản mạng xã hội mượn tiền
7. Giả gửi quà, trúng thưởng, nạp nhận thưởng
8. Lừa đảo tour, vé rẻ
9. Lừa tình, dẫn dụ đầu tư, tiền ảo, đa cấp.....
10. Lừa đầu tư tài chính
11. Tuyển CTV, tuyển dụng lao động.....
12. Giả biên lai, đòi hoàn tiền
13. Lừa chuyển tiền nhằm để chiếm đoạt tiền
14. Sử dụng công nghệ deepfake - kỹ thuật AI để giả người thân, công an
15. Lừa đảo mã QR giả
16. Lừa cài đặt/cập nhật thông tin VNeID
17. Giả Shipper lừa chuyển tiền
18. Mạo danh dịch vụ hỗ trợ lấy lại tiền đã bị lừa

II. Dấu hiệu lừa đảo



1. Dấu hiệu qua cuộc gọi
2. Dấu hiệu qua tin nhắn, email
3. Dấu hiệu qua trang web và biểu mẫu giả
4. Dấu hiệu ứng dụng giả mạo
5. Dấu hiệu tài khoản mạng xã hội đáng ngờ
6. Dấu hiệu nguồn thông tin giả mạo

III. Xử lý khi gặp lừa đảo



1. Xử lý khi gặp lừa đảo trực tuyến
2. Trường hợp đã chuyển tiền cho kẻ lừa đảo
3. Bị mất tài khoản/mất quyền thiết bị.....

IV. Phòng tránh lừa đảo



1. Quy tắc “6 KHÔNG”
2. Kiểm tra nguồn gốc thông tin.....
3. Cảnh giác với tương tác trên mạng xã hội.....
4. Bảo vệ tài khoản và thiết bị.....
5. Quản lý và sao lưu dữ liệu tài chính.....

V. Kênh hỗ trợ khi gặp lừa đảo



1. Công an địa phương
2. Ngân hàng hoặc ví điện tử liên quan
3. Cục An ninh mạng (A05 – Bộ Công an)
4. Báo cáo lừa đảo qua VNeID.....

LỜI MỞ ĐẦU

Thời gian qua, người dân Việt Nam, đặc biệt là khách hàng ngân hàng, thường xuyên đối mặt với nguy cơ lừa đảo qua không gian mạng. Các đối tượng lừa đảo sử dụng thủ đoạn tinh vi, khai thác tâm lý và điểm yếu của con người để chiếm đoạt niềm tin, dẫn dắt theo các kịch bản đã được chuẩn bị. Các hình thức lừa đảo trực tuyến ngày càng gia tăng, bao gồm đánh cắp thông tin tài khoản, lừa đảo qua giao dịch giả mạo, hay các chiêu trò liên quan đến đầu tư tài chính, với mục tiêu cuối cùng nhắm đến tài sản và tiền gửi của khách hàng.

Bên cạnh các giải pháp kỹ thuật bảo mật, việc nâng cao nhận thức và trang bị kỹ năng từ cơ bản đến nâng cao cho khách hàng được xem là biện pháp then chốt để ngăn chặn tác động tiêu cực từ lừa đảo trực tuyến. Khi khách hàng, đặc biệt là các nhóm dễ bị tổn thương, nắm vững kỹ năng nhận diện và phòng chống lừa đảo, họ sẽ chủ động hơn, từ đó giảm thiểu rủi ro trong các giao dịch ngân hàng trực tuyến.

Phòng chống lừa đảo trên không gian mạng không chỉ là trách nhiệm của các cơ quan chức năng hay tổ chức tài chính, mà là trách nhiệm chung của toàn xã hội. Trong bối cảnh tội phạm công nghệ ngày càng tinh vi, mỗi cá nhân cần chủ động nâng cao nhận thức và trang bị đầy đủ kiến thức, kỹ năng cần thiết để tự bảo vệ mình.



Đặc biệt, khi sử dụng các dịch vụ ngân hàng trực tuyến, người dùng cần thận trọng trong việc bảo mật thông tin cá nhân, tài khoản đăng nhập, mã OTP, và tuyệt đối không chia sẻ thông tin nhạy cảm qua các kênh không chính thống. Việc sử dụng dịch vụ một cách an toàn, có hiểu biết sẽ góp phần quan trọng trong việc ngăn chặn, giảm thiểu rủi ro lừa đảo, bảo vệ tài sản cá nhân và giữ gìn sự an toàn cho toàn hệ thống tài chính.

I. CÁC THỦ ĐOẠN LỪA ĐẢO

Giả danh cơ quan nhà nước



Kẻ gian mạo danh Công an, Viện Kiểm sát, Tòa án... làm giả giấy tờ, con dấu để tăng độ tin cậy.

Gọi điện hoặc nhắn tin thông báo nạn nhân liên quan vụ án, yêu cầu chuyển tiền để "xác minh", "điều tra", tạo áp lực tâm lý nhằm chiếm đoạt tài sản.

Giả danh ngân hàng, ví điện tử



Kẻ gian giả mạo nhân viên ngân hàng hoặc ví điện tử,

Gọi điện, gửi tin nhắn hỗ trợ thực hiện dịch vụ: cập nhật thông tin sinh trắc học/xác minh tài khoản, cung cấp OTP/các dịch vụ thẻ, tài khoản/hoàn tiền, hoàn phí và hướng dẫn, truy cập vào đường link giả mạo.

Dùng phần mềm gián điệp, lừa người dùng nhập thông tin vào trang web giả để lấy cắp tài khoản. Gửi tin nhắn mạo danh ngân hàng yêu cầu cập nhật thông tin.

Mục tiêu là chiếm đoạt tiền trong tài khoản của nạn nhân.

Đối tượng giả làm nhân viên điện, nước, internet...

Giả nhân viên dịch vụ điện/nước/viễn thông



Gọi điện, nhắn tin thông báo nợ tiền điện/nước/cước phí hoặc sử dụng dịch vụ bất thường, đe dọa nếu không thanh toán ngay sẽ bị ngừng dịch vụ. Sau đó, gửi hóa đơn giả mạo hoặc hướng dẫn tải ứng dụng giả mạo của công ty điện lực/nước/viễn thông hoặc gửi mã QR yêu cầu thanh toán qua các kênh để chiếm đoạt tiền trong tài khoản.



Giả danh trường học, giáo viên



Kẻ gian giả danh giáo viên hoặc nhân viên nhà trường,...

Thông báo học sinh nhận học bổng, hoàn học phí, hoặc đi trại hè... Sau đó yêu cầu phụ huynh cung cấp thông tin, đóng phí để lừa đảo chiếm đoạt tiền.

Giả hỗ trợ hoàn tiền, xử lý giao dịch lỗi



Các đối tượng giả danh nhân viên ngân hàng, ví điện tử hoặc sàn thương mại điện tử;

Viện lý do hỗ trợ “hoàn tiền”, “xử lý lỗi giao dịch” để lừa người dùng cung cấp OTP, thông tin tài khoản. Sau đó, chúng chiếm đoạt tiền và chặn liên lạc, gây thiệt hại cho nạn nhân.

Hack tài khoản mạng xã hội mượn tiền



Kẻ gian chiếm quyền kiểm soát tài khoản Facebook, Telegram...

Rồi giả danh chủ tài khoản nhắn tin mượn tiền người thân, bạn bè. Nạn nhân tin tưởng chuyển tiền mà không kiểm tra lại, dẫn đến bị lừa đảo.

I. CÁC THỦ ĐOẠN LỪA ĐẢO

EXIMBANK



Giả gửi quà, trúng thưởng, nạp nhận thưởng



Kẻ lừa đảo thông báo cho nạn nhân đã trúng thưởng một món quà giá trị hoặc được nhận quà miễn phí,...

Kẻ lừa đảo yêu cầu thanh toán một khoản phí (phí vận chuyển, phí làm hồ sơ, thuế, v.v.) để nhận được món quà đó. Thực chất, đây là một cách để chiếm đoạt tiền của nạn nhân và có thể là cả thông tin cá nhân.

Lừa đảo tour, vé rẻ



Đối tượng quảng cáo hoặc lập các hội nhóm bán vé máy bay, thanh lý voucher du lịch, quảng cáo các gói khuyến mãi, giảm giá tour du lịch tại các khách sạn, khu nghỉ dưỡng nổi tiếng trên mạng xã hội.

Khi khách hàng liên hệ, chúng yêu cầu chuyển khoản đặt cọc một phần tiền. Sau khi nhận tiền, trang web hoặc hội nhóm kẻ trên sẽ biến mất.

Lừa tình, dẫn dụ đầu tư



Kẻ gian làm quen qua mạng, giả yêu đương để tạo lòng tin.

Sau đó dẫn dụ nạn nhân rót tiền vào các dự án đầu tư giả, sàn ảo rồi chiếm đoạt tài sản.

I. CÁC THỦ ĐOẠN LỪA ĐẢO

EXIMBANK



Lừa đầu tư tài chính, tiền ảo, đa cấp



Đối tượng mời gọi đầu tư vào sản phẩm chứng khoán, ngoại hối, tiền ảo... với cam kết lợi nhuận cao, khả năng rút vốn dễ dàng.

Ban đầu, chúng trả lãi đầy đủ để tạo lòng tin, khi nạn nhân tiếp tục đầu tư với số tiền lớn hơn, kẻ gian can thiệp hệ thống, lập tức chặn tài khoản và chiếm đoạt toàn bộ số tiền.

Tuyển CTV, tuyển dụng lao động



Kẻ gian giả mạo tuyển cộng tác viên/tuyển dụng lao động, tạo nhóm, làm nhiệm vụ online như tăng tương tác, đặt đơn ảo... với hứa hẹn hoa hồng cao hoặc nộp tiền tham gia các khóa học ngắn hạn để đủ điều kiện nhận việc.

Ban đầu trả thưởng nhỏ để tạo lòng tin, sau đó yêu cầu nạn nhân nạp tiền nhiều lần rồi chiếm đoạt.

Giả biên lai, đòi hoàn tiền



Kẻ gian giả gửi nhầm tiền và cung cấp biên lai chuyển khoản giả.

Yêu cầu nạn nhân chuyển lại tiền. Nếu nạn nhân không kiểm tra kỹ, sẽ bị lừa mất tiền thật.

I. CÁC THỦ ĐOẠN LỪA ĐẢO

EXIMBANK



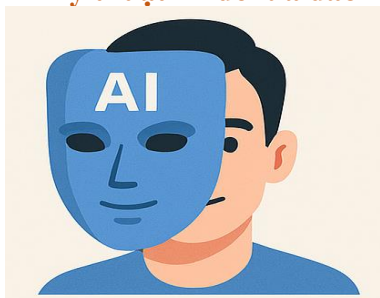
Lừa chuyển nhầm để chiếm đoạt tiền



Kẻ gian cố ý chuyển khoản một số tiền nhỏ rồi giả vờ nhầm, yêu cầu hoàn lại.

Sau đó, chúng gửi biên lai giả số tiền lớn hơn để lừa nạn nhân hoàn tiền vượt mức, nhằm chiếm đoạt phần chênh lệch.

Sử dụng công nghệ deepfake - kỹ thuật AI để lừa đảo



Đối tượng sử dụng công nghệ deepfake để mô phỏng hình ảnh khuôn mặt/giọng bằng AI để tạo video giả người thân, bạn bè, cấp trên, cán bộ nhà nước...

Gọi điện, nhắn tin yêu cầu/thúc giục chuyển tiền gấp, tạo cảm giác cấp bách, để khiến nạn nhân mất cảnh giác, bị lừa đảo.

Lừa đảo mã QR giả



Kẻ gian tạo mã QR giả mạo thanh toán, quyền góp, đăng nhập dịch vụ.

Khi nạn nhân quét mã, có thể bị chuyển tiền sai người, bị đánh cắp thông tin cá nhân, tài khoản ngân hàng.



Lừa cập nhật thông tin VNeID



Kẻ gian giả cơ quan Công an, cơ quan tư pháp, cơ quan Bảo hiểm xã hội, thuế ...

Yêu cầu cung cấp/cập nhật thông tin trên VNeID, hướng dẫn cài đặt và kích hoạt định danh điện tử để đánh cắp thông tin cá nhân.

Giả Shipper lừa chuyển tiền



Kẻ gian giả danh nhân viên giao hàng (shipper),...

Gọi điện hoặc nhắn tin thông báo có đơn hàng cần giao, yêu cầu người nhận chuyển khoản trước để thanh toán phí giao hàng, phí COD, hoặc các khoản phí phát sinh khác.

Giả danh dịch vụ hỗ trợ lấy lại tiền đã bị lừa



Nhắm vào tâm lý hoang mang của những người vừa bị lừa đảo qua mạng, các đối tượng đóng vai luật sư, nhân viên ngân hàng, kỹ sư công nghệ thông tin... quảng cáo có thể giúp những người từng bị lừa đảo lấy lại tiền đã mất.

Chúng liên tục gọi điện, nhắn tin và yêu cầu nạn nhân phải trả trước “phí dịch vụ”. Sau khi thu được tiền từ nạn nhân, các đối tượng lập tức cắt đứt liên lạc.



QUA CUỘC GỌI

-  Tự xưng công an, tòa án, ngân hàng,... để gây áp lực
-  Nói bạn liên quan vụ án, nợ xấu, tiền bị treo
-  Yêu cầu cung cấp OTP, mật khẩu, chuyển tiền để “điều tra/xác minh”, sẽ trả lại tiền sau khi được chứng minh vô tội/xử lý xong thông tin sai lệch về nợ xấu/tiền treo.
-  Không cho dùng máy, dọa xử lý hình sự



QUA TIN NHẮN, EMAIL

-  Gửi từ địa chỉ lạ, giả mạo tên tổ chức uy tín
-  Nội dung giật gân, lỗi chính tả, hỏi thúc hành động
-  Gửi link lạ, tệp đính kèm độc hại
-  Yêu cầu cung cấp thông tin cá nhân, tài khoản, OTP

WEB, BIỂU MẪU GIẢ MẠO



-  Link lạ khác với trang chính thức
-  Giao diện giống thật nhưng sai logo
-  Không có bảo mật HTTPS hoặc biểu tượng ổ khóa
-  Yêu cầu nhập thông tin cá nhân, OTP lạ

ỨNG DỤNG GIẢ MẠO



-  Không có trên App Store hoặc CH Play
-  Biểu tượng, tên gần giống ứng dụng thật
-  Đòi quyền truy cập bất thường
-  Giao diện sơ sài, lỗi chính tả, quảng cáo lạ



TÀI KHOẢN MẠNG XÃ HỘI ĐÁNG NGỜ



Mới tạo, ít bạn bè, hoạt động lạ



Ảnh mờ, thiếu thông tin cá nhân



Nhắn tin mượn tiền, gửi link lạ



Gọi điện, nhắn tin nhờ chuyển tiền

NGUỒN THÔNG TIN GIẢ MẠO



Không rõ nguồn phát hành



Ngôn từ giật gân, thiếu dẫn chứng



Link lạ, không có trên báo chí



Nội dung sai lệch, khó kiểm chứng



III. XỬ LÝ KHI GẶP LỪA ĐẢO

EXIMBANK



Xử lý khi gặp lừa đảo trực tuyến



- Lưu lại bằng chứng,
- Chặn tin nhắn, cuộc gọi lừa đảo



Báo cơ quan công an gần nhất



Tổ giám qua VN-ID

Trường hợp đã chuyển tiền cho kẻ lừa đảo



Ngừng ngay việc chuyển tiền



Báo ngân hàng, yêu cầu dừng giao dịch



Ghi lại bằng chứng giao dịch



Cảnh báo người thân, bạn bè

Báo cơ quan công an gần nhất

Bị mất tài khoản/mất quyền thiết bị



Yêu cầu ngân hàng khóa tài khoản



Đổi mật khẩu, xác thực 2 bước



Theo dõi tài khoản ngân hàng



Quét thiết bị bằng phần mềm bảo mật



Báo cơ quan công an gần nhất



Tổ giám qua VN-ID



QUY TẮC 6 “KHÔNG”

Bảo vệ bản thân trước các thủ đoạn lừa đảo trực tuyến

- 1 **KHÔNG** cung cấp thông tin cá nhân, địa chỉ, số điện thoại, số tài khoản ngân hàng của mình cho đối tượng không quen biết; thận trọng rà soát và kiểm tra kỹ thông tin trước khi thực hiện các giao dịch chuyển tiền.
- 2 **KHÔNG** kết bạn và nói chuyện với người lạ, đặc biệt là những tài khoản có hình ảnh ngoại hình đẹp và bắt mắt. Tuyệt đối không nhận lời mời tham gia các hội nhóm mà không rõ mục đích đối tượng.
- 3 **KHÔNG** truy cập, đăng nhập vào các đường dẫn, liên kết, website, ứng dụng hoặc mở tệp đính kèm đến từ người gửi không xác định, không rõ nguồn gốc.
- 4 **KHÔNG** cán bộ Cơ quan Nhà nước, Bộ Công an, Viện Kiểm sát, Tòa án hay đơn vị tài chính... nào gọi điện để điều tra qua điện thoại, yêu cầu phải cung cấp thông tin cá nhân hay đóng tiền.
- 5 **KHÔNG** thực hiện chuyển khoản trước; tuyệt đối không đặt cọc, chuyển khoản tiền cho các đối tượng lạ trong bất cứ trường hợp nào.
- 6 **KHÔNG** tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một cách dễ dàng, những lợi nhuận "phi thực tế" mà không tốn sức lao động, những lời mời, dụ dỗ “việc nhẹ lương cao”...



Bảo vệ thông tin cá nhân



Không chia sẻ thông tin cá nhân cho người lạ



Không lưu thông tin nhạy cảm trên thiết bị không bảo mật



Cảnh giác với email, tin nhắn, cuộc gọi lạ



Thường xuyên kiểm tra và cập nhật bảo mật thiết bị



Kiểm tra nguồn gốc thông tin trước khi cung cấp



Cẩn trọng khi tham gia hội nhóm, kết bạn qua mạng xã hội



Không cung cấp OTP, mật khẩu, mã xác thực



Cảnh giác khi kết nối qua mạng xã hội



Không kết bạn với người lạ không rõ danh tính



Báo cáo tài khoản nghi ngờ lừa đảo hoặc giả mạo



Không chia sẻ thông tin cá nhân, tài chính



Thiết lập quyền riêng tư cho tài khoản mạng xã hội



Thận trọng với lời mời tham gia nhóm lạ



Không nhấp vào liên kết từ người lạ

Công an địa phương gần nhất



- Website UBND xã/phường: tra cứu mục Liên hệ hoặc Thông tin cán bộ.
- Bảng thông tin công cộng tại UBND hoặc công an xã.
- Tổng đài địa phương: tiếp nhận phản ánh và chuyển đến công an xã/phường.

Ngân hàng hoặc ví điện tử có liên quan



- Liên hệ tổng đài chăm sóc khách hàng hoặc đến trực tiếp ngân hàng liên quan.
- Liên hệ bộ phận hỗ trợ của ví điện tử liên quan.
- **Tổng đài DVKH 24/7 Eximbank: 1900 6655**

Cơ quan an ninh mạng và phòng chống tội phạm công nghệ cao



- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (PA05).

Báo cáo qua ứng dụng VneID



1. Đăng nhập ứng dụng VNeID.
2. Chọn **Dịch vụ khác** → *Kiến nghị, phản ánh*.
3. Tạo mới yêu cầu, điền thông tin (có thể chọn **Ẩn danh**).
4. Đính kèm bằng chứng (nếu có).
5. Xác nhận và gửi.

EXIMBANK



CHUNG TAY PHÒNG, CHỐNG LỪA ĐẢO TRỰC TUYẾN

Ngân hàng thương mại cổ phần Xuất Nhập khẩu Việt Nam
Tổng đài DVKH 24/7: 1900 6655, Email: contact@eximbank.com.vn