Nhờ đơn vị chuyển cho UBND huyện

BỘ CÔNG AN **CÔNG AN TỈNH AN GIANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2058/TB-CAT-PC02 V/v thông báo phương thức, thủ đoạn của đối tượng lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao	*An Giang, ngày 24 tháng 5 năm 2022*

Kính gửi:
- Các sở, ban ngành tỉnh;
- UBND 11 huyện, thị xã, thành phố;
- Đài Phát thanh - Truyền hình An Giang;
- Báo An Giang.

Thời gian qua, Công an các đơn vị, địa phương trên toàn quốc đã chủ động tăng cường phòng ngừa, đấu tranh, xử lý hoạt động lừa đảo chiếm đoạt tài sản, đã khám phá nhiều chuyên án, vụ án lớn, bắt, khởi tố hàng trăm đối tượng, ngăn chặn và thu hồi số lượng lớn tài sản bị chiếm đoạt, được các ngành, các cấp ghi nhận và đánh giá cao, Nhân dân đồng tình ủng hộ, góp phần đảm bảo an ninh trật tự, hoạt động sản xuất, kinh doanh của doanh nghiệp được giữ vững, đời sống Nhân dân được nâng lên.

Tuy nhiên, tình hình tội phạm lừa đảo chiếm đoạt tài sản thông qua mạng viễn thông, mạng intenet, mạng xã hội tiếp tục diễn biến phức tạp, xảy ra trên toàn quốc với nhiều thủ đoạn hoạt động mới, tinh vi, gây thiệt hại lớn về tài sản của người dân, gây bức xúc trong dư luận xã hội. Theo Thông báo của của Cục Cảnh sát hình sự - Bộ Công an tại Công văn số 1200/C02-P9 ngày 29/4/2022 và tình hình thực tế tại địa phương, Công an tỉnh xin thông báo một số phương thức, thủ đoạn nổi lên của các đối tượng lừa đảo chiếm đoạt tài sản như sau:

1. Đối tượng giả danh các nhà mạng gọi điện thông báo số thuê bao điện thoại của bạn đã trúng thưởng tài sản có giá trị lớn, để nhận được tài sản đó phải mất phí, nếu đồng ý thì mua thẻ cào nạp vào số tài khoản mà các đối tượng lừa đảo cung cấp, khi người dân đóng tiền vào để nhận thưởng thì các đối tượng chặn liên lạc và chiếm đoạt số tiền đó.

2. Đối tượng sử dụng mạng xã hội (qua Facebook, Zalo, Viber…) để kết bạn, thông báo gửi quà, sau đó giả danh nhân viên sân bay, hải quan, thuế yêu cầu nộp tiền để nhận quà rồi chiếm đoạt.

3. Đối tượng giả danh là cán bộ Ngân hàng gọi điện cho bị hại thông báo bị hại có người chuyển tiền vào tài khoản nhưng do bị lỗi nên chưa chuyển được hoặc thông báo phần mềm chuyển tiền Internet Banking của khách hàng bị lỗi…nên yêu cầu khách hàng cung cấp mã số thẻ và mã OTP để kiểm tra. Các đối tượng sử dụng thông tin bị hại cung cấp để truy cập vào tài khoản và rút tiền của bị hại.

4. Giả danh Công an, Tòa án gọi điện thông báo người dân có liên quan đến vụ án hoặc xử phạt nguội vi phạm giao thông, yêu cầu bị hại chuyển tiền vào tài

khoản mà các đối tượng lừa đảo đưa ra để phục vụ công tác điều tra, xử lý. Khi người dân do lo sợ và chuyển tiền vào tài khoản các đối tượng yêu cầu thì các đối tượng chuyển tiếp số tiền đó vào nhiều tài khoản khác và chiếm đoạt. Đã xảy ra nhiều vụ với số tiền bị chiếm đoạt rất lớn, từ vài tỷ đến hàng chục tỷ đồng.

5. Lợi dụng sự nhẹ dạ cả tin và nhu cầu kiếm tiền nhanh của bị hại, các đối tượng giả mạo tuyển cộng tác viên xử lý đơn hàng cho các sàn thương mại điện tử để thực hiện hành vi chiếm đoạt tài sản. Bằng thủ đoạn lập các trang Facebook giả mạo các nhãn hàng, trang thương mại điện tử như: Tiki.vn, Lazada, TokyoLive, Shopee... và chạy quảng cáo, khi bị hại nhắn tin hỏi cách thức làm cộng tác viên, các đối tượng sẽ gửi các thông tin về công ty, nhân viên chăm sóc khách hàng... và yêu cầu gửi thông tin cá nhân, kết bạn Zalo để tư vấn. Ban đầu đối tượng gửi đường dẫn các sản phẩm có giá trị nhỏ khoảng vài trăm ngàn đồng để bị hại chọn và xác thực đơn, chụp ảnh đơn hàng gửi cho đối tượng qua Zalo, Facebook chuyển tiền vào các tài khoản do đối tượng cung cấp và được đối tượng chuyển lại toàn bộ số tiền đã bỏ ra mua hàng cùng với hoa hồng từ 3-20%. Sau một số lần tạo niềm tin bằng cách trả gốc và hoa hồng như cam kết ban đầu, tiếp theo đối tượng viện lý do là "bạn đã được công ty nâng hạng" và gửi các đường dẫn sản phẩm trên sàn Lazada, Shopee... có giá trị lớn hơn và tiếp tục yêu cầu bị hại chụp lại hình ảnh sản phẩm đồng thời chuyển tiền. Khi đã nhận được, đối tượng không chuyển tiền mà tiếp tục thông báo cho cộng tác viên phải tiếp tục thực hiện nhiệm vụ khác thì mới được chuyển lại tiền và hoa hồng (thực chất là tiếp tục chuyển tiền vào tài khoản đối tượng). Sau đó các đối tượng chiếm đoạt tiền của bị hại.

6. 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 (Facebook, Zalo, Viber…) mạo danh. Sau đó 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; hoặc đối tượng lừa đảo sử dụng hack (chiếm đoạt quyền điều khiển) tài khoản xã hội sau đó tạo ra kịch bản nhắn tin lừa đảo đến bạn bè, người thân (vay, mượn tiền..) của chủ tài khoản mạng xã hội và chiếm đoạt tiền của các bị hại chuyển đến tài khoản ngân hàng do các đối tượng chỉ định.

7. Lừa đảo thông qua các sàn giao dịch trên mạng. Các đối tượng mời chào, lôi kéo bị hại tham gia đầu tư vào các sàn giao dịch tiền ảo, do đối tượng thiết lập, cam kết sẽ hưởng lợi nhuận cao khi tham gia hệ thống. Các đối tượng thường quảng bá, đánh bóng tên tuổi bằng cách đăng tin, bài trên mạng xã hội, tổ chức các buổi hội thảo, gặp mặt offline, tự nhận là chuyên gia đầu tư, người truyền cảm hứng, người dẫn đường… để lừa đảo, kêu gọi đầu tư vào hệ thống do chúng thiết lập. Khi huy động được lượng tiền đủ lớn, các đối tượng sẽ can thiệp vào các giao dịch, điều chỉnh thắng thua hoặc báo lỗi, ngừng hoạt động (sập sàn) để chiếm đoạt tiền của nguời tham gia.

8. Thủ đoạn cho vay tiền qua app (vay tiền online). Lợi dụng tâm lý vay tiền online thuận lợi, nhanh chóng, không phải ra ngân hàng làm thủ tục, các đối tượng lập ra các trang trên mạng xã hội (zalo, facebook...) chạy quảng cáo để tiếp

cận các bị hại. Sau khi tiếp cận được nạn nhân, các đối tượng sẽ gửi các đường link kết nối với CH Play để các bị hại cài đặt ứng dụng vào điện thoại và làm theo ứng dụng của App. Sau đó, khi bị hại đăng nhập App để vay tiền thì app sẽ báo lỗi, các đối tượng yêu cầu bị hại phải chuyển tiền đặt cọc để mở lại App thì mới giải ngân được (sau khi giải ngân thì sẽ trả lại tiền cọc và tiền cho vay), hoặc các đối tượng yêu cầu nạn nhân mua bảo hiểm khoản vay, đóng tiền phí giải ngân... Nhiều bị hại thực hiện chuyển nhiều lần để được vay cho đến khi nghi ngờ bị lừa không chuyển nửa thì các đối tượng lừa đảo thông báo nếu không chuyển nửa thì không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

9. Lợi dụng tình hình dịch Covid-19 để lừa đảo chiếm đoạt tài sản. Các đối tượng tạo các tài khoản mạng xã hội để đăng bán các dụng cụ, thiết bị y tế chống dịch... Khi bị hại kết nối và đặt cọc hoặc thanh toán số tiền theo thỏa thuận, các đối tượng chặn liên hệ, đổi số điện thoại và chiếm đoạt số tiền đã nhận được; hoặc lợi dụng nhu cầu người dân từ nước ngoài về nước gia tăng, các đối tượng tạo lập các tài khoản mạng xã hội giả để đăng tin trên các trang, hội nhóm... để đăng bán vé máy bay cho người dân có nhu cầu từ nước ngoài về nước. Khi bị hại hỏi mua, thỏa thuận xong giá cả thì các đối tượng yêu cầu thanh toán và đồng thời gửi cho khách hàng các hình ảnh giả về vé máy bay do các đối tượng tự tạo ra, sau đó chiếm đoạt số tiền bị hại thanh toán.

Do đó, Công an tỉnh đề nghị lãnh đạo các sở, ban ngành tỉnh và UBND cấp huyện tiếp tục chỉ đạo thực hiện nghiêm Kế hoạch 415/KH-UBND, ngày 22/7/2020 của UBND tỉnh An Giang triển khai thực hiện Chỉ thị 21/CT-TTg của Thủ tướng Chính phủ về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản; đẩy mạnh tuyên truyền, thông báo rộng rãi phương thức, thủ đoạn lừa đảo chiếm đoạt tài sản bằng hình thức sử dụng công nghệ cao như đã nêu trên để cán bộ, công nhân, viên chức và quần chúng Nhân dân nâng cao ý thức cảnh giác, chủ động phòng ngừa. Nếu phát hiện trường hợp như trên, tuyệt đối không cung cấp thông tin cá nhân, tài khoản hoặc nộp tiền, phí theo yêu cầu và báo ngay cho cơ quan Công an gần nhất để phối hợp điều tra, xử lý./.

Nơi nhận:
- Như trên;
- TT. UBND tỉnh;
- VP UBND tỉnh;
- Lưu: VT, PC02(Đ2).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH AN GIANG

Đại tá Bùi Tấn Ân

PHỤ LỤC

MỘT SỐ THỦ ĐOẠN LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN QUA MẠNG VIỄN THÔNG, MẠNG INTERNET, MẠNG XÃ HỘI

1. Đối tượng giả danh các nhà mạng gọi điện thông báo số thuê bao điện thoại của bạn đã trúng thưởng tài sản có giá trị lớn, để nhận được tài sản đó phải mất phí, nếu đồng ý thì mua thẻ cào nạp vào số tài khoản mà các đối tượng lừa đảo cung cấp, khi người dân đóng tiền vào để nhận thưởng thì các đối tượng chặn liên lạc và chiếm đoạt số tiền đó.

2. Đối tượng sử dụng mạng xã hội (qua Facebook, Zalo, Viber…) để kết bạn, thông báo gửi quà, sau đó giả danh nhân viên sân bay, hải quan, thuế yêu cầu nộp tiền để nhận quà rồi chiếm đoạt.

3. Đối tượng giả danh là cán bộ Ngân hàng gọi điện cho bị hại thông báo bị hại có người chuyển tiền vào tài khoản nhưng do bị lỗi nên chưa chuyển được hoặc thông báo phần mềm chuyển tiền Internet Banking của khách hàng bị lỗi… nên yêu cầu khách hàng cung cấp mã số thẻ và mã OTP để kiểm tra. Các đối tượng sử dụng thông tin bị hại cung cấp để truy cập vào tài khoản và rút tiền của bị hại.

4. Giả danh Công an, Tòa án gọi điện thông báo người dân có liên quan đến vụ án hoặc xử phạt nguội vi phạm giao thông, yêu cầu bị hại chuyển tiền vào tài khoản mà các đối tượng lừa đảo đưa ra để phục vụ công tác điều tra, xử lý. Khi người dân do lo sợ và chuyển tiền vào tài khoản các đối tượng yêu cầu thì các đối tượng chuyển tiếp số tiền đó vào nhiều tài khoản khác và chiếm đoạt. Đã xảy ra nhiều vụ với số tiền bị chiếm đoạt rất lớn, từ vài tỷ đến hàng chục tỷ đồng.

5. Lợi dụng sự nhẹ dạ cả tin và nhu cầu kiếm tiền nhanh của bị hại, các đối tượng giả mạo tuyển cộng tác viên xử lý đơn hàng cho các sàn thương mại điện tử để thực hiện hành vi chiếm đoạt tài sản. Bằng thủ đoạn lập các trang Facebook giả mạo các nhãn hàng, trang thương mại điện tử như: Tiki.vn, Lazada, TokyoLive, Shopee... và chạy quảng cáo, khi bị hại nhắn tin hỏi cách thức làm cộng tác viên, các đối tượng sẽ gửi các thông tin về công ty, nhân viên chăm sóc khách hàng... và yêu cầu gửi thông tin cá nhân, kết bạn Zalo để tư vấn. Ban đầu đối tượng gửi đường dẫn các sản phẩm có giá trị nhỏ khoảng vài trăm ngàn đồng để bị hại chọn và xác thực đơn, chụp ảnh đơn hàng gửi cho đối tượng qua Zalo, Facebook chuyển tiền vào các tài khoản do đối tượng cung cấp và được đối tượng chuyển lại toàn bộ số tiền đã bỏ ra mua hàng cùng với hoa hồng từ 3-20%. Sau một số lần tạo niềm tin bằng cách trả gốc và hoa hồng như cam kết ban đầu, tiếp theo đối tượng viện lý do là "bạn đã được công ty nâng hạng" và gửi các đường dẫn sản phẩm trên sàn Lazada, Shopee... có giá trị lớn hơn và tiếp tục yêu cầu bị hại chụp lại hình ảnh sản phẩm đồng thời chuyển tiền. Khi đã nhận được, đối tượng không chuyển tiền mà tiếp tục thông báo cho cộng tác viên phải tiếp tục thực hiện nhiệm vụ khác thì mới được chuyển lại tiền và hoa hồng (thực chất là tiếp tục chuyển tiền vào tài khoản đối tượng). Sau đó các đối tượng chiếm đoạt tiền của bị hại.

6. 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 (Facebook,

Zalo, Viber…) mạo danh. Sau đó 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; hoặc đối tượng lừa đảo sử dụng hack (chiếm đoạt quyền điều khiển) tài khoản xã hội sau đó tạo ra kịch bản nhắn tin lừa đảo đến bạn bè, người thân (vay, mượn tiền..) của chủ tài khoản mạng xã hội và chiếm đoạt tiền của các bị hại chuyển đến tài khoản ngân hàng do các đối tượng chỉ định.

7. Lừa đảo thông qua các sàn giao dịch trên mạng. Các đối tượng mời chào, lôi kéo bị hại tham gia đầu tư vào các sàn giao dịch tiền ảo,... do đối tượng thiết lập, cam kết sẽ hưởng lợi nhuận cao khi tham gia hệ thống. Các đối tượng thường quảng bá, đánh bóng tên tuổi bằng cách đăng tin, bài trên mạng xã hội, tổ chức các buổi hội thảo, gặp mặt offline, tự nhận là chuyên gia đầu tư, người truyền cảm hứng, người dẫn đường... để lừa đảo, kêu gọi đầu tư vào hệ thống do chúng thiết lập. Khi huy động được lượng tiền đủ lớn, các đối tượng sẽ can thiệp vào các giao dịch, điều chỉnh thắng thua hoặc báo lỗi, ngừng hoạt động (sập sàn) để chiếm đoạt tiền của nguời tham gia.

8. Thủ đoạn cho vay tiền qua app (vay tiền online). Lợi dụng tâm lý vay tiền online thuận lợi, nhanh chóng, không phải ra ngân hàng làm thủ tục, các đối tượng lập ra các trang trên mạng xã hội (zalo, facebook...) chạy quảng cáo để tiếp cận các bị hại. Sau khi tiếp cận được nạn nhân, các đối tượng sẽ gửi các đường link kết nối với CH Play để các bị hại cài đặt ứng dụng vào điện thoại và làm theo ứng dụng của Aap. Sau đó, khi bị hại đăng nhập app để vay tiền thì app sẽ báo lỗi, các đối tượng yêu cầu bị hại phải chuyển tiền đặt cọc để mở lại aap thì mới giải ngân được (sau khi giải ngân thì sẽ trả lại tiền cọc và tiền cho vay), hoặc các đối tượng yêu cầu nạn nhân mua bảo hiểm khoản vay, đóng tiền phí giải ngân... Nhiều bị hại thực hiện chuyển nhiều lần để được vay cho đến khi nghi ngờ bị lừa không chuyển nửa thì các đối tượng lừa đảo thông báo nếu không chuyển nửa thì không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

9. Lợi dụng tình hình dịch covid 19 để lừa đảo chiếm đoạt tài sản. Các đối tượng tạo các tài khoản mạng xã hội để đăng bán các dụng cụ, thiết bị y tế chống dịch... Khi bị hại kết nối và đặt cọc hoặc thanh toán số tiền theo thỏa thuận, các đối tượng chặn liên hệ, đổi số điện thoại... và chiếm đoạt số tiền đã nhận được; hoặc lợi dụng nhu cầu người dân từ nước ngoài về nước gia tăng, các đối tượng tạo lập các tài khoản mạng xã hội giả để đăng tin trên các trang, hội nhóm... để đăng bán vé máy bay cho người dân có nhu cầu từ nước ngoài về nước. Khi bị hại hỏi mua, thỏa thuận xong giá cả thì các đối tượng yêu cầu thanh toán và đồng thời gửi cho khách hàng các hình ảnh giả về vé máy bay do các đối tượng tự tạo ra, sau đó chiếm đoạt số tiền bị hại thanh toán.

PHÒNG CẢNH SÁT HÌNH SỰ