**ĐỀ CƯƠNG TUYÊN TRUYỀN CÁC HÌNH THỨC**

**LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG**

***Kính thưa các thầy cô giáo trong nhà trường cùng các em học sinh thân mến, lời đầu tiên tôi xin gửi lời chào trân trọng nhất đến với các thầy cô giáo và các em học sinh trường THPT… Bình Lục.***

***Hôm nay được sự nhất trí về công tác phối hợp tuyên truyền, Công an huyện Bình Lục xin có vài nội dung để trao đổi, tuyên truyền về vấn đề là điểm nóng của xã hội hiện nay, đó là vấn đề tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng.***

**I. Tình hình chung**

- Hiện nay với sự phát triển của công nghệ 4.0 mang lại lợi ích thiết thực trong đời sống của chúng ta, với sự phát triển mạnh mẽ của mạng Internet, hệ thống thanh toán điện mang lại sự tiện lợi rất lớn, sự kết nối giữa con người với con người qua không gian mạng như Facebook, Zalo. Nhà nhà, người người đều sử dụng các dịch vụ tiện ích mà công nghệ số mang lại… có bạn nào không sử dụng mạng Internet, facbook, zalo không nhỉ.

- Bên cạnh sự phát triển của công nghệ cũng kéo theo tội phạm sử dụng công nghệ cao để phạm tội diễn ra phổ biến, phức tạp với nhiều phương thức thủ đoạn tinh vi, gây thiệt hại lớn về tài sản, gây bức xúc trong dư luận xã hội, ảnh hưởng đến an ninh - trật tự, đến hoạt động sản xuất kinh doanh của doanh nghiệp và đời sống Nhân dân.

- Lực lượng Công an đã tuyên truyền, cảnh báo và giải quyết xử lý nhiều đối tượng thực hiện hành vi lừa đảo qua không gian mạng nhưng một số người dân do thiếu hiểu biết vẫn bị các đối tượng lừa đảo, chủ yếu là phụ nữ, học sinh sinh viên, do lòng tham, do lợi ích trước mắt để tội phạm lợi dụng để thực hiện hành vi.

Do đó hôm nay trong buổi nói chuyện ngày hôm nay chúng ta sẽ tìm hiểu 1 vài phương thức thủ đoạn phổ biến của tội phạm LĐCĐTS trên không gian mạng cách nhận diện và phòng ngừa.

**II. NHẬN DIỆN VÀ PHÒNG NGỪA VỚI CÁC HÌNH THỨC LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG**

**1. Thủ đoạn Chiếm đoạt quyền sử dụng tài khoản cá nhân (zalo, facebook…), mạo danh người thân, người quen để lừa vay tiền, chuyển tiền**

Bằng một số hình thức như gửi link tham gia các cuộc bình chọn, khi nạn nhân click và đường link trên thì sẽ hiện lên giao diện đăng nhập giống như các trang mạng xã hội. Khi nạn nhân nhập các thông tin tài khoản của mình vào thì ngay lúc đó các đối tượng liền chiếm quyền sử dụng tài khoản Facebook, Zalo của người sử dụng, giả danh chủ tài khoản nhắn tin cho người thân, bạn bè hoặc các mối quan hệ uy tín để vay tiền hoặc nhờ chuyển tiền vào tài khoản ngân hàng (do chúng cung cấp) sau đó chiếm đoạt tài sản.

Đối tượng sử dụng thông tin cá nhân, hình ảnh của các đồng chí Lãnh đạo các cơ quan chính quyền, đoàn thể, … để thiết lập tài khoản mạng xã hội (zalo, facebook, …) mạo danh. Sau đó, các đối tượng dùng tài khoản mạo danh để kết bạn, nhắn tin trao đổi vay, mượn tiền của bạn bè, người thân, đồng nghiệp, cấp dưới, … và chiếm đoạt tiền của các bị hại chuyển đến.

Phòng ngừa: Khi thấy có người quen, người thân hỏi vay tiền, phải xác minh, gọi điện, liên lạc qua hình thức khác để xác định có đúng người sử dụng tài khoản Facebook, Zalo không? Sử dụng tài khoản ngân hàng chính chủ

**2. Lừa đặt cọc mua hàng giá rẻ**

Các đối tượng đăng tin bán ô tô, xe máy, thiết bị điện tử, sắt thép… trên các trang mạng xã hội (Facebook, zalo,…) với số tiền thấp hơn giá trị thực rất nhiều và yêu cầu bị hại đặt cọc trước. Sau khi nhận được tiền đặt cọc bằng hình thức chuyển khoản trước từ người đặt mua hàng, đối tượng không giao hàng hoặc giao hàng giả, sau đó khóa trang mạng, cắt liên lạc, chiếm đoạt tài sản.

**3. Lừa cho vay tiền qua mạng**

***Lợi dụng tâm lý muốn được vay vốn với số tiền lớn, lãi suất thấp, không cần thế chấp tài sản, thủ tục nhanh gọn, các đối tượng đã đăng tin cho vay vốn thông qua các ứng dụng, mạng xã hội như (Zalo, Facebook…). Sau khi tiếp cận được nạn nhân, các đối tượng yêu cầu nạn nhân tải các ứng dụng (app) vay tiền của chúng vào điện thoại của nạn nhân để thu thập thông tin cá nhân, danh bạ điện thoại.***

Tiếp theo, chúng yêu cầu nạn nhân chuyển tiền nhiều lần vào các tài khoản mà chúng cung cấp với các lý do như chuyển tiền để chứng minh tài chính, nộp tiền thuế khoản vay, chuyển tiền để bảo đảm hồ sơ vay, tài khoản yêu cầu vay bị sai hoặc thiếu thông tin; số tiền vay vượt quá định mức vay… Sau khi nạn nhân chuyển tiền thì các đối tượng nhanh chóng rút tiền khỏi tài khoản, khóa sim, cắt đứt liên lạc nhằm chiếm đoạt tài sản.

**4. Lừa tuyển cộng tác viên các sàn thương mại điện tử (Shopee, Sen Đỏ, Lazada, ...) hoặc ứng dụng Tiktok, tuyển việc làm tại nhà**

***Lợi dụng chức năng quảng cáo của các ứng dụng trên, các đối tượng đăng hàng loạt các bài tuyển cộng tác viên các sàn thương mại điện tử (Shopee, Tiki, Sendo, Lazada…), Tiktok. Làm các nhiệm vụ chuyển tiền thanh toán các đơn hàng tăng tương tác, doanh số…*** theo các đơn hàng bất kỳ mà chúng gửi, hứa hẹn trả tiền công và lợi nhuận cao từ 10% đến 30%. Nguy hiểm hơn là một số đối tượng hướng dẫn bị hại thực hiện các nhiệm vụ trên các trang web đánh bạc mà bị hại hoàn toàn không nhận thức được. Sau khi tạo dựng niềm tin cho bị hại bằng một số đơn hàng giá trị nhỏ thanh toán hoa hồng đầy đủ, chúng yêu cầu bị hại thanh toán đơn hàng giá trị lớn hơn, sau đó đưa ra các lý do người cộng tác vi phạm quy định như lỗi sai cú pháp, vượt quá định mức số tiền thanh toán trong ngày, quá hạn… dẫn đến bị khóa tài khoản và yêu cầu bị hại chuyển thêm nhiều lần tiền để bảo lãnh, xác minh tài khoản… thì mới cho rút lại tiền gốc và lãi. Đối tượng đưa bị hại vào tình trạng muốn lấy lại tiền, tiếc tiền nên phải theo cho đến khi hết khả năng thanh toán thì mới biết bị lừa.

Các đối tượng đăng tải bài viết trên các hội nhóm Tuyển việc làm với nội dung tuyển nhân viên làm các công việc tại gia đình như: Bóc tỏi, gia công quần áo, đánh máy vi tính, cắt mác quần áo… và rất nhiều thủ đoạn tương tự. Nhắm vào tâm lý của người dân cần các công việc làm thêm tại nhà hoặc các bà mẹ đang nuôi còn nhỏ cần thêm thu nhập, các đối tượng đăng tải các thông tin tuyển dụng cộng tác viên thực hiện các công việc có mức thu nhập từ 50.000đ đến 100.000đ/ngày hoặc đăng tuyển thông tin tuyển dụng lao động tại các công ty với mức thu nhập từ 7.000.000đ đến 8.000.000đ/tháng. Các thông tin, bài viết do các đối tượng đăng tải thường không rõ địa chỉ, mập mờ thông tin liên hệ hoặc yêu cầu người dân nhắn tin riêng.

Khi người dân liên hệ, các đối tượng yêu cầu người dân kết bạn bằng Zalo hoặc Telegram, sau đó các đối tượng yêu cầu người dân chuyển tiền đặt cọc để trở thành cộng tác viên hoặc dẫn dụ người dân tải các ứng dụng xem Tiktok, Facebook… và nạp tiền thực hiện nhiệm vụ với mục đích là để lừa đảo chiếm đoạt tài sản.

**5. Giả danh cơ quan chức năng để lừa đảo, chiếm đoạt tài sản.**

***Đối tượng gọi điện cho nạn nhân giả danh Tòa án, Viện Kiểm sát, Công an, Giáo viên trường học gọi điện đe dọa nạn nhân chuyển tiền vào tài khoản của đối tượng. Dưới đây là một số hình thức giả mạo cán bộ Cơ quan Nhà nước:***

**\* Giả danh Công an, Viện Kiểm sát, Tòa án đe dọa nạn nhận chuyển tiền cho đối tượng để điều tra**

Đối tượng gọi điện cho nạn nhân tự xưng là cán bộ Công an, cán bộ Viện kiểm sát thông báo bị hại có liên quan đến đường dây rửa tiền, buôn lậu ma túy mà Bộ Công an đang tiến hành điều tra....Sau đó, đối tượng gửi lệnh bắt, tạm giữ giả mạo và đe dọa nạn nhân kê khai tài chính, tài sản, tiền mặt hiện có, tiền trong tài khoản ngân hàng đồng thời đối tượng yêu cầu cung cấp thông tin liên quan tài khoản ngân hàng để phục vụ cho công tác điều tra, xác minh, hoặc nộp thêm tiền để chứng minh thu nhập. Nhiều bị hại do tâm lý lo sợ dẫn đến lầm tưởng các đối tượng là cán bộ Công an, Viện kiểm sát thật và sợ ảnh hưởng đến uy tín, danh dự của cá nhân và gia đình nên đã cung cấp các thông tin theo yêu cầu của đối tượng, nộp tiền vào tài khoản theo yêu cầu của đối tượng và bị các đối tượng chiếm đoạt.

**\* Giả danh Công an đe dọa người dân cài đặt ứng dụng VNeID giả mạo**

Đối tượng giả danh Cơ quan Công an gọi điện cho người dân hướng dẫn cài đặt ứng dụng ***VNeID (giả mạo)***, kích hoạt tài khoản định danh điện tử. Đối tượng lợi dụng sự không hiểu biết của người dân, gọi điện thoại sau đó gửi đường dẫn (link) qua các ứng dụng chat trực tuyến như Zalo, Messenger, Telegram…hướng dẫn người dân truy cập đường link để cài đặt phần mềm VNeID giả mạo có giao diện giống với ứng dụng VNeID thật. Sau khi người dân cài đặt ứng dụng VNeID giả mạo được cấp quyền truy cập mức cao (bao gồm cả đọc dữ liệu cá nhân và đọc tin nhắn chứa mã OTP), đối tượng kiểm soát được ứng dụng tài khoản ngân hàng sau đó thực hiện lệnh chuyển tiền trên điện thoại bị hại, thực hiện hành vi chiếm đoạt tài sản.

**\* Giả danh Giáo viên chủ nhiệm thông báo học sinh cấp cứu**

Các đối tượng sử dụng sim, số điện thoại “rác” gọi điện cho nhiều phụ huynh học sinh mạo danh giáo viên chủ nhiệm thông báo con, em mình bị tai nạn trong lúc đi học hiện đang được cấp cứu tại bệnh viện. Để tạo niềm tin, đối tượng tiếp theo sẽ giả danh bác sỹ hoặc nhân viên y tế gọi điện cho phụ huynh thông báo con, em mình đang trong tình trạng nguy hiểm cần phải phẫu thuật gấp nếu không sẽ ảnh hưởng đến tính mạng. Lợi dụng tâm lý hoang mang của phụ huynh, các đối tượng liên tục gây áp lực và yêu cầu phụ huynh phải chuyển tiền vào tài khoản ngân hàng do các đối tượng chỉ định để thực hiện phẫu thuật cho con, em mình. Bên cạnh những hình thức lừa đảo như: Giả mạo người nước ngoài làm quen tặng quà; Tuyển dụng việc làm tại nhà; Tuyển cộng tác viên cho Shopee, Lazada…thì hình thức trên mới xuất hiện gây tâm lý lo lắng cho các phụ huynh.

**\* Giả danh nhà mạng thông báo sim bị khoá, phải gửi tiền để tránh mất sim**

**6. Thủ đoạn lợi dụng tình cảm**

*Các đối tượng sử dụng các ứng dụng mạng xã hội như Facebook, Zalo… chủ động kết bạn với mục tiêu. Đối tượng lừa đảo tạo một hồ sơ giả mạo, sử dụng hình ảnh đánh cắp của người khác với ngoại hình đẹp và lôi cuốn, sau đó sử dụng các chiêu trò lừa đảo để thu hút sự quan tâm của nạn nhân, như: Giới thiệu bản thân là người nước ngoài đang độc thân (quân nhân nước ngoài, doanh nhân…). Đối tượng lừa đảo tạo một mối quan hệ tình cảm giả với nạn nhân bằng cách sử dụng các chiêu trò như tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa, như: Đưa nạn nhân sang nước ngoài để chung sống, hứa hẹn sẽ về Việt Nam để lập gia đình… Sau khi có được tình cảm của nạn nhân, đối tượng đề nghị nạn nhân một số yêu cầu của bọn chúng, như sau:*

**- Đối tượng lừa gửi tiền, hàng, bưu kiện có giá trị lớn**

Sau khi lấy được lòng tin từ bị hại, các đối tượng hứa hẹn sẽ chuyển tiền và món hàng có giá trị lớn cho bị hại. Khi bị hại nhận lời, các đối tượng khác giả danh nhân viên sân bay, hải quan, bưu điện, thuế... liên lạc với bị hại đe dọa bị hại phải chuyển tiền phải nộp các loại thuế, lệ phí, cước phí… để có thể nhận tiền, hàng hóa từ nước ngoài gửi về.

**- Đe dọa phát tán hình ảnh nhạy cảm để chiếm đoạt tài sản**

Đối tượng dẫn dụ nạn nhân thực hiện cuộc gọi video để trao đổi các hình ảnh, video khoả thân (chat sex) giữa nạn nhân và đối tượng nhằm mục đích ghi lại các tin nhắn, hình ảnh, video nhạy cảm của nạn nhân. Khi có được các hình ảnh, video nhạy cảm của nạn nhân, đối tượng thực hiện đe doạ cưỡng đoạt tài sản nếu nạn nhân không nộp đủ số tiền mà đối tượng yêu cầu thì đối tượng đe dọa đăng tải các hình ảnh nhạy cảm nạn nhân trên mạng xã hội và gửi cho bạn bè, người thân của nạn nhân.

**7. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa**

\* Các em cần chú ý, nhiều đối tượng lôi kéo, dụ dỗ mua bán các tài khoản ngân hàng để thực hiện hành vi lừa đảo chiếm đoạt tài sản

Nếu có ai hỏi mua TK ngân hàng kèm sim điện thoại phải chú ý không bị lôi kéo dụ dỗ, do thiếu hiểu biết có thể tiếp tay cho hành vi phạm tội.

***\* Trên đây là 1 số thủ đoạn lừa đảo chiếm đoạt tài sản và cách phòng ngừa để chúng ta không bị mất tài sản, có bạn nào có câu hỏi gì không?...***

***Nếu không có câu hỏi gì thì Công an huyện Bình Lục xin kết thúc buổi tuyên truyền tại đây, xin được chúc các thầy cô trong nhà trường đạt nhiều thành công trong công tác giảng dậy, chúc các em học sinh học tập thật tốt để trở thành công dân có ích cho xã hội.***

***Sau đây, xin mời các đ.c phát tài liệu cho các thầy cô và các em học sinh.***