|  |  |
| --- | --- |
| CÔNG AN TỈNH ĐỒNG NAI  **PHÒNG AN NINH MẠNG VÀ PHÒNG CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO** |  |

**NHẬN THỨC CHUNG VỀ AN NINH MẠNG VÀ**

**TÌNH HÌNH TỘI PHẠM LỪA ĐẢO TRỰC TUYẾN HIỆN NAY.**

**NHẬN DIỆN VÀ PHÒNG TRÁNH**

**I. CÁC KHÁI NIỆM VÀ NHẬN THỨC CHUNG**

**1. Một số khái niệm cơ bản liên quan công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao**

(1) **Không gian mạng** là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian (Khoản 3, Điều 2, Luật An ninh mạng).

Không gian mạng được xác lập từ 06 thành tố:

- Chính sách, pháp luật quy định các quy tắc ứng xử cho tổ chức, cá nhân khi tham gia không gian mạng, quy định các mối quan hệ giữa cơ quan quản lý nhà nước với tổ chức, cá nhân; giữa các quốc gia và tổ chức quốc tế, tạo hành lang pháp lý bảo đảm hoạt động an toàn và hiệu quả của không gian mạng, mở đường cho công nghệ phát triển an toàn.

- Năng lực công nghệ là khả năng sử dụng công nghệ sẵn có và nghiên cứu công nghệ mới tác động đến không gian mạng. Các loại công nghệ nền tảng, như công nghệ mạng (nếu không có công nghệ mạng, thì không có Internet, mạng viễn thông, truyền thông...), công nghệ điện tử, bán dẫn, vi xử lý (nếu không có công nghệ điện tử, bán dẫn, vi xử lý sẽ không có các nền tảng phần cứng), công nghệ phần mềm (nếu không có công nghệ phần mềm thì không có “linh hồn” cho máy tính và mạng máy tính hoạt động). Ngoài ra, còn có các quy định chuẩn công nghệ, các quy trình phương thức giao tiếp, giao diện giữa các tầng kiến trúc của công nghệ... Tất cả những điều đó nói lên khả năng sáng tạo và ứng dụng công nghệ do con người làm chủ, đóng vai trò cốt lõi trong việc tác động vào không gian mạng, năng lực công nghệ đủ mạnh là yếu tố nền tảng để làm chủ các hoạt động trên không gian mạng.

- Nội dung thông tin được lưu trữ, xử lý và trao đổi trên không gian mạng, làm nảy sinh các yêu cầu nghiệp vụ chuyên ngành hoặc nhu cầu xã hội, được thực hiện trên không gian mạng nhằm phục vụ cho mục đích nhất định. Nội dung thông tin sẽ quyết định không gian mạng của một ngành khoa học nà đó được tạo ra như thế nào, việc sử dụng và phát triển ra sao. Đây chính là định hướng cho sự phát triển không gian mạng.

- Nguồn nhân lực chính là con người được đào tạo bài bản, hoạt động chuyên biệt, hiểu biết pháp luật, nắm vững công nghệ và kiến thức, nghiệp vụ chuyên ngành. Một nguồn nhân lực như vậy sẽ luôn giành thế chủ động thế chủ động trên không gian mạng. Yếu tố nguồn nhân lực đóng vai trò quyết định cho mọi hoạt động của con người trên không gian mạng.

- Tổ chức bộ máy là hệ thống cơ quan quản lý nhà nước vận hành thông suốt từ khâu hạ tầng kỹ thuật đến dịch vụ ứng dụng, quản lý, bảo vệ và điều tiế chính sách, pháp luật trên không gian mạng. Vai trò của nó là kết nối một cách hiệu quả các yếu tố trên không gian mạng.

- Ý thức của người trên không gian mạng là sự tôn trọng chính sách pháp luật, chuẩn công nghệ, quy tắc nghiệp vụ. Ý thức con người quyết định tốc độ và xu hướng phát triển của không gian mạng.

(2) **An ninh mạng** là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân (Khoản 1, Điều 2, Luật An ninh mạng).

(3) **Bảo vệ an ninh mạng** là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng (Khoản 2, Điều 2, Luật An ninh mạng).

(4) **Tội phạm mạng** là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự (Khoản 7, Điều 2, Luật An ninh mạng).

(5) **Tấn công mạng** là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử (Khoản 8, Điều 2, Luật An ninh mạng).

(6) **Khủng bố mạng** là việc sử dụng không gian mạng, công nghệ thông từ hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bị (Khoản 9, Điều 2, Luật An ninh mạng).

(7) **Gián điệp mạng** là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu hoặc phương tiện điện tử của cơ quan, tổ chức, cá nhân (Khoản 10, Điều 2, Luật An ninh mạng).

**2. Nhận thức về an ninh mạng trong tình hình hiện nay**

(1) ***An ninh mạng là vấn đề an ninh phi truyền thống,*** bởi: (1) Mang tính toàn cầu, một quốc gia đơn lẻ không thể giải quyết được. (2) Mang tính phi chính phủ, bởi nhiều nguy cơ đe dọa an ninh mạng không xuất phát từ đường lối chính sách của quốc gia mà do một nhóm người, một tổ chức nào đó gây ra. (3) Mang tính tương đối, không phải hành vi tấn công mạng nào cũng có mục đích hóa, có thể từ vấn đề xâm phạm an ninh quốc gia. (4) Có tính chuyển hoá, có thể từ vấn đề an ninh phi truyền thống trở thành vấn đề an ninh truyền thống khi vũ khí mạng được sử dụng vào các hoạt động vũ trang. (5) Mang tính vận động, các mối đe dọa gây ra từ an ninh mạng không cố định mà luôn thay đổi cả nội dung và hình thức. (6) Mang tính vô hình và khó xác định, không ai dự đoán được các mối đe dọa an ninh mạng sẽ xảy ra ở đâu, khi nào và hậu quả ra sao.

(2) ***An ninh mạng có quan hệ tác động qua lại với các vấn đề an ninh truyền thống là an ninh chính trị và an ninh quân sự***. Biến động chính trị với tên gọi “Mùa xuân Ả Rập” tại hàng loạt quốc gia Trung Đông - Bắc Phi, sâu máy tính Stuxnet phá hủy hàng nghìn máy ly tâm tại Nhà máy Hạt nhân Busher và biến thể của nó là tác nhân gây nổ kho chứa tên lửa đạn đạo Sejil-2 của Iran, hàng loạt các bản thiết kế vũ khí tối tân của Mỹ bị tin tặc đánh cắp, hay mới đây là hệ thống tên lửa phòng không Patriot của Đức đặt tại Thổ Nhĩ Kỳ bị tin tặc kiểm soát... là những minh chứng rõ nhất cho thấy an ninh mạng đã tác động từ an ninh chính trị và an ninh quân sự như thế nào. Ở chiều ngược lại, xuất phát từ lợi ích chính trị, quân sự, các quốc gia không chỉ quan tâm bảo đảm an ninh mạng bằng năng lực công nghệ, chính sách, chiến lược mà còn quan tâm để hoạt động tình báo, gián điệp mạng, “diễn biến hòa bình” trên không gian mạng dẫn tới nguy cơ chiến tranh mạng.

(3) ***An ninh mạng có quan hệ tác động qua lại, chồng lấn, chuyển hóa với các vấn đề an ninh phi truyền thông khác***, như an ninh kinh tế, an ninh thông tin, an ninh tư tưởng - văn hóa và đấu tranh phòng, chống tội phạm xuyên quốc gia, khủng bố...

**II. QUY ĐỊNH PHÁP LUẬT VỀ AN NINH MẠNG VÀ PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO**

Quy định pháp luật về an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao hiện hành đề cập các nội dung cơ bản sau: Quy định các hành vi bị nghiêm cấm, các hành vi vi phạm về an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; quy định về xử phạt vi phạm pháp luật về an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; biện pháp bảo vệ an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; quy định về trách nhiệm bảo vệ an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao.

***2.2.1. Quy định về các hành vi bị nghiêm cấm***

- Điều 8, Luật An ninh mạng quy định các hành vi bị nghiêm cấm về an ninh mạng, bao gồm:

+ Sử dụng không gian mạng để thực hiện các hành vi: Vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội; Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; Xúi giục, lôi kéo, kích động người khác phạm tội.

+ Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, gây sự cổ, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

+ Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử, phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử, xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

+ Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng, tần công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

+ Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

+ Hành vi khác vi phạm quy định của Luật An ninh mạng.

- Đối với quy định liên quan đến bảo vệ bí mật nhà nước, nghiêm cấm các hành vi: Soạn thảo, lưu giữ tài liệu bí mật nhà nước trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng internet, mạng máy tính mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định pháp luật về cơ yếu; Truyền đưa bí mật nhà nước trên phương tiện thông tin, viễn thông trái với quy định của pháp luật về cơ yếu; đăng tải phát tán bí mật nhà nước trên phương tiện thông tin đại chúng, mạng internet, mạng máy tính, mạng viễn thông....

- Đối với quy định về bảo vệ dữ liệu cá nhân, nghiêm cấm các hành vi: Xử lý dữ liệu cá nhân trái với quy định của pháp luật về bảo vệ dữ liệu cá nhân; Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu gây ảnh hưởng tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân khác; cản trở hoạt động bảo vệ dữ liệu cả nhân của cơ quan có thẩm quyền; lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.

**2.2.2. Các tội danh vi phạm pháp luật về phòng chống tội phạm sử dụng công nghệ cao thuộc thẩm quyền điều tra, KTVA của lực lượng ANM**

Theo quy định tại khoản 5 điều 25 Thông tư 56/2017/TT-BCA ngày 16/11/2017 của Bộ Công an (sửa đổi, bổ sung 2018), Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an cấp tỉnh có thẩm quyền khởi tố vụ án hình sự, lấy lời khai, khám nghiệm hiện trường, khám xét, thu giữ, tạm giữ và bảo quản vật chứng, tài liệu liên quan trực tiếp đến vụ án, chuyển hồ sơ vụ án cho Cơ quan điều tra có thẩm quyền trong thời hạn 07 ngày, kể từ ngày ra quyết định khởi tố vụ án, đối với các tội danh sau:

**Chương XIII. CÁC TỘI XÂM PHẠM AN NINH QUỐC GIA**

Điều 108. Tội phản bội Tổ quốc

Điều 109. Tội hoạt động nhằm lật đổ chính quyền nhân dân

Điều 110. Tội gián điệp

Điều 111. Tội xâm phạm an ninh lãnh thổ

Điều 112. Tội bạo loạn

Điều 113. Tội khủng bố nhằm chống chính quyền nhân dân

Điều 114. Tội phá hoại cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam

Điều 115. Tội phá hoại việc thực hiện các chính sách kinh tế - xã hội

Điều 116. Tội phá hoại chính sách đoàn kết

Điều 117. Tội làm, tàng trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam

Điều 118. Tội phá rối an ninh

Điều 119. Tội chống phá cơ sở giam giữ

Điều 120. Tội tổ chức, cưỡng ép, xúi giục người khác trốn đi nước ngoài hoặc trốn ở lại nước ngoài nhằm chống chính quyền nhân dân

Điều 121. Tội trốn đi nước ngoài hoặc trốn ở lại nước ngoài nhằm chống chính quyền nhân dân

**Chương XXVI. CÁC TỘI PHÁ HOẠI HÒA BÌNH, CHỐNG LOÀI NGƯỜI VÀ TỘI PHẠM CHIẾN TRANH**

Điều 421. Tội phá hoại hòa bình, gây chiến tranh xâm lược

Điều 422. Tội chống loài người

Điều 423. Tội phạm chiến tranh

Điều 424. Tội tuyển mộ, huấn luyện hoặc sử dụng lính đánh thuê

Điều 425. Tội làm lính đánh thuê

**Chương XXI. CÁC TỘI XÂM PHẠM AN TOÀN CÔNG CỘNG, TRẬT TỰ CÔNG CỘNG**

**Mục 2. TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG**

Điều 285. Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật

Điều 286. Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử

Điều 287. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử

Điều 288. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông

Điều 289. Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác

Điều 290. Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản

Điều 291. Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hang

Điều 292. (bãi bỏ)

Điều 293. Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh

Điều 294. Tội cố ý gây nhiễu có hại

Điều 207. Tội làm, tàng trữ, vận chuyển, lưu hành tiền giả

Điều 208. Tội làm, tàng trữ, vận chuyển, lưu hành công cụ chuyển nhượng giả hoặc các giấy tờ có giá giả khác

Điều 282. Tội chiếm đoạt tàu bay, tàu thủy

Điều 283. Tội điều khiển tàu bay vi phạm các quy định về hàng không của nước Cộng hòa xã hội chủ nghĩa Việt Nam

Điều 284. Tội điều khiển phương tiện hàng hải vi phạm các quy định về hàng hải của nước Cộng hòa xã hội chủ nghĩa Việt Nam

Điều 299. Tội khủng bố

Điều 300. Tội tài trợ khủng bố

Điều 303. Tội phá hủy công trình, cơ sở, phương tiện quan trọng về an ninh quốc gia

Điều 304. Tội chế tạo, tàng trữ, vận chuyển, sử dụng, mua bán trái phép hoặc chiếm đoạt vũ khí quân dụng, phương tiện kỹ thuật quân sự

Điều 305. Tội chế tạo, tàng trữ, vận chuyển, sử dụng, mua bán trái phép hoặc chiếm đoạt vật liệu nổ

Điều 309. Tội sản xuất, tàng trữ, vận chuyển, sử dụng, phát tán, mua bán trái phép hoặc chiếm đoạt chất phóng xạ, vật liệu hạt nhân

Điều 337. Tội cố ý làm lộ bí mật nhà nước; tội chiếm đoạt, mua bán, tiêu hủy tài liệu bí mật nhà nước

Điều 338. Tội vô ý làm lộ bí mật nhà nước; tội làm mất vật, tài liệu bí mật nhà nước

Điều 174. Tội lừa đảo chiếm đoạt tài sản

Điều 206. Tội vi phạm quy định trong hoạt động của các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài

Điều 217a. Tội vi phạm quy định về kinh doanh theo phương thức đa cấp

Điều 225. Tội xâm phạm quyền tác giả, quyền liên quan

Điều 321. Tội đánh bạc

Điều 326. Tội truyền bá văn hóa phẩm đồi trụy

Điều 328. Tội môi giới mại dâm

**III. TÌNH HÌNH TỘI PHẠM LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG**

Những năm vừa qua, lừa đảo trực tuyến đã và đang trở thành vấn nạn trên toàn thế giới, trong đó có Việt Nam. Các đối tượng lợi dụng bối cảnh bùng nổ công nghệ thông tin đã thực hiện nhiều vụ lừa đảo trực tuyến, chiếm đoạt tài sản có giá trị cao, gây bức xúc trong dư luận và quần chúng nhân dân, ảnh hưởng nghiêm trọng đến trật tự an toàn xã hội. Nạn lừa đảo xảy ra ở hầu hết các địa phương trên cả nước, chiếm tỷ lệ cao trong cơ cấu tội phạm hình sự, da dạng về hình thức, phạm vi hoạt động xuyên quốc gia. Các đối tượng liên tục thay đổi phương thức, sử dụng nhiêu thủ đoạn phạm tội mới; hoạt động tinh vi, chuyên nghiệp hơn; có sự móc nối, học tập kinh nghiệm của các băng nhóm tội phạm trên thế giới.

Riêng năm 2023, thế giới ước tính thiệt hại là 1.026 tỉ USD, tương đương 1,05% GDP toàn cầu.

Tại Việt Nam, thống kê trên Cổng cảnh báo an toàn thông tin ghi nhận gần 16.000 phản ánh lừa đảo trực tuyến, gây thiệt hại hơn 390.000 tỉ đồng, tương đương 3,6% GDP; trong đó 91% liên quan lĩnh vực tài chính, tăng 64,78% so với năm 2022, tỉ lệ người dùng nhận tin nhắn, cuộc gọi lừa đảo trực tuyến là 73%. Trong đó, riêng lực lượng ANM và PC TP sử dụng CNC cả nước đã tiếp nhận hơn 3.500 vụ việc lừa đảo, tổng số tiền thiệt hại hơn 2.487 tỉ đồng.

Tại Đồng Nai, trong 6 tháng đầu năm 2024, đã tiếp nhận 76 vụ lừa đảo qua mạng, tổng số tiền thiệt hại trên 325,4 tỉ đồng. Đã làm rõ 04 vụ/14 đối tượng.

Thời gian qua, phòng An ninh mạng và PC TP sử dụng CNC đã tham mưu Ban Giám đốc Công an tỉnh phối hợp các đơn vị có liên quan triển khai rất nhiều các hoạt động tuyên truyền về phương thức, thủ đoạn của các loại tội phạm lừa đảo qua mạng với nhiều hình thức khác nhau (tờ rơi, tuyên truyền trực tiếp, qua báo, đài truyền hình, qua cổng thông tin điện tử, mạng xã hội…). Tuy nhiên vẫn có nhiều người dân nhận thức chưa đầy đủ hoặc chưa nhận thức được phương thức thủ đoạn phạm tội của các đối tượng, thiếu cảnh giác và ý thức tự bảo vệ bản thân khi hoạt động trên môi trường mạng nỗn đã trở thành nạn nhân của các vụ lừa đảo.

Qua công tác nắm tình hình, phòng ngừa, đấu tranh với tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, phòng An ninh mạng và PCTP sử dụng CNC xác định các đối tượng lừa đảo sử dụng nhiều hình thức khác nhau, nhắm đến mọi khía cạnh đời sống xã hội của người dân, với mỗi phương thức, các đối tượng đều xây dựng nhiều kịch bản tiếp cận khác nhau. Đặc điểm của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng là:

- Hoạt động trên không gian mạng hoặc sử dụng các thiết bị, phần mềm công nghệ có tính ẩn danh cao để thực hiện hành vi phạm tội.

- Khai thác lỗ hỗng bảo mật trên các thiết bị điện tử hoặc sơ hở của người dùng khi tham gia môi trường mạng.

- Đánh vào lòng tham, tâm lý hoang mang, thiếu nhận thức, cảnh giác của người dân khi tham gia mạng xã hội.

- Hoạt động có tổ chức, phân công nhiệm vụ cụ thể cho từng nhóm khác nhau. Xây dựng kịch bản cho nhân viên trước từng tình huống cụ thể.

- Lợi dụng những sơ hở trong công tác quản lý nhà nước về cung cấp dịch vụ viễn thông, internet, ngân hàng... để thực hiện hành vi phạm tội nhằm trốn tránh sự phát hiện của cơ quan chức năng.

**III. CÁC HÌNH THƯC LỪA ĐẢO TRỰC TUYẾN**

Hiện nay, rất nhiều cơ quan chức năng đưa ra cảnh báo về thủ đoạn lừa đảo trực tuyến. Nổi bật là các đơn vị thuộc Bộ Thông tin truyền thông và Bộ Công an. Số lượng hình thức được cảnh báo rất nhiều, có đơn vị đưa ra 8, có đơn vị đưa ra 11, 24, 32…. Theo Cẩm nang phòng chống lừa đảo trên không gian mạng của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), thì có 10 phương thức lừa đảo phổ biến nhất hiện nay, đó là

**1. Lừa đảo mua bán hàng hóa, dịch vụ (vé máy bay, du lịch...) giá rẻ**

***• Dấu hiệu:***

- Các đối tượng đăng tải bài viết quảng cáo các loại hàng hóa, dịch vụ với mức giá rẻ hơn so với thị trường. Khi người dân liên hệ, các đối tượng tạo vỏ bọc uy tín, yêu cầu người dân chuyển tiền đặt cọc hoặc trả tiền trước, sau đó chiếm đoạt số tiền trên.

- Đăng bài viết quảng cáo dịch vụ làm thị thực (visa) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa. Sau khi nạn nhân chuyển khoản đặt cọc hoặc thanh toán trước chi phí, các đối tượng yêu cầu nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ... Sau đó lấy nhiều lý do khác nhau để không trả lại tiền.

- Giả mạo website/fanpage của công ty du lịch uy tín, làm giả ảnh chụp biên lai, hóa đơn thanh toán và đề nghị nạn nhân chuyển khoản thanh toán chi phí tour du lịch. Sau khi khách hàng chuyển tiền để thanh toán dịch vụ du lịch các đối tượng sẽ chiếm đoạt tiền và chặn liên lạc.

- Mạo danh đại lý bán vé máy bay, tự tạo ra các website, trang mạng xã hội, với địa chỉ đường dẫn, thiết kế tương tự kênh của các hãng hoặc đại lý chính thức, đăng tải nhiều bài viết thể hiện việc đặt vé máy bay cho nhiều đoàn khách khác nhau. Nếu khách hàng liên hệ, các đối tượng sẽ đặt chỗ máy bay, gửi mã đặt chỗ để làm tin hoặc sử dụng phần mềm chỉnh sửa ảnh để tạo vé máy bay giả và yêu cầu khách hàng thanh toán. Sau khi nhận thanh toán, các đối tượng không xuất ra vé máy bay và ngắt liên lạc.

***• Biện pháp phòng tránh:***

- Để tránh bị lừa đảo trước các thủ đoạn nêu trên, người dân cần tìm hiểu kỹ thông tin khi lựa chọn mua sắm hàng hóa hoặc các gói dịch vụ trên mạng, nên lựa chọn mua hàng, dịch vụ đặt tour, đặt phòng, đặt vé máy bay... của những công ty uy tín. Để yên tâm hơn, người dân có thể đề nghị phía đối tác cho xem hóa đơn chứng từ, giấy phép hoạt động kinh doanh, giấy tờ, chứng chỉ hành nghề... của công ty lữ hành, du lịch; đề nghị thanh toán sau khi nhận và kiểm tra hàng đối với các giao dịch mua hàng trực tuyến.

- Đồng thời, chú ý các dấu hiệu nhận biết website giả mạo thông qua tên website và tên miền. Thông thường ten các website giả sẽ gần giống với tên các website thật nhưng sẽ có thêm hoặc thiếu một số ký tự. Tên miền giả thường sử dụng những đuôi lạ như **.cc, .xyz, .tk...**

- Đặc biệt, đối với các trang mạng xã hội hoạt động mua bán, quảng bá các gói du lịch, nhất là gói du lịch giá rẻ, vé máy bay giá rẻ, người dân nên chọn các trang mạng xã hội có dấu tích xanh (đã được xác thực) hoặc chọn các trang mạng xã hội uy tín mà mình biết rõ thông tin của người bán. Lưu lại thông tin liên quan để kịp thời phát hiện dấu hiệu lừa đảo, trình báo cho cơ quan Công an nơi gần nhất để được hướng dẫn giải quyết.

**2. Chiếm đoạt tài khoản mạng xã hội sau đó giả mạo người thân, quen nhắn tin, gọi điện yêu cầu chuyển tiền.**

Đây là hình thức lừa đảo khá phổ biến, các đối tượng sau khi đánh cắp được tài khoản mạng xã hội sẽ nghiên cứu cách thức nói chuyện của chủ tài khoản với bạn bè, người thân hoặc thu thập các video của chủ tài khoản còn lưu trên mạng xã hội, sử dụng căn cước công dân giả đăng ký tài khoản ngân hàng online trùng với tên của chủ tài khoản mạng xã hội bị đánh cắp, khiến cho nạn nhân lầm tưởng rằng đang chuyển tiền cho bạn bè, người thân cùa mình. Sau đó nhắn tin hoặc gọi điện cho người thân, quen hỏi vay tiền hoặc nhờ chuyển khoản hộ.

Hiện nay, đối tượng lừa đảo còn sử dụng trí tuệ nhân tạo (AI), nổi bật là công nghệ deepfake, để tạo ra các cuộc gọi video giả mạo với chất lượng cao từ những hình ảnh, âm thanh thu được từ facebook nhằm tăng lòng tin cho nạn nhân.

***• Dấu hiệu:***

- Tin nhắn hoặc email đáng ngờ: Nếu bạn nhận được một tin nhắn hoặc email từ một người bạn trong danh sách bạn bè yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu chuyển tiền hoặc thực hiện hành động khẩn câp, hãy cảnh giác. Đặc biệt, nếu tin nhắn có chứa các lời khẩn cấp, đe dọa hoặc yêu cầu không phù hợp, hãy kiểm tra lại xem có phải tin nhắn thực sự từ bạn bè của bạn hay không.

- Sự thay đổi đột ngột trong ngôn ngữ hoặc phong cách viết: Nếu tin nhắn từ bạn bè có sự thay đổi đột ngột trong cách viết, từ ngữ không giống với phong cách thông thường hoặc có chứa các lời lẽ lạ lùng, cẩn thận hơn.

- Đường link đáng ngờ: Kiểm tra đường link được chia sẻ trong tin nhắn. Nếu đường link có dấu hiệu đáng ngờ như URL không phổ biến, thiếu ký tự an toàn (https://), hoặc điều hướng đến các trang web không rõ nguồn gốc hoặc đáng ngờ, hãy tránh nhấp chuột hoặc truy cập vào đường link đó.

- Yêu cầu cung cấp thông tin cá nhân hoặc thông tin đăng nhập: Lưu ý rằng bạn không nên cung câp thông tin cá nhân nhạy cảm hoặc thông tin đăng nhập (tên đăng nhập, mật khẩu) thông qua tin nhắn hoặc email. Lừa đảo thường sử dụng chiêu này để chiếm quyền điều khiển tài khoản của bạn.

***• Biện pháp phòng tránh:***

- Xác minh thông tin: Nếu bạn nhận được một tin nhắn hoặc email đáng ngờ từ một người bạn, hãy thử liên hệ trực tiếp với họ thông qua các phương tiện khác (điện thoại, tin nhắn, email) để xác minh xem tin nhắn đó có phải từ họ hay không. Đừng sử dụng thông tin liên hệ được cung cấp trong tin nhắn đáng ngờ để xác minh.

- Thay đổi mật khẩu ngay lập tức của tài khoản MXH và sử dụng một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Đặc biệt, phải sử dụng bảo mật 02 lớp, còn gọi là 2FA (2 factor authentication)

- Thông báo cho bạn bè và người thân trong danh sách bạn bè của bạn về tình huống và cảnh báo họ không nên tin tưởng hoặc phản hồi vào những tin nhan lừa đảo.

- Không click vào đường dẫn lạ do người thân, bạn bè gửi qua mạng xã hội; tìm cách liên lạc trực tiếp với người thân để kiểm tra thông tin.

Ngoài ra, hãy luôn giữ cảnh giác và tuân thủ các biện pháp bảo mật cơ bản như không chia sẻ thông tin cá nhân và mật khẩu với bất kỳ ai, không bấm vào các liên kết không rõ nguồn gốc hoặc tin nhắn đáng ngờ, và cập nhật phần mềm bảo mật định kỳ để tránh các lỗ hổng bảo mật.

**3. Lừa đảo chuẩn hóa thông tin cá nhân (thuê bao di động, VNeID, tài khoản ngân hàng...) để yêu cầu truy cập hoặc cài đặt ứng dụng độc hại.**

Đây là hình thức lừa đảo giả danh cơ quan quản lý Nhà nước để yêu cầu người dân truy cập đường link chứa mã độc hoặc tải về ứng dụng giả mạo chứa mã độc. Sau khi người dân click vào đường dẫn hoặc tải về ứng dụng, cho phép truy cập thiết bị, các đối tượng sẽ thu thập được dữ liệu về thông tin cá nhân, tài khoản ngân hàng... nhằm mục đích chiếm đoạt tài sản.

***• Dấu hiệu:***

- Cuộc gọi đến từ số điện thoại cá nhân hoặc số điện thoại giả mạo thương hiệu (Brandname) như VNeID, 113, Vinaphone, Viettel…, các đối tượng giả danh cơ quan quản lý Nhà nước (cảnh sát khu vực, cán bộ quản lý hộ tịch, nhà cung cấp dịch vụ viễn thông, điện lực hoặc nhân viên ngân hàng...), thông báo đề nghị người dân bổ sung hoặc sửa đổi dữ liệu thông tin cá nhân để chuẩn hóa theo quy định.

- Các đối tượng yêu cầu người dân cung cấp thông tin cá nhân để chuẩn hóa, hoặc truy cập vào các đường dẫn giả mạo, tải ứng dụng chứa mã độc để chiếm quyền điều khiển thiết bị điện tử hoặc các tài khoản ngân hàng, thuê bao di động... Đối tượng gây áp lực bằng cách đe dọa nếu không làm theo hướng dẫn thì có thể sẽ bị khóa thuê bao di động, khóa tài khoản ngân hàng hoặc cơ quan Công an sẽ đến nhà làm việc...

- Trong một số trường hợp, để tạo lòng tin, các đối tượng gọi video call cho người dân với trang phục Công an hoặc giả mạo văn phòng làm việc của các cơ quan quản lý Nhà nước.​​

***• Biện pháp phòng tránh:***

- Cảnh giác khi nhận các cuộc gọi tự xưng là cán bộ cơ quan quản lý nhà nước, nhân viên ngân hàng, nhà mạng... đề nghị cung cấp thông tin cá nhân. Tuyệt đối không chia sẻ, cung cấp thông tin của bản thân cho người khác qua điện thoại hoặc mạng xã hội.

- Liên hệ trực tiếp đến Công an phường/xã nơi cư trú khi nhận được yêu cầu chỉnh sửa/ bổ sung thông tin cá nhân; Liên hệ đến số hotline của nhà mạng, ngân hàng khi nhận được yêu cầu chuẩn hóa thông tin thuê bao hoặc tài khoản ngân hàng.

**4. Giả mạo cơ quan, tổ chức, cá nhân tuyển người mẫu, cầu thủ nhí, người đại diện thương hiệu sau đó lôi kéo làm nhiệm vụ online.**

Lợi dụng các sự kiện lớn sắp diễn ra hoặc thời gian nghỉ lễ của trẻ nhỏ, các đối tượng tạo lập các trang mạng xã hội đăng thông tin tuyển người mẫu, ca sĩ, cầu thủ nhí hoặc tuyển đại diện cho các thương hiệu lớn để quảng bá sản phẩm. Sau khi người dân đăng ký tham gia, chúng sẽ thu thập thông tin cá nhân của người dân và gia đình. Các đối tượng tiếp tục hướng dẫn người dân vào trang web của chương trình để làm nhiệm vụ tăng tương tác, tăng lượt bình chọn, sau đó yêu cầu chuyển tiền để hoàn thành nhiệm vụ.

***• Dấu hiệu:***

- Đối tượng chủ động tạo lập các trang web, trang facebook…, lấy danh nghĩa các Công ty truyền thông, trung tâm đào tạo bóng đá… đăng tin quảng cáo trên mạng xã hội.

- Khi người dân liên hệ sẽ được các đối tượng hướng dẫn cung cấp thông tin cá nhân của bản thân và gia đình. Sau đó, các đối tượng gửi đường dẫn để người dân truy cập vào đăng ký tài khoản, làm nhiệm vụ online, chuyển tiền đặt cọc để hoàn thành nhiệm vụ, nhận lại tiền sau khi hoàn thành nhiệm vụ.

- Được mời vào các nhóm kín trên mạng xã hội, trong đó có nhiều tài khoản “vào vai” các phụ huynh khác để thúc giục nạn nhân chuyển tiền hoàn thành nhiệm vụ.

***• Biện pháp phòng tránh:***

- Tìm hiểu kỹ về các Công ty, Trung tâm trước khi đăng ký cho bản thân và người nhà tham gia các chương trình qua mạng xã hội. Chỉ chọn các Công ty, Trung tâm có uy tín, đã kiểm tra, xác thực chính xác thông tin (liên hệ hotline của các Công ty đăng tải trên trang web chính thống).

- Tuyệt đối không cung cấp thông tin cá nhân của bản thân và người thân cho các trang web, trang mạng xã hội khi chưa xác định chính xác mức độ uy tín để phòng tránh việc bị lừa đảo cũng như các mục đích xấu khác.

- Cảnh giác trước khi chuyển tiền phí tham dự chương trình, nếu có thể hãy đến trực tiếp văn phòng của Công ty/ Trung tâm để làm việc; không thực hiện các giao dịch chuyển tiền để làm nhiệm vụ online.

**5. Giả danh công ty tài chính, ngân hàng để hỗ trợ cho vay, nâng hạn mức tín dụng... sau đó yêu cầu chuyền tiền để làm thủ tục.**

Những năm gần đây, nhu cầu vay tiền trực tuyến qua App hoặc nâng hạn mức tín dụng chi tiêu Online của người dân tăng cao, các đối tượng đã giả danh công ty tài chính, ngân hàng đăng tải thông tin quảng cáo dịch vụ cho vay Online lãi suất thấp, thủ tục đơn giản, giải ngân nhanh chóng hoặc hỗ trợ nâng hạn mức cho các tài khoản tín dụng. Để được giải quyết thủ tục, người dân cần nộp trước một khoản phí để làm hồ sơ hoặc để bảo đảm tài sản… Số tiền này được hứa hẹn sẽ trả lại sau khi hoàn thành thủ tục. Thực tế, sau khi người dân chuyển tiền, các đối tượng sẽ cắt liên lạc hoặc lấy lý do khác nhau để không trả lại tiền.

***• Dấu hiệu:***

- Đối tượng sử dụng số điện thoại, tin nhắn hoặc email giả mạo gần giống với thông tin của nhân viên ngân hàng, liên hệ với người dân có nhu cầu.

- Các đối tượng lập nhiều trang mạng xã hội quảng cáo dịch vụ cho vay tiền online qua app. Khi người dân liên hệ sẽ được các đối tượng hướng dẫn cài ứng dụng nhằm mục đích thu thập thông tin cá nhân hoặc ứng dụng chứa mã độc nhằm chiếm quyền điều khiển thiết bị. Để được giải ngân khoản vay, người dân cần đóng khoản phí đảm bảo tài sản, sau đó các đối tượng sẽ chiếm đoạt số tiền này.

- Giả danh nhân viên ngân hàng quảng cáo dịch vụ mở thẻ tín dụng, nâng cấp hạn mức tín dụng tiêu dùng cho người dân. Đe được đáp ứng dịch vụ, người dân cần cung cấp thông tin cá nhân, chuyển một khoản phí đảm bảo để được duyệt nâng hạn mức.

***• Biện pháp phòng tránh:***

- Nên tìm hiểu kỹ và sử dụng dịch vụ của các cơ quan, doanh nghiệp uy tín trong lĩnh vực tài chính, ngân hàng.

- Cảnh giác khi thực hiện các giao dịch trong lĩnh vực tài chính, ngân hàng qua mạng. Liên hệ trực tiếp đến hotline trên trang chủ của các ngân hàng, công ty tài chính để kiểm tra thông tin.

- Không chuyển tiền đặt cọc, đảm bảo tài sản khi có nhu cầu vay tiền hoặc đăng ký dịch vụ tín dụng... qua mạng.

- Việc cài dặt ứng dụng qua mạng tiềm ẩn nhiều rủi ro liên quan đến lộ thông tin cá nhân, bị cài mã độc chiếm quyền điều khiển thiết bị diện tử.

**6. Giả mạo danh nghĩa cơ quan, tổ chức phát tán tin nhắn SMS Brandname chứa đường dẫn truy cập vào các website giả mạo yêu cầu cung cấp thông tin cá nhân hoặc tải về ứng dụng độc hại.**

Tình trạng tin nhắn SMS Brandname giả mạo phần lớn xuất phát từ việc các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới người dùng với mục đích nhằm chiếm đoạt tài sản.

Các điện thoại với tính năng tự động kết nối vào các trạm BTS có cường đô sóng mạnh, do cơ chế này nên các máy điện thoại tự động kết nối vào trạm BTS giả đang phát sóng 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. Ngoài ra, các đối tượng có thể sử dụng các phần mềm spam tin nhắn iMessage để phát tán tin nhắn giả mạo thương hiệu đến người dùng sử dụng thiết bị có hệ điều hành IOS. Bên cạnh dó, do tính năng tự động nhận diện thương hiệu trên điện thoại nên các tin nhắn giả mạo nhận được giống những tin nhắn chính thống đã nhận được trước đó.

***• Dấu hiệu:***

- Dấu hiệu của hành vi lừa đảo trên là nhận tin nhắn mang tên các cơ quan, tổ chức, doanh nghiệp chính thống (như: Bo Cong an, Bo Thong tin va Truyen thong, Vietcombank...) bên trong chứa nội dung như tin nhắn thông thường, kèm theo hướng dẫn giả mạo, đề nghị người dân truy cập, nhập thông tin tài khoản để chiếm đoạt hoặc cài đặt ứng dụng chứa mã độc nhằm chiếm quyền điều khiển thiết bị;

- Các trang web giả mạo thường chứa mã độc hoặc giả mạo trang web chính thống của cơ quan, tổ chức, yêu cầu đăng nhập tài khoản, nhập mã OTP nhằm mục đích chiếm đoạt tài sản.

***• Biện pháp phòng tránh:***

- Kiểm tra kỹ nội dung khi nhận được tin nhắn từ các cơ quan, tổ chức, đặc biệt là các tin nhắn gây chú ý (trúng thưởng, cảnh báo, khuyến mãi...). Không click vào các đường dẫn có dấu hiệu đáng ngờ, kiểm tra kỹ tên miền trang web trước khi đăng nhập thông tin tài khoản.

- Tuyệt đối không chia sẻ thông tin cá nhân, tài khoản ngân hàng, mã OTP với bất kỳ ai.

- Khi nhận được các tin nhắn có dấu hiệu bất thường phải liên lạc ngay với đơn vị chủ quản của brandname thông qua hotline. Gọi điện thoại đến cơ quan, tố chức liên quan để xác thực xem có phải trang web, ứng dụng là của họ hay không.

**7. Lừa đảo tham gia đầu tư sàn chứng khoán ảo, tiền ảo, đa cấp... sau đó khóa, đánh cháy tài khoản hoặc đánh sập sàn.**

Trước xu thế đầu tư vào các hoạt động trực tuyến như chứng khoán, tiền ảo… của người dân tăng cao trong những năm gần đây, tội phạm lừa đảo qua mạng đẩy mạnh hoạt động thông qua hình thức này. Các đối tượng lừa đảo tạo lập các sàn chứng khoán, đa cấp, tiền ảo… một cách dễ dàng, sử dụng mạng xã hội quảng cáo, tuyển người tham gia đầu tư với những lời hứa hẹn hấp dẫn như: cam kết có lãi, lợi nhuận cao, kiếm tiền dễ dàng… khiến cho không ít nạn nhân sập bẫy, mất số tiền lớn. Hầu hết nạn nhân khi tham gia đầu tư đều được tư vấn chi tiết cách thức mở tài khoản, đầu tư các khoản tiền nhỏ để thử và nhận lại khoản lãi suất tương ứng nhằm mục đích đánh vào lòng tham. Sau khi thấy có thể kiếm được tiền từ các sàn này, nạn nhân được mời gọi đầu tư số tiền lớn hơn và lấy nhiều lý do để không thể rút được tiền ra mà phải đóng thêm nhiều khoản phí với cam kết sẽ được nhận lại toàn bộ cả tiền phí và tiền lãi ban đầu (hệ thống thanh toán lỗi, nhập sai nội dung giao dịch, sai tài khoản, cơ quan thuế nước ngoài điều tra…) hoặc khóa tài khoản, cho sập sàn giao dịch và cắt liên lạc với nạn nhân.

***• Dấu hiệu:***

- Lợi nhuận rất cao, thường trên 10% / tháng, thậm chí lên đến 30% - 60%.

- Các đối tượng thường chủ động tiếp cận với người dân để tìm cách giới thiệu, quảng cáo về trang web hoặc sàn giao dịch mà mình đang đầu tư và thu được lợi nhuận cao từ việc đầu tư này.

- Phương thức tiếp cận nạn nhân của các đối tượng rất đa dạng, có thể từ quảng cáo trên mạng xã hội, hoặc vào vai doanh nhân thành đạt kết bạn làm quen, trò chuyện tình cảm trong thời gian dài, dần dần lôi kéo đầu tư.

- Các đối tượng tìm nhiều cách để không gặp mặt nạn nhân, lấy lý do ở nước ngoài, đi công tác... giả mạo định vị để tạo lòng tin. Chúng luôn đóng vai là người đầu tư cùng khiến nhiều nạn nhân dù đã nghi ngờ bị lừa đảo nhưng vẫn tin tưởng vào "người bạn" của mình nên tiếp tục chuyển tiền.

- Nạn nhân thường được đưa vào các nhóm kín trên mạng xã hội có nhiều tài khoản ảo đóng vai "chuyên gia đọc lệnh", thành viên cùng tham gia đầu tư. Các tài khoản ảo thường xuyên đăng tin chuyển tiền thành công hoặc đã nhận được lãi suất từ sàn đầu tư sau khi làm theo hướng dẫn của các "chuyên gia". Khi nạn nhân có dấu hiệu nghi ngờ, cân nhắc chuyển tiền, các tài khoản ảo liên tục thúc giục việc chuyển tiền để nhóm tiếp tục hoạt động.

***• Biện pháp phòng tránh:***

- Cần cảnh giác khi tham gia đầu tư chứng khoán, đa cấp, tiền ảo... vào các sàn giao dịch trực tuyến trên mạng không rõ thông tin hoặc thông tin có dấu hiệu bị giả mạo. Người dân cũng cần tìm hiểu kỹ thông tin về sàn giao dịch trước khi đầu tư, đặc biệt là các sàn đầu tư đăng tải địa chỉ ảo, không có thật, hoặc giả mạo của sàn đầu tư chính thống.

- Nâng cao cảnh giác khi giao tiếp với người lạ trên mạng xã hội, tuyệt đối không chia sẻ thông tin cá nhân, làm theo hướng dẫn khi chưa xác định chính xác nhân thân, lai lịch của người đó.

- Chỉ đầu tư vào các sàn giao dịch chính thống đã được các cơ quan quản lý nhà nước cấp phép hoạt động. Trước khi đầu tư, nên đến trực tiếp văn phòng của các sàn giao dịch để được tư vấn, hỗ trợ và kiểm chứng thông tin.

**8. Lừa đảo tình cảm sau đó dẫn dụ đầu tư tài chính, làm nhiệm vụ online hoặc gửi tiền, quà có giá trị**.

Hình thức lừa đảo tình cảm hiện nay không còn mới, tuy nhiên vẫn có rất nhiều người dân dính phải bẫy lừa đảo của các đối tượng. Các đối tượng lập ra nhiều tài khoản mạng xã hội ảo, lấy ảnh, thông tin của những người nổi tiếng hoặc có ngoại hình ưa nhìn, vỏ bọc doanh nhân, nhắn tin trò chuyện trong thời gian dài với nạn nhân. Trong khi trò chuyện, các đối tượng chia sẻ việc mình kiếm được nhiều tiền thông qua công việc đầu tư, làm nhiệm vụ qua mạng, lôi kéo nạn nhân tham gia cùng nhằm chiếm đoạt tài sản. Ngoài ra, đối tượng có thể tự xưng mình là người nước ngoài, ngỏ ý muốn gửi quà tặng có giá trị cao cho nạn nhân, sau đó giả danh các cơ quan chức năng (Công an, Thuế, Hải quan…) đề nghị nạn nhân đóng các khoản phí để nhận được quà.

***• Dấu hiệu:***

- Nhận được tin nhắn hỏi thăm từ các tài khoản MXH (khen tấm hình đẹp, hỏi thăm khung cảnh, khen ngoại hình,...) với mục đích tiếp cận, làm quen. Những tài khoản này sẽ liên tục hỏi thăm trong một thời gian dài.

- Yêu cầu kết bạn qua các tài khoản MXH, đặc biệt là các ứng dụng hẹn hò (Facebook, Zalo, Tinder,...). Theo đó, các tài khoản này thường có vỏ bọc “hào nhoáng” như ngoại hình đẹp, cuộc sống giàu có, đi du lịch nhiều nơi,...

- Trong thời gian trò chuyện, các đối tượng sẽ thường xuyên chia sẻ về cuộc sống, sinh hoạt,... Trong đó lồng ghép nội dung mình đang làm công việc online và kiếm được nhiều tiền từ đây.

- Trong một số trường hợp, các đối tượng sẽ nhờ nạn nhân đăng nhập tài khoản của mình trên sàn đầu tư để làm nhiệm vụ giúp vì lý do đang bận, việc này nhằm mục đích cho nạn nhân làm quen trước khi rủ tham gia.

- Khi nạn nhân tham gia, có thể sẽ nhận được tiền lãi sau một số lần đầu tư ban đầu với số tiền nhỏ. Dần dần hệ thống sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc nhiều lý do để “giam tiền” như: Cơ quan thuế nước ngoài phong tỏa, thao tác sai, lỗi giao dịch,... và yêu cầu nạn nhân chuyển thêm tiền để có thể rút toàn bộ.

- Hứa hẹn tặng quà có giá trị cao gửi từ nước ngoài về. Đối tượng sau thời gian trò chuyện sẽ tỏ ý yêu mến nạn nhân, muốn tặng cho nạn nhân những món quà có giá trị cao. Tuy nhiên, việc gửi quà gặp nhiều trục trặc như: Bị cơ quan chức năng tạm giữ do giá trị cao, cần khoản phí thông quan,... Theo đó, nhiều nạn nhân với tâm lý sẽ nhận được quà giá trị rất lớn nên sẽ chấp thuận ứng trước một số tiền để hoàn thiện thủ tục.

***• Biện pháp phòng tránh:***

- Cẩn trọng khi tiếp xúc với người lạ trên mạng, đặc biệt là các tài khoản lạ, không có bạn chung, từ nước ngoài,... Tuyệt đối không tin tưởng vào những bạn bè qua mạng khi chưa gặp mặt và nắm rõ thông tin cá nhân.

- Tuyệt đối không tham gia đầu tư vào các sàn thương mại điện tử không rõ thông tin, không tham gia làm nhiệm vụ hưởng hoa hồng, đầu tư online,... với lợi nhuận cao

- Kiểm tra kỹ các thông tin khi có đề nghị nhận quà tặng từ người lạ, cần xác minh thông tin qua đơn vị vận chuyển chính thống, không chuyển tiền trả những khoản phí trước khi nhận và kiểm tra hàng.

- Việc tìm kiếm bạn bè, kết bạn qua mạng xã hội tiềm ẩn nhiều nguy cơ rủi ro trở thành nạn nhân lừa đảo hoặc bị xâm hại bởi các hành vi khác. Vì vậy cần tìm hiểu thật kỹ thông tin, gặp mặt trực tiếp và xác định chính xác danh tính trước khi đi đến một mối quan hệ với bạn quen qua MXH.

**9. Lừa đảo qua hình thức tuyển cộng tác viên cho các sàn thương mại điện tử, việc nhẹ lương cao**

Những năm gần đây, hình thức lừa đảo tuyển cộng tác viên làm việc online cho các sàn thương mại điện tử là rất phổ biến. Đánh trúng tâm lý muốn kiếm thêm thu nhập từ các công việc online, không mất thời gian đi làm, các đối tượng tạo lập các trang thương mại điện tử giả mạo, lấy danh nghĩa các doanh nghiệp uy tín tuyển cộng tác viên làm việc ngoài giờ, dụ dỗ nạn nhân tham gia đóng trước các khoản tiền tạm ứng để nhận nhiệm vụ hoặc mua các gói nhiệm vụ từ số tiền nhỏ đến số tiền lớn.

***• Dấu hiệu:***

- Các đối tượng thường sử dụng các tài khoản mạng xã hội giả mạo đăng tin tuyển cộng tác viên làm việc online, chỉ cần máy tính kết nối mạng, làm nhiệm vụ đánh giá sản phẩm, thanh toán đơn hàng ảo, click quảng cáo... có thể kiếm về thu nhập cao.

- Nhận được lời mời từ các số điện thoại hoặc tài khoản mạng xã hội ảo. Các tài khoản nay thường chủ động liên hệ nạn nhân, nhắn tin trò chuyện nhằm thu thập thông tin cá nhân, chiếm lòng tin và dụ dỗ nạn nhan tham gia hệ thống.

- Các công việc này thường yêu cầu nạn nhân đóng trước một khoản tiền nhỏ ban đầu và sẽ trả lương hoặc hoa hồng đầy đủ cho nạn nhân để tạo lòng tin. Dần dần, hệ thống sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc dùng nhiều cách khác nhau để không cho nạn nhân rút tiền về mà phải đóng nhiều khoản phí khác nhau.

***• Biện pháp phòng tránh:***

- Cẩn trọng khi tìm kiếm việc làm thông qua mạng xã hội. Khi có nhu câu tìm việc làm online, cần tìm hiểu kỹ về các đơn vị tuyển dụng, đặc biệt là các thông tin tuyển dụng việc nhẹ lương cao, cộng tác viên đánh giá sản phẩm trên các sàn thương mại điện tử, công việc yêu cầu ứng tiền trước để làm nhiệm vụ...

- Cảnh giác khi nhận được lời mời tham gia làm cộng tác viên online từ các tài khoản hoặc bạn bè ảo trên mạng xã hội. Các tài khoản này thường không có danh tính rõ ràng hoặc giả mạo, khi đề nghị gặp mặt trực tiếp sẽ tìm nhiều cách lẩn tránh.

- Tuyệt đối không chuyển tiền trước để thực hiện các nhiệm vụ, công việc tìm kiếm qua mạng khi chưa xác thực chính xác danh tính của công ty chủ quảm liên hệ đến công ty chính thống để xác thực thông tin trước khi tham gia làm cộng tác viên.

**10. Giả danh cơ quan công quyền (công an, viện kiểm sát, tòa án, hải quan...), văn phòng luật sư, ngân hàng... gọi điện đe dọa yêu cầu chuyển tiền hoặc hỗ trợ lấy lại tiền đã bị lừa đảo**.

Đây là hình thức lừa đảo đã xuất hiện trong vài năm trở lại đây. Các đối tượng lợi dụng tâm lý hoang mang, lo sợ của người dân khi bị cơ quan chức năng thông báo liên quan, đến hành vi vi phạm pháp luật. Chúng sử dụng các ứng dụng gọi điện thoại giả mạo danh nghĩa cơ quan chức năng, tiến hành theo bước: thu thập thông tin cá nhân, đe dọa liên quan đến hành vi vi phạm pháp luật, yêu cầu chuyển tiền phục vụ công tác điều tra và cấm không được trao đổi với bất kỳ vì lý do bảo mật.

Ngoài ra, chúng tạo nhiều trang mạng xã hội giả mạo cơ quan công quyền (công an, viện kiểm sát, tòa án, luật sư, kỹ sư An ninh mạng..) đăng tin quảng cáo hoặc chủ động liên hệ các nạn nhân đã bị lừa đảo chiếm đoạt tài sản bởi các hình thức khác và tuyên bố có thể giúp lấy lại tiền bị lừa, yêu cầu chuyển khoản phí dịch vụ trước nhằm chiếm đoạt tài sản.

***• Dấu hiệu:***

- Nhận được cuộc gọi từ số điện thoại lạ hoặc tổng đài ảo (113 BOCONGAN...) thông báo về hành vi vi phạm pháp luật (vi phạm giao thông, liên quan vụ án đang điều tra...). Qua cuộc gọi này, các đối tượng sẽ thu thập thông tin cá nhân của người dân và đe dọa, gây áp lực tâm lý nhằm không cho người dân có cơ hội hỏi ý kiến người thân hoặc cơ quan chức năng. Sau khi thu thập được thông tin, chúng sẽ kết nối người dân đển cuộc gọi khác được giới thiệu là cơ quan kiểm sát, tòa án... để tiếp tục gây áp lực tâm lý, yêu cầu người dân chuyển tiền ngay đến tài khoản của chúng để phục vụ công tac điều tra hoặc xử lý vi phạm giao thông. Có trường hợp, chúng yêu cầu nạn nhân mở tài khoản ngân hàng mới theo số điện thoại do chúng cung cấp, sau đó chuyển toàn bộ tiền từ tài khoản của nạn nhân (tài khoản liên quan đển vụ án như đối tượng thông báo) đến tài khoản mới mở để niêm phong, tạm giữ nhằm chiếm đoạt số tiền này. Quá trình thực hiện tội phạm, chúng luôn yêu cầu nạn nhân giữ bí mật với lý do đây là vụ án, chuyên án đặc biệt nghiêm trọng…

- Các đối tượng thường gợi ý về việc nếu không thể đến cơ quan chức năng làm việc thì chúng hỗ trợ làm việc thông qua điện thoại. Khi người dân đề nghị gặp mặt, chúng có thể sử dụng công nghệ giả mạo gương mặt (deepfake) với trang phục công an, kiểm sát, tòa án... để gọi diện video với người dân, tìm cách lẫn tránh không gặp mặt trực tiếp.

- Một số nạn nhân sau khi bị lừa đảo bởi các hình thức khác có thể nhận được đề nghị giúp đỡ lấy lại tiền từ các tài khoản mạng xã hội giả mạo cơ quan chức năng (công an, kiểm sát, luật sư...). Các đối tượng thường tạo các trang mạng xã hội đăng nhiều thông tin cảnh báo lừa đảo, thêm người dân vào các nhóm chung với nhiều thành viên đóng vai nạn nhân trong các vụ lừa đảo khác đã lấy được tiền hoặc cũng đang nhờ sự trợ giúp để lấy lại tiền. Khi nạn nhân đồng ý, chúng sẽ yêu cầu chuyển trước khoản phí dịch vụ và chiếm đoạt số tiền này.

***• Biện pháp phòng tránh:***

- Cảnh giác khi nhận được cuộc gọi tự xưng là cán bộ cơ quan công quyền, liên hệ cơ quan chức năng nơi gần nhất hoặc số điện thoại của cơ quan công quyền đăng tải trên các trang chính thống dể xác thực thông tin trước khi làm theo yêu cầu của người kết nối. Lưu ý: cơ quan chức năng không làm việc qua điện thoại, chỉ làm việc tại trụ sở cơ quan. Và đặc biệt, cơ quan công quyền không bao giờ yêu cầu chuyển tiền, cung cấp thông tin tài khoản ngân hàng…

- Không cung cấp thông tin cá nhân cho bất kỳ ai thông qua điện thoại khi chưa xác thực chính xác danh tính của người liên hệ với mình.

- Không tin vào các lời quảng cáo hỗ trợ lấy lại tiền đã bị lừa đảo. Cơ quan chức năng cần xác minh làm rõ vụ việc, làm việc trực tiếp với nạn nhân, không hỗ trợ lấy lại tiền qua mạng.

- Luôn Ịuộn giữ tâm lý bình tĩnh khi nhận được cuộc gọi thông báo liên quan đến hành vi vi phạm pháp luật hoặc sau khi bị lừa đảo chiếm đoạt tài sản. Trình báo đến cơ quan Công an nơi sinh sống, làm việc để được hướng dẫn cụ thể, không làm theo đề nghị của các cá nhân, tổ chức khi chưa xác thực danh tính.

**Các phương thức đảo khác (cho số lô đề, chuyển nhầm tiền, lấy lại tài khoản mạng xã hội, gọi video nhạy cảm để tống tiền).**

Bên cạnh các phương thức lừa đảo phổ biến còn hiện nhiều hình thức khác như: cho số lô đề, chuyển nhầm tiền, lấy lại tài khoản mạng xã hội, gọi video nhạy cảm nhằm tống tiền nạn nhân...

***• Dấu hiệu:***

- Các đối tượng thường sử dụng số điện thoại rác, nhiều tài khoản mạng xã hội giả mạo, không có thông tin chính thống, quảng cáo về các hình thức dịch vụ khác nhau, yêu cầu chuyển tiền phí hoặc đặt cọc trước.

- Bất ngờ nhận được một khoản tiền chuyển nhầm với các nội dung giao dịch nhạy cảm, sau đó có người liên hệ xin lại số tiền trên.

- Các đối tượng chủ động nhắn tin làm quen qua mạng xã hội hoặc các ứng dụng kết bạn, gạ gẫm gọi điện video với các hình ảnh nhạy cảm, kích dục sau đó lưu lại video và tống tiền nạn nhân.

***• Biện pháp phòng tránh:***

- Cẩn trọng khi tìm kiếm dịch vụ trên không gian mạng, đặc biệt là các giao dịch yêu cầu chuyển tiền đặt cọc hoặc phí dịch vụ trước khi thực hiện.

- Không chuyển lại tiền chuyển nhầm theo đề nghị của các cá nhân qua điện thoại. Hãy trình báo cơ quan Công an nơi gần nhất hoặc liên hệ với ngân hàng chủ quản. Trường hợp có người lạ liên hệ xin lại tiền chuyển nhầm, hãy ỵêu cầu đến cơ quan Công an nơi gần nhất hoặc trụ sở ngân hàng làm việc trực tiếp thông qua nhân viên ngân hàng.

- Luôn luôn để phòng khi kết bạn với người lạ qua mạng xã hội, không để lộ thông tin cá nhân, hình ảnh nhạy cảm khi hoạt động trên mạng xã hội.

**IV. NGUỜI DÂN CẦN LÀM GÌ SAU KHI BỊ LỪA ĐẢO TRỰC TUYẾN**

- Khi nghi ngờ bản thân có biểu hiện đang bị lửa đảo qua mạng, hãy tìm kiếm thông tin về các hình thức lừa đảo trên mạng internet hoặc xin sự tư vấn từ bạn bè, người thân. Đừng ngại ngùng chia sẻ câu chuyện mình đang gặp phải, người bên ngoài sẽ luôn có tâm lý bình tĩnh, tỉnh táo hơn.

- Trình báo ngay sự việc đến cơ quan Công an nơi gần nhất để nhận được tư vấn và hỗ trợ kịp thời.

- Liên hệ với Ngân hàng chủ quản để báo cáo sự việc và đề nghị hỗ trợ

- Lưu lại tất cả thông tin như lịch sử trò chuyện, các số điện thoại, tài khoản mạng xã hội liên quan, sao kê giao dịch ngân hàng và cung cấp cho cơ quan Công an khi trinh báo.

- Cài đặt lại mật khẩu các tài khoản cá nhân trong trường hợp bị đánh cắp thông tin cá nhân hoặc bị tấn công chiếm quyền điều khiển thiết bị điện tử.

- Cảnh báo cho bạn bè, người thân về hình thức lừa đảo mình đã hoặc đang gặp phải nhằm chủ động phòng ngừa.