Cục Thuế TP Hà Nội:

CẨM NANG NHẬN DIỆN VÀ PHÒNG TRÁNH LỪA ĐẢO TRỰC TUYẾN

I. Lừa đảo cuộc gọi video Deepfake, Deepvoice

Deepfake, deep voice đang là một mối đe dọa đối với sự trung thực và tin cậy của video, hình ảnh và giọng nói. Thông qua các ứng dụng "Tổng cục thuế" giả mạo, các đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video, đoạn ghi âm hoặc hình ảnh giả, sao chép chân dung, giọng nói, tạo ra các đoạn video giả mạo cán bộ thuế để lừa đảo.

Phần lớn hình thức lừa đảo trực tuyến này nhắm tới việc lừa đảo tài chính để thực hiện nghĩa vụ với NSNN. Nên khi người nộp thuế nhận được các cuộc gọi liên quan đến các nội dung yêu cầu thực hiện nghĩa vụ thuế, đề nghị cung cấp thông tin cá nhân, MST, tài khaorn giao dịch thuế điện tử thì nên bình tĩnh, cảnh giác, tỉnh táo xác nhận thêm.

- **Dấu hiệu nhận biết:**

- Thời gian gọi thường ngắn.

- Khuôn mặt thiếu tính cảm xúc và khá "trơ" khi nói, hoặc tư thế trông lúng túng, không tự nhiên, hoặc là hướng đầu và cơ thể trong video không nhất quán với nhau…

- Màu da của nhân vật trong video bất thường, ánh sáng kỳ lạ và bóng đổ không đúng vị trí. Điều này có thể khiến cho video trông rất giả tạo và không tự nhiên.

- Âm thanh không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.

- Ngắt giữa chừng, bảo là mất sóng, sóng yếu... Yêu cầu chuyển tiền mà tài khoản chuyển tiền không phải của người đang thực hiện cuộc gọi.

- **Biện pháp phòng tránh:**

Nếu nhận được một cuộc gọi video hoặc cuộc gọi thông thường yêu cầu chuyển tiền nộp thuế gấp, trước tiên hãy bình tĩnh và xác minh thông tin:

- Người nộp thuế cần liên lạc trực tiếp với Cơ quan Thuế thông qua đường dây nóng được công bố trên website chính thức của ngành thuế khác kiểm tra lại thông tin có đúng là NNT nhận được thông báo, quyết định thực hiện nghĩa vụ thuế không.

- Không thực hiện chuyển tiền cho người lạ. Chỉ làm việc trực tiếp tại Cơ quan thuế hoặc các đơn vị được Cơ quan Thuế ủy quyền thu như Bưu điện Hà Nội.

- Lưu ý các cuộc gọi thoại hay video có chất lượng kém, chập chờn là một yếu tố để nghi ngờ người gọi cũng như tính xác thực của cuộc gọi.

II.Giả mạo trang thông tin điện tử, email Cơ quan Thuế

- **Dấu hiệu nhận biết:**

Các đối tượng lừa đảo có thể tạo trang web, email có giao diện, hình ảnh, nội dung gần giống của Cơ quan Thuế để người dùng nhầm tưởng là trang web, email do Cơ quan Thuế cung cấp. Sau đó, các đối tượng đính kèm nội dung yêu cầu người dùng phải truy cập vào liên kết giả mạo, khai báo thông tin cá nhân, tài khoản ngân hàng và từ đó thực hiện hành vi đánh cắp, chiếm đoạt thông tin dữ liệu người dùng, lừa đảo.

* **Dấu hiệu nhận biết website, email không an toàn**

- Đường dẫn URL trên thanh địa chỉ của trình duyệt không kết thúc bằng đuôi "gdt.gov.vn". VD như: "gdtgov.cfd"

- Những website không đáng tin cậy và kém an toàn thông thường không được chú trọng nhiều về nội dung, thông tin đăng tải cẩu thả, sai lỗi chính tả,… do các website lừa đảo thường không có thời gian kỹ càng để kiểm duyệt và chỉnh sửa các nội dung.

- Các website lừa đảo thường sẽ xuất hiện những cảnh báo, đe dọa hoặc nhắc hạn (khai nộp thuế, quyết toán thuế,…) ngay khi người dùng truy cập trang, mục đích là để đánh lừa và dụ dỗ người dùng điền các thông tin quan trọng nhằm đánh cắp dữ liệu cá nhân, hoặc điều hướng truy cập đến những website không an toàn khác có chứa mã độc hại. Do đó, người nộp thuế cần bình tĩnh, cảnh giác và không thực hiện theo yêu cầu.

*** Biện pháp phòng tránh**

- Kiểm tra địa chỉ URL: Luôn kiểm tra URL của trang web trước khi cung cấp thông tin cá nhân.

+ Địa chỉ URL của Tổng cục Thuế: https://www.gdt.gov.vn/wps/portal

+ Địa chỉ URL của Cổng thông tin điện tử của Tổng cục Thuế: https://thuedientu.gdt.gov.vn

+ Địa chỉ URL của Cục Thuế TP Hà Nội: https://hanoi.gdt.gov.vn/wps/portal

- Sử dụng trình duyệt an toàn: Sử dụng trình duyệt web có tính năng bảo mật cao và cập nhật phiên bản mới nhất như: Google Chrome, Mozilla Firefox và Safari thường có các cơ chế bảo mật tích hợp giúp ngăn chặn truy cập vào trang web độc hại.

- Cẩn thận với email và liên kết: Người nộp thuế tuyệt đối không tải hoặc cài đặt ứng dụng của Cơ quan thuế cho máy tính qua các đường dẫn không phải do Tổng cục Thuế , Cục Thuế cung cấp.

- Không cho phép bất kỳ cá nhân nào truy cập trực tiếp vào máy tính của mình để hỗ trợ cài đặt, sử dụng phần mềm của cơ quan thuế,... Tránh nhấp vào liên kết trong email không xác định, kiểm tra nguồn gốc của email (đuôi email là *@gdt.gov.vn*) và đảm bảo rằng nó là đáng tin cậy trước khi tiếp tục.

- Không cung cấp tên, số điện thoại, email, mã số thuế, tài khoản giao dịch điện tử,…qua điện thoại, email, mạng xã hội và các trang web khác. Chỉ sử dụng dịch vụ thuế điện tử thông qua website chính thức của cơ quan thuế. Các website chính thức của cơ quan thuế thường sử dụng giao thức https và kết thúc bằng đuôi gdt.gov.vn.

- Sử dụng phần mềm bảo mật: Cài đặt và duy trì phần mềm diệt virus, phần mềm chống độc, tường lửa và các công cụ bảo mật khác trên thiết bị máy tính/di động. Cập nhật thường xuyên để bảo vệ chống lại các mối đe dọa mới nhất.

- Giữ tỉnh táo và cảnh giác: Luôn truy cập vào trang web chính thức của Cơ quan Thuế và thực hiện các thay đổi thông qua đó, thay vì truy cập qua liên kết trong email hoặc thông báo không xác định.

- Đừng dễ tin vào thông báo đột xuất: Cẩn thận với các thông báo đột xuất yêu cầu cập nhật thông tin cá nhân hoặc yêu cầu thay đổi mật khẩu, hay các thông báo nộp thuế.

- Báo cáo các trang web phishing: Nếu phát hiện một trang web phishing, hãy báo cáo, phản ánh kịp thời cho Cơ quan Thuế theo số điện thoại đường dây nóng hoặc cơ quan chức năng có thẩm quyền để họ có thể đối phó với tình huống đó và ngăn chặn người khác trở thành nạn nhân tiếp theo.

III. Lừa đảo dịch vụ hỗ trợ nộp NSNN/ lấy lại tiền khi bị nộp thừa vào NSNN

Hiện nay trên các nền tảng mạng xã hội cũng đã xuất hiện hình thức lừa đảo đáng chú ý đó là lừa đảo dịch vụ hỗ trợ nộp NSNN/lấy lại tiền khi bị nộp thừa vào NSNN.

- **Dấu hiệu nhận biết:**

- Tạo một danh tính giả: kẻ lừa đảo sẽ xây dựng hình tượng của các Công chức Thuế để người nộp thuế có thể tin tưởng (liên hệ qua Facebook, zalo cá nhân). Điều này có thể liên quan đến việc tạo các hồ sơ giả, trang web giả hoặc tài liệu giả để đánh lừa người nộp thuế. Qua đó, đề nghị cung cấp dịch vụ hỗ trợ nộp NSNN hoặc lấy lại tiền khi bị nộp thừa vào NSNN.

- Yêu cầu thanh toán hoặc thông tin nhạy cảm: Sau khi tạo dựng niềm tin, đối tượng lừa đảo sẽ yêu cầu thanh toán dưới hình thức giả danh phí xử lý, yêu cầu pháp lý hoặc bất kỳ lý do hợp lý nào khác.

- Tiếp tục giả mạo, cung cấp thông tin cập nhật và sự đảm bảo để giữ cho nạn nhân tham gia và ngăn họ nghi ngờ ý đồ thật sự của kẻ lừa đảo.

*** Biện pháp phòng tránh:**

- Không chuyển tiền ngay lập tức: Mọi người hãy luôn kiểm tra và xác nhận rõ ràng nguồn gốc và mục đích của giao dịch chuyển tiền trước khi thực hiện. Không chuyển tiền dựa trên các đề nghị đột xuất, không xác định hoặc không rõ ràng.

- Kiểm tra thông tin chuyển khoản: Kiểm tra kỹ các thông tin liên quan đến người nhận và số tài khoản trước khi thực hiện giao dịch chuyển tiền. So sánh thông tin với nguồn tin chính thức hoặc thông qua ngân hàng chủ quản để đảm bảo tính xác thực.

- Xác minh danh tính: Khi bạn nhận được cuộc gọi, tin nhắn hoặc yêu cầu thông tin cá nhân qua điện thoại, hãy xác minh danh tính của người gọi bằng cách yêu cầu thông tin địa chỉ, số điện thoại liên hệ hoặc liên lạc lại qua một kênh tin cậy khác.

- Báo cáo sự việc: Nếu bạn nghi ngờ hoặc trở thành nạn nhân bị lừa đảo, hãy ngay lập tức báo cáo sự việc cho cơ quan chức năng như: Cơ quan Thuế, Cơ quan Công an hoặc ngân hàng, để họ tiến hành điều tra và cung cấp sự hỗ trợ.

- Luôn luôn giữ cảnh giác và không đồng ý thực hiện bất kỳ giao dịch tài chính nào mà không có đầy đủ thông tin và xác minh. Bảo vệ thông tin tài chính cá nhân của bạn và tìm hiểu thêm về các hình thức lừa đảo phổ biến để tránh trở thành nạn nhân

IV. Phát tán tin nhắn giả danh cơ quan thuế để trục lợi

• Dấu hiệu nhận biết:

Tình trạng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo, mạo danh cơ quan thuế đang có chiều hướng gia tăng mức độ, tần suất liên tục. Các đối tượng không chỉ sử dụng nhiều đầu số di động, mà còn sử dụng tin nhắn giả mạo Cơ quan Thuế với nội dung: thông báo quyết định xử phạt, thông báo thời hạn kê khai nộp thuế, … để người nộp thuế truy cập vào các ứng dụng hoặc các trang web của cơ quan thuế với mục đích lừa đảo, chiếm đoạt tiền.

Các điện thoại với tính năng tự động kết nối vào các trạm BTS có cường độ sóng mạnh, do cơ chế này nên các máy điện thoại tự động kết nối vào trạm BTS giả đang phát 2G ở gần. Các đối tượng đem thiết bị lên ô tô hoặc xe máy để di chuyển

đến những nơi đông người, phát tán tin nhắn tới những thuê bao kết nối vào trạm BTS giả.

- **Biện pháp phòng tránh**

- Để chủ động ngăn chặn tình trạng này, mỗi người nộp thuế phải trang bị đầy đủ các kiến thức, thông tin liên quan đến các hình thức mạo danh cơ quan thuế; đồng thời tham khảo các khuyến cáo trên các trang Thông tin điện tử của Cục Thuế TP Hà Nội để phòng tránh sập bẫy lừa đảo.

- Cơ quan thuế khẳng định không ủy quyền cho bất cứ công ty hoặc cá nhân ngoài ngành Thuế nào thực hiện thu thuế hộ (trừ hệ thống bưu điện được ủy quyền thu thuế hộ kinh doanh). Cơ quan thuế không yêu cầu người nộp thuế cung cấp thông tin cá nhân thông qua SMS, email, zalo, facebook, phần mềm chat,... Bởi vậy, việc xuất hiện các tin nhắn có nội dung **"**cơ quan thuế yêu cầu cung cấp thông tin cá nhân của người nộp thuế" là điều bất thường.

- Hãy đọc kỹ nội dung tin nhắn, kiểm tra các lỗi chính tả, xem xét một cách tỉnh táo, cẩn thận, không vội vã trả lời hay thực hiện yêu cầu theo nội dung trong tin nhắn. Khi nhận được tin nhắn hoặc thông báo lạ, người nộp thuế cần liên hệ lại với cán bộ thuế theo số điện thoại được công bố trên trang Thông tin điện tử của Cục Thuế TP Hà Nội (https://hanoi.gdt.gov.vn) để xác thực tại thông tin.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ tự xưng là cơ quan thuế; không đăng nhập tài khoản giao dịch điện tử, tài khoản eTax Mobile cá nhân vào những địa chỉ này.

- Ngoài ra, người nộp thuế cần lưu lại các bằng chứng như tin nhắn hoặc ghi âm cuộc gọi, phản ánh tới doanh nghiệp viễn thông quản lý thuê bao để yêu cầu xử lý, đồng thời cung cấp các bằng chứng đã có tới các Cơ quan Công an và Cơ quan Thuế gần nhất đề nghị xử lý hành vi sai phạm của các đối tượng theo quy định pháp luật.

V. Giả danh Cơ quan Thuế gọi điện, lừa đảo nộp NSNN, Quyết định xử phạt

Đối tượng tự xưng danh (mạo danh, giả danh) là cán bộ, công chức của cơ quan Thuế các cấp (Tổng cục Thuế, Cục Thuế, Chi cục Thuế) yêu cầu người nộp thuế nộp tiền vào ngân sách nhà nước, nộp tiền theo quyết định xử phạt. Ngoài ra, có trường hợp các đối tượng lừa đảo mời chào, dụ dỗ doanh nghiệp mua sách, tài liệu, cẩm nang về thuế hoặc các ấn phẩm vinh danh doanh nghiệp, lập quỹ hỗ trợ của ngành thuế, ….

- **Dấu hiệu nhận diện:**

- Sử dụng số điện thoại giả mạo: Đối tượng sẽ sử dụng các số điện thoại giả mạo như: các số điện thoại: **097.972.6956; 0911289086; 0932.472.015;**

0372.490.193; 0906.237.207; 0904.947.468; 0962.170.568; 0971.353.069; 0911.698.356; 0946.100.620; 0966.217.199; 0394.714.349; 0964.364.282;... Những số điện thoại này có thể hiển thị dưới dạng tên gọi "Cơ quan thuế" trên màn hình điện thoại của người nộp thuế.

- Đe dọa và áp lực tâm lý: Đối tượng sẽ sử dụng các cách thức đe dọa, áp lực tâm lý như khống chế, hăm dọa về việc người nộp thuế có liên quan đến hành vi chậm nộp thuế, nợ thuế, trốn thuế,… hoặc các vụ án hình sự về thuế đang được điều tra để tạo áp lực và đánh vào sợ hãi của họ.

- Yêu cầu chuyển tiền hoặc thông tin cá nhân: Đối tượng sẽ yêu cầu người nộp thuế chuyển tiền vào một tài khoản của cá nhân hoặc cung cấp thông tin cá nhân người nộp thuế như tên, số điện thoại, email, mã số thuế, tài khoản giao dịch điện tử,...

- Tạo áp lực thời gian: Đối tượng thường tạo áp lực thời gian cho người nộp thuế, tuyên bố rằng họ phải nộp tiền ngay lập tức cho hành vi vi phạm thủ tục hành chính về thuế để tránh hậu quả nghiêm trọng. Chúng sẽ cố gắng thuyết phục người nộp thuế rằng không có thời gian để suy nghĩ hay tham khảo.

- **Biện pháp phòng tránh:**

- Giữ bình tĩnh, nâng cao cảnh giác và không bị đánh lừa bởi áp lực tâm lý và đe dọa.

- Không cung cấp thông tin cá nhân, mã số thuế, tài khoản giao dịch điện tử, tiền bạc, tài sản,… qua điện thoại, email, mạng xã hội, các trang web không rõ nguồn gốc hoặc các phương tiện truyền thông khác.

- Báo cáo sự việc: Nếu bạn nhận được cuộc gọi đe dọa hoặc nghi ngờ có dấu hiệu lừa đảo, hãy thông báo ngay cho cơ quan công an địa phương để được hỗ trợ và tư vấn.

- Cơ quan Thuế khẳng định không có chủ trương, cũng như không cử cán bộ gọi điện thoại, fax,… yêu cầu bạn chuyển tiền nộp phạt cho hành vi vi phạm thủ tục hành chính về thuế, nộp tiền vào ngân sách nhà nước, hay cung cấp thông tin cá nhân qua điện thoại một cách đột ngột mà không có văn bản thông báo trước.

Ngoài ra, cơ quan Thuế khẳng định không mang sách đến bán cho người nộp thuế. Tất cả các văn bản, tài liệu được cơ quan Thuế cấp miễn phí và đăng tải đầy đủ trên website của cơ quan Thuế tại địa chỉ: https://hanoi.gdt.gov.vn. Các chương trình tập huấn của cơ quan Thuế tổ chức đều miễn phí và sẽ gửi giấy mời tới người nộp thuế.

VI. Chiếm quyền sử dụng điện thoại bằng đường link giả mạo

Thời gian gần đây, xuất hiện các đối tượng giả danh cán bộ thuế yêu cầu người dân truy cập vào các đường link giả mạo để chiếm quyền sử dụng điện thoại từ xa, sau đó lấy cắp thông tin cá nhân, thông tin tài khoản ngân hàng với mục đích chiếm đoạt tài sản.

- **Dấu hiệu nhận diện:**

Đối tượng lừa đảo hướng dẫn người nộp thuế thực hiện nghĩa vụ thuế bằng cách bấm vào một đường link gửi qua Zalo, Facebook,…Nếu thực hiện theo yêu cầu, ngay lập tức, các tính năng thông thường trên chiếc điện thoại của người dùng sẽ không thể sử dụng được nữa. Bằng cách này, các đối tượng chiếm quyền điều khiển điện thoại di động, máy tính của người dùng từ xa để thực hiện các thao tác: soạn, gửi tin nhắn SMS; mở khóa thiết bị di động; bật tắt mạng Internet, đọc, ghi danh bạ; tự thực hiện khôi phục mật khẩu tài khoản, tự đăng ký các dịch vụ Internet Banking, thay đổi hạn mức giao dịch của tài khoản, sau đó truy cập vào tài khoản, chuyển tiền của bị hại. Đặc biệt, các tin nhắn xác thực mã OTP, chuyển tiền, đều bị phần mềm gián điệp ẩn chuyển cho các đối tượng lừa đảo mà chủ điện thoại không hay biết.

- **Biện pháp phòng tránh:**

- Hãy đọc kỹ nội dung tin nhắn, kiểm tra các lỗi chính tả, xem xét một cách tỉnh táo, cẩn thận, không vội vã trả lời hay thực hiện yêu cầu theo nội dung trong tin nhắn. Khi nhận được tin nhắn hoặc thông báo lạ, người nộp thuế cần liên hệ lại với cán bộ thuế theo số điện thoại được công bố trên trang Thông tin điện tử của Cục Thuế TP Hà Nội để xác thực tại thông tin.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ tự xưng là cơ quan thuế hoặc không rõ nguồn gốc về ủy quyền đóng thuế, mua bán hóa đơn. Không đăng nhập tài khoản giao dịch điện tử, tài khoản eTax Mobile cá nhân vào những địa chỉ này.

- Để tránh tình trạng lừa đảo khi thực hiện giao dịch với cơ quan thuế hoặc thực hiện các nghiệp vụ về thuế, người nộp thuế có thể lên trực tiếp Cơ quan Thuế hoặc liên hệ cán bộ đầu mối của Cục Thuế, Chi cục Thuế trên địa bàn để được hỗ trợ qua số điện thoại được công bố trên trang Thông tin điện tử của Cục Thuế TP Hà Nội (https://hanoi.gdt.gov.vn).

PHÒNG TTHT NTT