ỦY BAN NHÂN DÂN **TỈNH KIÊN GIANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1736/UBND-NC V/v thực hiện công tác phòng, chống tội phạm sử dụng công nghệ cao	*Kiên Giang, ngày 23 tháng 9 năm 2022*

Kính gửi:
- Giám đốc, Thủ trưởng các sở, ban, ngành cấp tỉnh (Đảng, chính quyền, đoàn thể);
- Chủ tịch Ủy ban nhân dân các huyện, thành phố.

Theo báo cáo của Công an tỉnh, trong 6 tháng đầu năm 2022 tội phạm lợi dụng không gian mạng xâm phạm trật tự xã hội trên địa bàn tỉnh diễn biến phức tạp, nổi lên một số thủ đoạn sau:

- Sử dụng không gian mạng để lừa đảo, chiếm đoạt tài sản: Phát hiện 02 vụ đối tượng giả danh là cán bộ các cơ quan chức năng thông báo điều tra, nạn nhân lo sợ và chuyển tiền vào tài khoản do đối tượng cung cấp và bị chiếm đoạt; 01 vụ đối tượng tạo lập website giả mạo trang thương mại điện tử Shopee, tự xưng là nhân viên Shopee, sử dụng mạng xã hội lôi kéo nạn nhân làm cộng tác viên kinh doanh online, yêu cầu nạn nhân nạp tiền thực hiện nhiệm vụ thanh toán đơn hàng trước và được hưởng hoa hồng, đến khi nạn nhân nạp số tiền lớn thì bị chiếm đoạt; 02 vụ đối tượng chiếm quyền tài khoản mạng xã hội (Zalo, Facebook), giả mạo chủ tài khoản để nhắn tin mượn tiền rồi chiếm đoạt; 01 vụ đối tượng lập website giả mạo giao diện trang web chính thức của ngân hàng cho vay vốn online, lôi kéo người cần vay chuyển tiền vào tài khoản ngân hàng do đối tượng cung cấp rồi chiếm đoạt; 03 vụ lôi kéo nạn nhân chuyển khoản đầu tư giao dịch tiền ảo, chứng khoán do các đối tượng tự tạo lập sau đó gây lỗi để chiếm đoạt tiền.

- Tổ chức đánh bạc và đánh bạc trực truyến theo hình thức quyền chọn nhị phân BO: Phát hiện 02 vụ đối tượng lôi kéo người chơi đầu tư vào các sàn ngoại hối do đối tượng tổ chức thiết lập, người chơi lựa chọn cặp ngoại hối, tiền kỹ thuật số để đặt cược tăng hay giảm trong một đơn vị thời gian; khi đặt cược thắng, người chơi nhận về số tiền bằng số tiền cược sau khi trừ đi phí của sàn, nếu thua, người chơi sẽ mất toàn bộ tiền đã đặt cược.

- Phát hiện 02 vụ có dấu hiệu cho vay lãi nặng với thủ đoạn quảng cáo cho người dân vay tiền trực tuyến qua các App trên điện thoại di động (với số tiền cho vay từ 01 đến 05 triệu đồng trên 01 App); khi người vay không có khả năng chi trả, các đối tượng gọi điện, đăng hình ảnh xúc phạm danh dự, nhân phẩm của người vay, bạn bè, người thân, đồng nghiệp trên mạng xã hội để khủng bố tinh thần, đe dọa tính mạng,... gây áp lực để buộc người vay trả nợ.

Đáng chú ý, xảy ra các trường hợp nạn nhân của các vụ lừa đảo, chiếm đoạt tài sản, người đánh bạc, người vay tiền qua App,... công tác, làm việc trong các cơ quan, tổ chức trên địa bàn tỉnh. Điển hình như: (1) Vụ việc cán bộ Văn phòng Huyện ủy Kiên Lương vay tiền qua website, các đối tượng cho vay đã cắt ghép hình ảnh, xúc phạm lãnh đạo tỉnh Kiên Giang, huyện Kiên Lương và gia đình người vay,... để gây áp lực buộc trả nợ; (2) Vụ việc nhân viên hợp đồng Bệnh viện Ung bướu tỉnh vay tiền qua App, các đối tượng cho vay đã nhiều lần gọi điện thoại, nhắn tin cho Kế toán trưởng và lãnh đạo Bệnh viện Ung bướu tỉnh với từ ngữ, lời lẽ đe dọa, thô tục để gây áp lực buộc nhân viên này trả nợ; (3) Vụ việc nguyên Chủ tịch UBND xã Cửa Dương bị các đối tượng giả danh Công an, Viện Kiểm sát lừa đảo chiếm đoạt 1,9 tỷ đồng.

Để phòng, chống tội phạm sử dụng công nghệ cao, trên cơ sở đề xuất của Công an tỉnh, UBND tỉnh đề nghị Giám đốc, Thủ trưởng các sở, ban, ngành cấp tỉnh (Đảng, chính quyền, đoàn thể) và Chủ tịch UBND các huyện, thành phố theo chức năng, nhiệm vụ thực hiện một số nội dung sau:

1. Tuyên truyền, giáo dục cán bộ, công chức, viên chức, người lao động trong cơ quan và người dân về phương thức, thủ đoạn lợi dụng không gian mạng để lừa đảo, chiếm đoạt tài sản; các biện pháp phòng ngừa (có nội dung tuyên truyền kèm theo). Không tham gia cá cược, đánh bạc trái phép dưới mọi hình thức; vay tiền trực tuyến qua App cho vay không hợp pháp.

2. Xem xét hình thức xử lý kỷ luật cán bộ, công chức, viên chức, người lao động đối với các trường hợp cá cược, đánh bạc trái phép; vay tiền trực tuyến gây ảnh hưởng đến hoạt động ổn định của cơ quan, tổ chức.

Giám đốc, Thủ trưởng các sở, ban, ngành cấp tỉnh (Đảng, chính quyền, đoàn thể) và Chủ tịch UBND các huyện, thành phố căn cứ vào nội dung Công văn này và tình hình thực tế của ngành, địa phương để tổ chức triển khai thực hiện, nâng cao hiệu quả công tác phòng, chống tội phạm sử dụng công nghệ cao trong tình hình hiện nay./.

Nơi nhận:
- Như trên;
- CT, các PCT UBND tỉnh;
- Công an tỉnh (qua Phòng AN mạng và PCTP sử dụng công nghệ cao);
- Lãnh đạo VP, P. NC, KGVX;
- Lưu: VT, CA tỉnh, hvlu.

CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH KIÊN GIANG

Lâm Minh Thành

NỘI DUNG TUYÊN TRUYỀN, PHỔ BIẾN
Nhận diện thủ đoạn; cách phòng, chống hoạt động lừa đảo qua điện thoại và trên không gian mạng
(Kèm theo Công văn số 1736/UBND-NC ngày 23 / 9 /2022 của Ủy ban nhân dân tỉnh)

---

1. Nhận diện 12 thủ đoạn phổ biến

1.1. Đối tượng giả danh là cán bộ Công an, Viện Kiểm sát, Tòa án gọi điện thông báo với chủ thuê bao việc có liên quan đến vụ án hình sự để khai thác các thông tin cá nhân và tài khoản ngân hàng; sau đó yêu cầu nạn nhân phải chuyển toàn bộ tiền có trong tài khoản cho chúng với lý do kiểm tra nguồn gốc, sẽ trả lại sau và đe dọa nếu không chuyển tiền sẽ bị bắt giam, nhằm thực hiện hành vi lừa đảo chiếm đoạt tài sản.

1.2. Đối tượng sử dụng SIM điện thoại đăng ký không chính chủ hoặc thông qua mạng xã hội Facebook, Zalo mạo danh các công ty viễn thông gửi tin nhắn thông báo khách hàng trúng các phần thưởng có giá trị như: Vật có giá trị, tiền mặt số lượng lớn,...; yêu cầu nạn nhân gửi tiền vào các tài khoản ngân hàng do chúng chuẩn bị trước hoặc mua các thẻ cào điện thoại để chuyển cho chúng làm thủ tục nhận thưởng, nhằm thực hiện hành vi lừa đảo chiếm đoạt tài sản.

1.3. Đối tượng sử dụng SIM điện thoại đăng ký không chính chủ giả danh nhân viên ngân hàng gọi điện thông báo có chương trình tri ân khách hàng, đề nghị nạn nhân cung cấp số điện thoại đăng ký dịch vụ internet banking và mã xác thực OTP (là mã do ngân hàng cung cấp để thực hiện giao dịch chuyển nhận tiền) để nhận quà tặng là một khoản tiền có giá trị lớn từ ngân hàng; sau khi nạn nhân cung cấp các thông tin này chúng chiếm quyền sử dụng dịch vụ internet banking và chuyển toàn bộ số tiền có trong tài khoản ngân hàng của nạn nhân sang tài khoản chúng đã chuẩn bị trước để chiếm đoạt.

1.4. Sử dụng SIM đăng ký không chính chủ, mạo danh nhân viên nhà mạng gọi điện, nhắn tin cho chủ thuê bao, lấy lý do hỗ trợ khách hàng nâng cấp SIM từ 3G lên 4G, yêu cầu khách hàng làm theo cú pháp, truy cập đường link do chúng cung cấp. Nếu làm theo, SIM của chủ thuê bao sẽ bị khóa, thông tin của số thuê bao được chuyển sang SIM mới của đối tượng. Trong thời gian chiếm quyền kiểm soát SIM, đối tượng bẻ khóa, truy cập vào các tài khoản của chủ thuê bao gắn với số điện thoại cá nhân, nhất là tài khoản thẻ tín dụng. Mục đích chiếm quyền sử dụng số điện thoại để phá bảo mật, nhận mã OTP từ nhà cung cấp dịch vụ hay ngân hàng để có thể bẻ khóa, xâm nhập chiếm đoạt tài sản trong tài khoản.

1.5. Qua mạng xã hội Facebook, đối tượng giới thiệu là người nước ngoài kết bạn, làm quen với nạn nhân, sau đó tán tỉnh, yêu đương, đề nghị chuyển quà như: Trang sức, mỹ phẩm và ngoại tệ số lượng lớn qua đường hàng không về Việt Nam để làm quà tặng; tiếp theo giả danh nhân viên sân bay yêu cầu nạn nhân chuyển tiền vào tài khoản ngân hàng cho chúng với lý do làm thủ tục nhận hàng, nhằm thực hiện hành vi lừa đảo chiếm đoạt tài sản.

1.6. Đối tượng hack các tài khoản Facebook, sử dụng mạo danh chủ tài khoản nhắn tin đề nghị người nhà mua thẻ cào điện thoại gửi cho chúng hoặc mượn tiền và yêu cầu gửi vào các tài khoản ngân hàng do chúng cung cấp để thực hiện hành vi chiếm đoạt.

1.7. Đối tượng gọi điện đến các thuê bao di động, hoặc qua mạng xã hội giới thiệu là có người nhà làm trong các công ty xổ số có khả năng biết trước kết quả, sau đó đối tượng gửi số lô, số đề; hứa cung cấp tiền để nạn nhân mua số lô, số đề, chia phần trăm hoa hồng cho đối tượng; sau đó đối tượng thông tin hết tiền, đề nghị nạn nhân ứng tiền mua số lô, số đề. Nếu may mắn trúng số lô, số đề, nạn nhân gửi tiền hoa hồng cho đối tượng và bị chiếm đoạt.

1.8. Đối tượng tạo ra các ứng dụng, website cho vay tiền, quảng cáo trên mạng xã hội (Facebook, Zalo) với mục đích tìm người muốn vay tiền để thực hiện hành vi lừa đảo. Sau khi người muốn vay tiền tải ứng dụng về điện thoại; đăng nhập thông tin theo yêu cầu, thì hệ thống website gửi tin nhắn qua Facebook, Zalo trực tuyến tại bộ phận xét duyệt và thông báo nếu muốn vay tiền thì người vay phải đóng lãi số tiền vay trước thì mới được gửi mã mật khẩu để rút tiền. Sau khi người vay tiền chuyển tiền vào tài khoản do các đối tượng cung cấp thì hệ thống thông báo người chuyển tiền nhập sai số tài khoản nên bị đóng băng và yêu cầu người vay phải chuyển thêm tiền để kích hoạt lại tài khoản. Số lần yêu cầu người vay tiền chuyển khoản thường không có giới hạn; toàn bộ số tiền người vay chuyển khoản vào tài khoản của các đối tượng chuẩn bị trước bị chiếm đoạt.

1.9. Đối tượng tạo lập các trang, tài khoản mạng xã hội (chủ yếu trên Zalo, Facebook), sau đó đăng tải các bài viết, tạo dựng, cung cấp những nội dung không có thật về cơ quan, tổ chức, cá nhân đang gặp hoàn cảnh khó khăn cần sự hỗ trợ, giúp đỡ; cung cấp tài khoản ngân hàng, đề nghị, kêu gọi chuyển tiền trợ giúp. Nếu người muốn trợ giúp chuyển tiền thì bị đối tượng chiếm đoạt.

1.10. Đối tượng lập công ty, website tổ chức kinh doanh sàn ngoại hối (forex), tiền điện tử (altcoin). Để thu hút "nhà đầu tư", đối tượng đưa những người tự xưng là chuyên gia về lĩnh vực tài chính, làm quen rồi chia sẻ kinh nghiệm, gọi điện thoại trực tiếp hoặc thông qua mạng xã hội mời người dân tham gia. Các đối tượng khẳng định lợi nhuận rất cao, khi người dân tham gia, nộp tiền để "đầu tư" thì bị chiếm đoạt.

1.11. Các đối tượng kết nối, giao tiếp với nạn nhân với nội dung tuyển dụng việc làm online. Sau khi nạn nhân liên lạc, đồng ý thì đối tượng giao việc ứng tiền của nạn nhân để chuyển đến các tài khoản do đối tượng chỉ định, sau khi thực hiện thành công, các đối tượng chuyển khoản trả cả tiền gốc và tiền công cho nạn nhân (với số tiền công lớn để tạo lòng tin của nạn nhân). Sau một vài giao dịch thành công, do được hưởng lợi lớn và tin tưởng đối tượng sẽ chuyển trả lại tiền nên các nạn nhân đã thực hiện chuyển số tiền lớn đến các tài khoản ngân hàng theo yêu cầu của đối tượng. Sau đó đối tượng không chuyển trả tiền như đã hứa hẹn và cắt liên lạc với nạn nhân.

1.12. Đối tượng sử dụng thông tin cá nhân giả mạo đăng ký các tài khoản mạng xã hội (Facebook, Zalo). Sau đó tìm kiếm những người bán hàng (hải sản, nông sản, khách sạn,...) trên mạng xã hội để kết bạn và nhắn tin mua hàng. Sau khi người bán hàng đồng ý, thì các đối tượng sẽ yêu cầu người bán hàng gửi thông tin tài khoản ngân hàng có đăng ký dịch vụ Internet banking, số điện thoại của mình cho đối tượng. Sau khi nhận được thông tin, đối tượng sẽ tạo cớ chuyển tiền mua hàng không thành công, đề nghị người bán hàng truy cập vào trang web giả mạo của ngân hàng để nhập đầy đủ thông tin như: Tên tài khoản, số tài khoản và mã OTP để hoàn tất thủ tục nhận tiền. Khi nạn nhân nhập thông tin và mã OTP thì các đối tượng chiếm quyền sử dụng dịch vụ Internet banking của tài khoản ngân hàng đó và ngay lập tức sẽ rút toàn bộ số tiền trong tài khoản của nạn nhân chuyển tới tài khoản khác để chiếm đoạt.

2. Nội dung hướng dẫn, khuyến cáo cách phòng, chống

- Không công khai các thông tin cá nhân như: Ngày, tháng, năm sinh; số chứng minh nhân dân hoặc căn cước công dân; số điện thoại, số tài khoản ngân hàng,... lên các trang mạng xã hội, để tránh bị các đối tượng lợi dụng khai thác, sử dụng thủ đoạn lừa đảo. Khi chia sẻ thông tin trên mạng xã hội cần chọn lọc những thông tin có thể chia sẻ công khai, thông tin giới hạn người xem.

- Cảnh giác, không tin tưởng vào những chiêu trò nhận thưởng qua mạng mà yêu cầu nạp tiền thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Tìm hiểu kỹ thông tin khi kết bạn với những người lạ trên mạng xã hội, đặc biệt là những người hứa hẹn cho, tặng số tiền lớn, những món quà đắt tiền.

- Cảnh giác với những trang web giả mạo dịch vụ chuyển tiền quốc tế, trang web ngân hàng,... Lưu ý chỉ nên nhập thông tin tài khoản ngân hàng trên các trang web chính thức của ngân hàng có uy tín.

- Không cung cấp mã OTP do ngân hàng gửi cho bất kỳ ai, kể cả nhân viên ngân hàng.

- Đối với các tin nhắn qua mạng xã hội, qua điện thoại người thân, bạn bè, người quen,... nhờ mua thẻ cào điện thoại, nhờ chuyển tiền hộ cần gọi điện trực tiếp để xác nhận thông tin với người nhờ, không nói chuyện qua tin nhắn.

- Chặn số điện thoại, tin nhắn đối với các số điện thoại, tài khoản mạng xã hội gọi điện, nhắn tin quấy nhiễu, hoặc có dấu hiệu lừa đảo, chiếm đoạt tài sản.

- Đối với các cá nhân có nhu cầu chuyển - nhận tiền từ nước ngoài về chỉ gửi, nhận thông qua ngân hàng có uy tín, không sử dụng các dịch vụ chuyển, đổi tiền quốc tế của cá nhân không hợp pháp.

- Khi phát hiện SIM điện thoại bị vô hiệu hóa, cần gọi ngay cho bộ phận dịch vụ chăm sóc khách hàng của nhà mạng để yêu cầu hỗ trợ, xác minh. Nếu mất điện thoại, cần báo nhà mạng khóa SIM ngay.

- Các cá nhân không mở hộ, cho thuê, bán tài khoản ngân hàng của mình cho người khác, đặc biệt là những đối tượng không quen biết. Trong nhiều trường hợp, các đối tượng lợi dụng tài khoản ngân hàng (do mua, mượn, thuê được) để chiếm đoạt tài sản của người khác. Đây là hành vi trực tiếp tiếp tay cho các đối tượng lừa đảo chiếm đoạt tài sản và sẽ bị xử lý theo quy định của pháp luật. Khi phát hiện đối tượng có hành vi mua, thuê người khác mở tài khoản ngân hàng cần báo cho cơ quan Công an gần nhất để phối hợp xử lý.

- Cần thận trọng tìm hiểu, kiểm chứng kỹ các thông tin đăng tải kêu gọi ủng hộ từ thiện trên các trang mạng xã hội; yêu cầu công khai, minh bạch thông tin về người cần giúp đỡ hoặc liên hệ với chính quyền địa phương, bệnh viện nơi họ điều trị để kiểm chứng thông tin.

- Các tổ chức, cá nhân quản trị, môi giới, lôi kéo người dân tham gia sàn ngoại hối, tiền điện tử hiện nay tại Việt Nam hoàn toàn không đúng với quy định của pháp luật, việc người dân đưa tiền vào đầu tư là rủi ro. Cần thận trọng khi tham gia các hoạt động đầu tư, kinh doanh trên mạng./.