NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
TRƯỜNG ĐẠI HỌC NGÂN HÀNG
TP. HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 552/TB-ĐHNH

Tp. Hồ Chí Minh, ngày 15 tháng 4 năm 2026

THÔNG BÁO
V/v phòng ngừa các phương thức, thủ đoạn lừa đảo, bắt cóc sinh viên qua mạng

Thời gian qua, trên địa bàn TP. Hồ Chí Minh liên tục xảy ra các vụ lừa đảo trên không gian mạng theo hình thức "bắt cóc online", tập trung nhắm vào học sinh, sinh viên với nhiều thủ đoạn tinh vi, gây hoang mang dư luận. Phần lớn nạn nhân sau khi được cơ quan Công an giải cứu rơi vào khủng hoảng tâm lý, có biểu hiện trầm cảm, sợ hãi hoặc xin nghỉ học. Một số trường hợp phụ huynh hoảng loạn, chuyển tiền theo yêu cầu của đối tượng, gây thiệt hại lớn. Trước tình hình đó, thực hiện các văn bản tuyên truyền, hướng dẫn của Phòng Cảnh sát hình sự - Công an Thành phố Hồ Chí Minh, Trường Đại học Ngân hàng TP. Hồ Chí Minh tiếp tục thông báo tới toàn bộ sinh viên của Trường cần cảnh giác với các thủ đoạn lừa đảo, chiếm đoạt tài sản. Sinh viên cần đọc kỹ các nội dung chi tiết như sau:

I. CÁC THỦ ĐOẠN LỪA ĐẢO

Các thủ đoạn lừa đảo thường được thể hiện dưới các hình thức sau:

1. Giả danh Công an, cơ quan nhà nước:

- Bước 1: cuộc gọi mạo danh nhân viên giao hàng

Mục đích kẻ xấu: Thu thập thông tin cá nhân, tạo niềm tin ban đầu.

Hành vi kẻ xấu: Gọi/Zalo/FB, tự xưng là shipper/bưu điện thông báo "đơn hàng 0 đồng" hoặc quà tặng.

Phản ứng nạn nhân: Tò mò, xác nhận thông tin, gửi họ tên, số điện thoại, địa chỉ, ảnh CMND/CCCD.

Hành động ngay (cần làm): Không cung cấp ảnh giấy tờ; hỏi lại kênh chính thức của đơn vị giao hàng; không nhấn các link lạ.

Bằng chứng cần lưu: Ghi âm cuộc gọi, chụp màn hình tin nhắn, lưu số điện thoại liên hệ.

- Bước 2: giả danh cán bộ Công an

Mục đích kẻ xấu: Gây sợ và kiểm soát tâm lý bằng quyền lực "Công an".

Hành vi kẻ xấu: Gọi từ số lạ, xưng là cán bộ Công an, đọc đúng họ tên, năm sinh, trường học; phát video dựng sẵn "cuộc làm việc", dẫn chứng đặc điểm nhận dạng (nốt ruồi, sẹo…), khẳng định nạn nhân "liên quan vụ án".

Phản ứng nạn nhân: Hoảng loạn, cố gắng chứng minh vô tội, làm theo chỉ dẫn.

Hành động ngay (cần làm): Giữ bình tĩnh, không cung cấp thêm thông tin; yêu cầu số hiệu/đơn vị và gọi lại qua số đường dây chính thức của Công an để xác minh. Đồng thời thông báo ngay cho người thân trong gia đình để biết.

Bằng chứng cần lưu: Ghi âm, chụp ảnh màn hình, lưu số gọi đến.

- Bước 3: Ép buộc tới nơi vắng, cấm liên lạc

Mục đích kẻ xấu: Cô lập nạn nhân, loại bỏ khả năng can thiệp từ gia đình hoặc cơ quan thật.

Hành vi kẻ xấu: Yêu cầu nạn nhân đến khách sạn/nhà nghỉ để "làm việc bảo mật"; cấm liên lạc, dọa bắt nếu tiết lộ.

Phản ứng nạn nhân: Sợ hãi, tuân theo, tự cách ly trong phòng; không nghe máy người thân.

Hành động ngay (cần làm): Nếu có thể, thông báo ngay cho gia đình vị trí; cố gắng giữ liên lạc an toàn; ghi nhận tên/địa chỉ nơi được yêu cầu đến.

Bằng chứng cần lưu: Tin nhắn hẹn địa điểm, địa chỉ khách sạn, thời gian đến.

- Bước 4: Quay video "khám xét" xâm phạm riêng tư

Mục đích kẻ xấu: Tạo video nhạy cảm dùng để uy hiếp và tống tiền.

Hành vi kẻ xấu: Bắt quay cận nốt ruồi, vết sẹo, hướng dẫn "công an nữ kiểm tra"; ép quay những cảnh xâm phạm.

Phản ứng nạn nhân: Xấu hổ, bị ép làm theo để "giải thích" hoặc "chứng minh".

Hành động ngay (cần làm): Tuyệt đối không quay những cảnh nhạy cảm; nói rõ bạn chỉ hợp tác khi có cán bộ thật và gia đình; cố gắng quay lại màn hình cuộc gọi để lưu chứng cứ (không thực hiện yêu cầu xâm phạm)

Bằng chứng cần lưu: File cuộc gọi/video, lịch sử cuộc gọi, ảnh chụp màn hình hướng dẫn quay.

- Bước 5: Dựng kịch bản nộp tiền điều tra (tống tiền)

Mục đích kẻ xấu: Chiếm đoạt tài sản bằng cách đe dọa tạm giam/khởi tố nếu không nộp phí.

Hành vi kẻ xấu: Yêu cầu nộp "phí điều tra" hoặc "phí bảo lãnh" bắt đầu bằng một khoản (ví dụ 250 triệu), sau đó leo thang. Dọa tạm giam nếu không nộp.

Phản ứng nạn nhân/gia đình: Lo lắng, tìm cách vay tiền, chuyển khoản vội vàng.

Hành động ngay (cần làm): Không chuyển tiền; liên hệ kênh chính thức của nhà trường và Công an để xác minh; báo cho ngân hàng nếu đã chuyển

Bằng chứng cần lưu: Giấy tờ/biên nhận giả, số tài khoản người nhận, tin nhắn/ghi âm đe dọa.

- Bước 6: Quay video "bắt cóc" gửi cho gia đình, uy hiếp tống tiền

Mục đích kẻ xấu: Tạo nỗi kinh hoàng cho gia đình để ép chuyển tiền.

Hành vi kẻ xấu: Hướng dẫn nạn nhân quay video giả bị bắt cóc (trói, la hét, nêu tên bố mẹ, yêu cầu số tiền) và gửi cho gia đình; kèm lời đe dọa "chuyển tiền ngay hoặc làm hại".

Phản ứng gia đình: Hoảng loạn, vội chuyển tiền.

Hành động ngay (cần làm): Gia đình cần bình tĩnh: gọi lại cho con qua số khác để xác minh; đưa bằng chứng tới Công an; không chuyển tiền ngay, xác minh qua cơ quan chức năng.

Bằng chứng cần lưu: Đoạn video, tin nhắn kèm yêu cầu, lịch sử chuyển khoản (nếu đã chuyển).

- Bước 7: Gia đình chuyển tiền - kẻ xấu cắt liên lạc, hậu quả

Mục đích kẻ xấu: Hoàn tất chiếm đoạt tài sản và trốn tránh.

Hành vi kẻ xấu: Nhận tiền, chặn số, xóa liên lạc, rút tiền.

Phản ứng sau cùng: Nạn nhân được tìm thấy hoảng loạn; gia đình mất tiền; vụ việc chỉ sáng tỏ khi nhà trường hoặc Công an vào cuộc.

Hành động ngay (cần làm): Khi phát hiện bị lừa - báo ngay Công an, cung cấp mọi chứng cứ; liên hệ ngân hàng để truy vết, nếu kịp thời yêu cầu phong tỏa tài khoản nhận.

Bằng chứng cần lưu: Toàn bộ lịch sử giao dịch, số tài khoản nhận, toàn bộ tin nhắn và video.

2. Diễn biến vụ việc theo các bước cụ thể Giả mạo tổ chức cấp học bổng, chương trình du học quốc tế cho sinh viên:

- Bước 1: Thông báo "danh sách mật"

Mục đích kẻ xấu: Thu thập và xác thực thông tin cá nhân; tạo niềm tin ban đầu bằng "thông tin nội bộ".

Hành vi kẻ xấu: Liên hệ qua Zalo/FB/điện thoại, tự xưng cán bộ Phòng Hợp tác Quốc tế; thông báo "17 suất học bổng/danh sách mật"; sử dụng thông tin thật của nạn nhân để tăng độ tin cậy.

Phản ứng sau cùng: Nạn nhân tin tưởng, cung cấp thêm thông tin cá nhân và chấp nhận các hướng dẫn tiếp theo.

Hành động ngay (cần làm): Không cung cấp ảnh CMND/CCCD hay thông tin nhạy cảm; hỏi lại kênh chính thức của nhà trường; báo cho phụ huynh/trường về cuộc liên hệ lạ.

Bằng chứng cần lưu: Chụp màn hình tin nhắn, ghi âm cuộc gọi, lưu số điện thoại/ID Zalo/Facebook, lưu các file đối tượng gửi.

- Bước 2: Tạo lòng tin và khơi gợi lòng tham

Mục đích kẻ xấu: Kích thích ham muốn được hưởng ưu đãi, khiến nạn nhân chủ động hợp tác tài chính.

Hành vi kẻ xấu: Nhấn mạnh "ít suất, danh sách mật, chỉ dành cho ưu tú"; hứa giữ suất nếu nộp phí bảo lưu với số tiền lớn.

Phản ứng sau cùng: Nạn nhân lo sợ mất cơ hội, quyết tâm nộp tiền để bảo đảm suất.

Hành động ngay (cần làm): Bình tĩnh xác minh qua phòng Công tác HSSV hoặc Phòng Hợp tác Quốc tế chính thức; không chuyển tiền ngay.

Bằng chứng cần lưu: Tin nhắn/giấy tờ hứa hẹn, hướng dẫn chuyển tiền, nội dung trao đổi.

- Bước 3: Yêu cầu chuyển tiền lần 1

Mục đích kẻ xấu: Thu tiền lần đầu, hợp thức hóa lòng tin bằng "ghi nhận" đã vào danh sách.

Hành vi kẻ xấu: Gửi hướng dẫn chuyển khoản vào tài khoản cá nhân/ví điện tử (gọi là "tài khoản ký quỹ"); gửi thư mời, danh sách 17 tên, con dấu/ chữ ký giả.

Phản ứng sau cùng: Nạn nhân chuyển tiền và tin rằng đã được ghi danh chính thức.

Hành động ngay (cần làm): Trước khi chuyển, xác minh số tài khoản với nhà trường; nếu đã chuyển — lưu biên lai, liên hệ ngân hàng và công an ngay.

Bằng chứng cần lưu: Biên lai chuyển tiền, số tài khoản nhận, nội dung thư mời/ danh sách giả, lịch sử chat.

- Bước 4: Đưa ra yêu cầu mới

Mục đích kẻ xấu: Tạo áp lực tài chính lớn, lôi kéo nạn nhân/gia đình vào vòng tống tiền liên tục.

Hành vi kẻ xấu: Thông báo cần chứng minh tài chính với số tiền để hoàn tất thủ tục; hứa hoàn trả và cung cấp "biên bản/giấy tờ đảm bảo".

Phản ứng sau cùng: Nạn nhân lo lắng, cảm thấy bị dồn vào chân tường; tìm cách vay mượn, cầu cứu gia đình.

Hành động ngay (cần làm): Tuyệt đối không chuyển thêm; yêu cầu kiểm tra xác thực giấy tờ qua kênh chính thức; báo công an khi yêu cầu bất hợp pháp.

Bằng chứng cần lưu: Mọi văn bản, email, biên bản giả, số tài khoản mới, lời cam kết bằng tin nhắn/ghi âm.

- Bước 5: Dựng hồ sơ và hợp thức hóa giấy tờ

Mục đích kẻ xấu: Tăng độ tin cậy bằng bằng chứng "chính quy" giả, giảm nghi ngờ của nạn nhân.

Hành vi kẻ xấu: Gửi file PDF, văn bản có logo/con dấu/chữ ký giả; sử dụng email có domain gần giống trường; biện minh quy trình là "bắt buộc, nội bộ".

Phản ứng sau cùng: Nạn nhân tin tưởng hơn, chấp nhận yêu cầu tiếp theo.

Hành động ngay (cần làm): So sánh hồ sơ với mẫu chính thức của trường;

gọi điện vào số hotline của trường để xác minh; không tin email/số điện thoại do bên lạ cung cấp.

Bằng chứng cần lưu: File PDF, header email, metadata file, địa chỉ email gửi, bản in giấy tờ giả.

- Bước 6: Gia tăng áp lực khi nạn nhân không có tiền

Mục đích kẻ xấu: Áp dụng chiến thuật đe dọa tâm lý để buộc nạn nhân hoặc gia đình phải nộp tiền.

Hành vi kẻ xấu: Dọa mất suất, bị loại, bị xử lý pháp lý; đề nghị "phương án thay thế" là yêu cầu nạn nhân tự quay video giả bị giam/bắt cóc để gửi cho gia đình.

Phản ứng sau cùng: Nạn nhân chịu áp lực, làm theo hướng dẫn (quay video, tỏ ra chịu đựng) hoặc cố tìm tiền.

Hành động ngay (cần làm): Không làm theo yêu cầu quay video; liên hệ gia đình và công an thật; ghi lại nội dung đe dọa; giữ bình tĩnh.

Bằng chứng cần lưu: Tin nhắn đe dọa, hướng dẫn quay video, thời gian/góc quay, số liên hệ kẻ xấu.

- Bước 7: Dùng video để uy hiếp từ đó tống tiền gia đình

Mục đích kẻ xấu: Gây hoảng loạn cho gia đình để ép chuyển tiền lập tức.

Hành vi kẻ xấu: Gửi video (do nạn nhân quay) cho cha mẹ, kèm lời đe dọa "chuyển tiền ngay nếu không sẽ làm hại/đưa ra nước ngoài".

Phản ứng sau cùng: Gia đình hoảng sợ, vội chuyển tiền hoặc làm theo yêu cầu.

Hành động ngay (cần làm): Gia đình cần gọi lại con bằng số điện thoại khác để kiểm tra thực tế; báo công an, không chuyển tiền ngay; đưa bằng chứng đến cơ quan chức năng.

Bằng chứng cần lưu: Video, tin nhắn tống tiền, số tài khoản yêu cầu chuyển, lịch sử cuộc gọi.

- Bước 8: Kết thúc chiếm đoạt và trốn tránh

Mục đích kẻ xấu: Hoàn tất chiếm đoạt tài sản rồi xóa dấu vết, trốn tránh truy tố.

Hành vi kẻ xấu: Nhận tiền, chặn số, xóa tài khoản, rút tiền; có thể tiếp tục yêu cầu thêm nếu còn đường liên lạc.

Phản ứng sau cùng: Nạn nhân hoảng loạn, gia đình mất tiền; vụ việc chỉ sáng tỏ khi nhà trường hoặc Công an xác minh.

Hành động ngay (cần làm): Ngay lập tức báo Công an, cung cấp toàn bộ bằng chứng; liên hệ ngân hàng yêu cầu phong tỏa/tìm tiền; nhà trường phát thông báo cảnh báo cộng đồng.

Bằng chứng cần lưu: Toàn bộ lịch sử chuyển khoản, số tài khoản nhận, tin nhắn, email, bản in giấy tờ giả, ghi âm cuộc gọi.

II. NHỮNG VIỆC SINH VIÊN CẦN LÀM

1. Sinh viên phải đọc hết và đọc kỹ các nội dung về thủ đoạn lừa đảo nói trên.

2. Sinh viên gửi thông báo này tới phụ huynh để phụ huynh cùng đọc.

III. THÔNG TIN LIÊN HỆ

- **Thông tin chính thức:** Mọi thông tin chính thức của Nhà trường đều được đăng tải trên website của Trường (https://hub.edu.vn/) và cổng thông tin sinh viên (https://online.hub.edu.vn/).
- **Liên hệ:** Trong trường hợp cần thiết, sinh viên và phụ huynh có thể liên hệ với Trường qua số điện thoại của các đơn vị được liệt kê ***tại đây***.
- Khi phát hiện hoặc nghi ngờ trường hợp "bắt cóc online", sinh viên, học viên, phụ huynh sinh viên, học viên có thể gọi trực tiếp đến số điện thoại 0693.187.200, (PC02 - Phòng Cảnh sát hình sự Công an TP.HCM) hoặc 028.3821.7080 (Đội 2, Phòng Cảnh sát hình sự Công an TP.HCM) để được hỗ trợ kịp thời.

Trân trọng./.

Nơi nhận:
- Ban Giám hiệu (để b/c);
- Các đơn vị (để thông báo);
- Sinh viên, học viên;
- Phụ huynh SV, HV;
- Lưu: TTSV&QHDN, VP.

TL. HIỆU TRƯỞNG
KT. GIÁM ĐỐC TRUNG TÂM SV&QHDN

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
TRƯỜNG ĐẠI HỌC NGÂN HÀNG THÀNH PHỐ HỒ CHÍ MINH

Hoàng Thị Tuyền