DONGA Bank

HƯỚNG DẪN NHẬN BIẾT CÁC HÀNH VI LỪA ĐẢO TRỰC TUYẾN

1. Các mối đe dọa trên không gian mạng:

1.1. Lừa đảo tài chính: thường bắt đầu bằng một tin nhắn hoặc thư điện tử (email) từ một người lạ có hình thức như được gửi trực tiếp tới người nhận để đưa ra đề xuất thực hiện theo yêu cầu từ người gửi, từ đó người nhận sẽ nhận được một khoản tiền lớn nhưng thực tế thì người nhận sẽ không thể nhận được hoặc bị mất tiền/ tài sản nếu làm theo yêu cầu.

1.2. Trộm danh tính: là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính, chủ yếu là lấy trộm thông tin thẻ tín dụng để tạo ra một món nợ lớn cho khách hàng hoặc lấy trộm thông tin tài khoản đăng nhập Internet Banking và sử dụng tiền trong tài khoản của khách hàng để giao dịch.

1.3. Phần mềm độc hại (Virus & Worms, Trojans, Phishing, Pharming, Rootkit, Hacking, trình theo dõi bàn phím Keylogger,…): các loại phần mềm này được thiết kế để gây hại máy tính hoặc thiết bị di động. Phần mềm độc hại có thể lấy cắp thông tin nhạy cảm từ các thiết bị, làm chậm hoạt động của thiết bị hay thậm chí gửi email giả mạo từ tài khoản email của khách hàng mà khách hàng không biết.

2. Nhận diện nhóm lừa đảo trên không gian mạng

2.1. Giả mạo thương hiệu

- Giả mạo thương hiệu của các tổ chức (Ngân hàng, cơ quan Nhà nước, công ty tài chính, chứng khoán…) để gọi điện hoặc gửi tin nhắn lừa đảo cho nạn nhân.
- Giả mạo các website/ trang nhật ký cá nhân (blog) chính thống (giao diện, địa chỉ tên miền/ đường dẫn,…) tạo uy tín lừa nạn nhân, thu thập thông tin cá nhân của người dân.

2.2. Chiếm đoạt tài khoản

- Chiếm quyền sử dụng các tài khoản mạng xã hội (Zalo, Facebook, Tiktok…) để tiến hành gửi tin nhắn lừa đảo cho bạn bè người thân nhằm chiếm quyền tài khoản, lấy cắp thông tin, chiếm đoạt tài sản, bôi nhọ danh dự, tống tiền…
- Các ứng dụng, quảng cáo tín dụng đen xuất hiện trên các website, gửi tràn lan qua các kênh thư điện tử rác, tin nhắn SMS, mạng xã hội Facebook, Telegram, Zalo,... Nạn nhân sẽ biến thành những con nợ trong khi chính nạn nhân cũng không biết.

2.3. Các hình thức kết hợp

- Sử dụng số điện thoại (trong nước, nước ngoài, đầu số lạ…) **giả danh cơ quan chức năng, Công an, nhà mạng viễn thông**… để tiến hành gọi điện thoại cho nạn nhân

thông báo vi phạm pháp luật và yêu cầu chuyển khoản.

- **Sử dụng số điện thoại đầu số lạ** gọi điện cho nạn nhân, khi bắt máy nạn nhân sẽ bị trừ tiền trong tài khoản mà không hề hay biết.
- **Giả mạo trang thương mại điện tử** lớn tại Việt Nam, nước ngoài để lừa nạn nhân làm cộng tác viên. Để dẫn dụ nạn nhân, đối tượng xấu thực hiện chạy quảng cáo lừa đảo trên các trang mạng xã hội hay gửi tin nhắn quảng cáo rác (spam) qua SMS.
- **Lan truyền tin giả** đánh vào tâm lý hiếu kỳ, sự thương người và lòng tin. Để thu hút lượt người xem, lượt thích các nội dung được đưa lên mạng xã hội và sau đó là lừa gạt chiếm đoạt tài sản qua hình thức từ thiện, kêu gọi đóng góp lừa đảo,…
- **Lừa đảo chiếm đoạt tài sản** qua quảng bá bán hàng trực tuyến trên các trang mạng xã hội (bán hàng giả, chất lượng kém, vé máy bay giả, khuyến mãi giả, hàng ảo hoặc rao bán giả mạo không tồn tại sản phẩm).
- **Giả mạo trang cá nhân, tài khoản** người dùng trên trang mạng xã hội Facebook, Telegram, Zalo,... để tạo uy tín và lừa nạn nhân sử dụng dịch vụ hoặc đầu tư. Chẳng hạn như lừa chiếm đoạt tài sản bằng cách chờ trực trên các trang người hâm mộ (Fanpage) có tích xanh, Fanpage của người nổi tiếng trên mạng xã hội để nhắn riêng với nạn nhân đóng giả là nhân viên, trợ lý.
- **Bẫy tình, lợi dụng tình cảm** lòng tin và sự thương hại để lừa đảo qua các trang mạng xã hội Facebook, Zalo, Tinder, Telegram,...
- **Lừa đảo cài cắm mã độc** thông qua đường dẫn độc hại, phần mềm độc hại (tiện ích mở rộng cho trình duyệt, phần mềm bẻ khóa - crack). Đối tượng tạo những công cụ, đường dẫn, phần mềm độc hại để chiếm đoạt tài sản, thông tin tài khoản mạng xã hội, tài khoản ngân hàng thông qua tiếp cận nạn nhân từ chạy quảng cáo có gắn đường dẫn truy cập độc hại, phát tán mã độc, phần mềm độc hại qua trang mạng xã hội, các công cụ tìm kiếm trên mạng Internet (Google Search), các cửa hàng ứng dụng CH Play, App Store và email.
- **Thông báo trúng thưởng, quà tặng, khuyến mại** để lừa nạn nhân nhằm đánh cắp thông tin tài khoản và tài sản thông qua các website giả mạo.
- **Thủ đoạn nâng cấp** lên sim 4G hay 5G để lừa lấy số điện thoại của nạn nhân nhằm chiếm đoạt thông tin tài khoản và tài sản.
- **Giả mạo email của ngân hàng, ví điện tử, tổ chức** uy tín để uy hiếp, đe doạ lừa tiền nạn nhân.
- **Lập sàn đầu tư tiền ảo** (crypto), đầu tư đa cấp, đầu tư nhị phân, đầu tư Forex,…nhằm lừa đảo chiếm đoạt tài sản.

- **Mạo danh cán bộ ngân hàng, Công an, tòa án, thuế và các ngành thiết yếu khác** (cán bộ ngành điện, nước, viễn thông, giáo dục, y tế….) truy cập website giả mạo, cài đặt các ứng dụng giả mạo cơ quan Nhà nước, các tổ chức, trong đó có chứa các mã độc nhằm theo dõi, đánh cắp thông tin giao dịch, trộm tiền trong tài khoản ngân hàng.

3. Một số hành vi lừa đảo

3.1. Lừa khách hàng thực hiện chuyển tiền

- Các đối tượng lừa đảo sẽ mạo danh cơ quan chức năng/ cơ quan Nhà nước liên hệ qua điện thoại hoặc mạng xã hội, dẫn dụ khách hàng thực hiện chuyển tiền đến tài khoản mà các đối tượng này cung cấp bằng cách:
    - Mạo danh cán bộ cơ quan Nhà nước như điều tra viên, cán bộ tòa án, cán bộ thuế,… để thông báo khách hàng đang bị điều tra hoặc có liên quan đến một vụ án hình sự đặc biệt nghiêm trọng do đó cần phải kiểm tra số tiền trong tài khoản của khách hàng.
    - Mạo danh nhân viên của các nhà cung cấp dịch vụ điện, nước, viễn thông, bưu điện… để thông báo khách hàng đang nợ cước số tiền lớn và yêu cầu phải thanh toán ngay hoặc thay đổi, nâng cấp dịch vụ đang sử dụng.
    - Mạo danh người thân hoặc người quen để liên lạc với khách hàng thông qua mạng xã hội hoặc gọi điện thoại để vay mượn hoặc chuyển tiền mua hàng, cấp cứu…
    - Mạo danh cơ quan, nhân viên chuyển phát thông báo khách hàng có bưu kiện đang bị tạm giữ và phải đóng các khoản phí để nhận về.
    - Mạo danh nhân viên của các tổ chức thông báo khách hàng trúng thưởng từ chương trình quay số ngẫu nhiên… và yêu cầu khách hàng chuyển tiền để làm lệ phí nhận thưởng.
- Điểm chung của hình thức này là các đối tượng sẽ nhấn mạnh khách hàng không có nhiều thời gian, từ đó gây tâm lý phải thực hiện ngay mà khách hàng không kịp kiểm tra lại. Các tài khoản được chỉ định chuyển khoản vào cũng là tài khoản cá nhân hoặc số điện thoại không thuộc bất kỳ tổ chức, doanh nghiệp nào.

3.2. Lừa khách hàng cung cấp thông tin đăng nhập, mã xác thực OTP qua hình thức cho vay online

- Các đối tượng lừa đảo sẽ tiếp cận với khách hàng thông qua những phương thức như:
    - Gửi tin nhắn rác chứa nội dung quảng cáo cho vay tiền đến số điện thoại của khách hàng.

- Lừa đảo bằng những lời mời cho vay qua mạng xã hội.
- Lừa đảo thông qua những website/ ứng dụng được quảng cáo cho vay tiền.

- Đánh vào tâm lý vay tiền online nhanh chóng mà không cần giấy tờ cá nhân, không cần gặp mặt trực tiếp, các đối tượng lừa đảo sẽ hướng dẫn khách hàng truy cập website hoặc tải ứng dụng để thực hiện khai báo và sao kê tài khoản ngân hàng trước khi được duyệt vay.

3.3. Lừa qua hình thức tin nhắn thương hiệu (SMS Brandname)

- Các đối tượng lừa đảo dùng thủ thuật để mạo danh tin nhắn thương hiệu DongA Bank, gửi các thông điệp sau:
  - Yêu cầu xác minh tài khoản, nhận tiền trúng thưởng…
  - Thông báo tài khoản bị khóa do nghi ngờ thực hiện giao dịch từ nước ngoài, đăng nhập trên thiết bị lạ hoặc các giao dịch vi phạm pháp luật như lừa đảo, đánh bạc…
  - Lời mời chào vay tiền từ ngân hàng…
  - Thông báo mật mã hết hạn, thông tin cá nhân bị thay đổi hoặc đăng ký dịch vụ bất kỳ nhưng khách hàng không phải là người thực hiện.
- Điểm chung của các tin nhắn này đều đính kèm đường dẫn truy cập gần giống hoặc không trùng khớp với địa chỉ của DongA Bank (địa chỉ chính xác của DongA Bank: www.dongabank.com.vn hoặc https://ebanking.dongabank.com.vn).

3.4. Lừa qua hình thức email giả mạo

Tương tự như thủ thuật giả mạo SMS Brandname, các đối tượng lừa đảo sẽ giả mạo các email được gửi từ DongA Bank cùng các nội dung như:

- Cảnh báo khách hàng rằng tài khoản của họ cần được cập nhật hoặc có hoạt động bất thường và yêu cầu cung cấp thông tin cá nhân như một cách để xác nhận danh tính và khôi phục tài khoản.
- Chứa những nội dung như quảng cáo liên quan đến tài chính ngân hàng hoặc nội dung cảnh báo gây hoang mang cho người đọc.
- Điểm chung của các email này đều chứa nội dung yêu cầu truy cập đường dẫn, tải tệp đính kèm hoặc điều hướng đến một website khác có giao diện tương tự với DongA Bank để khách hàng cung cấp các thông tin cá nhân, số tài khoản thẻ ngân hàng, mã xác thực OTP… nhằm thực hiện các hành vi theo mục đích tấn công.

3.5. Lừa qua hình thức nhận tiền từ quốc tế

- Các hành vi mà đối tượng lừa đảo thường áp dụng là:

- Giả mạo người thân, bạn bè ở nước ngoài muốn gửi tiền về Việt Nam thông qua tài khoản của khách hàng.
- Giả vờ mua hàng hóa tại các nơi bán hàng trực tuyến (shop online) giao ở Việt Nam và thanh toán trước bằng hình thức chuyển khoản.

- Điểm chung là sau khi trao đổi với đối tượng lừa đảo, khách hàng sẽ nhận được tin nhắn qua mạng xã hội hoặc tin nhắn SMS (tương tự như yêu cầu xác minh tài lừa đảo qua hình thức tin nhắn thương hiệu SMS Brandname) rằng có một khoản tiền đang chờ báo có và yêu cầu khách hàng xác thực tài khoản theo đường dẫn website có giao diện giả mạo các website dịch vụ chuyển tiền quốc tế như Western Union, Money Gram…

3.6. Cài đặt ứng dụng có chứa mã độc trên thiết bị di động

- Hiện nay xuất hiện rất nhiều ứng dụng chứa mã độc hoặc các ứng dụng giả mạo dùng để theo dõi điện thoại khách hàng nhằm đánh cắp thông tin cá nhân, thông tin tài khoản ngân hàng, thông tin đăng nhập Internet Banking của họ.
- Khách hàng cần tỉnh táo kiểm tra trước khi cài đặt và cấp quyền truy cập cho bất kỳ một ứng dụng nào trên các cửa hàng. Ví dụ: việc ứng dụng chỉnh ảnh yêu cầu cấp quyền truy cập danh bạ hoặc tin nhắn là không cần thiết, rất có khả năng cao ứng dụng này sẽ đánh cắp thông tin của khách hàng.
- Đối tượng lừa đảo sử dụng cách thức mạo danh nhân viên cơ quan, tổ chức có uy tín để thực hiện mục tiêu lừa nạn nhân cài đặt ứng dụng có chứa mã độc trên thiết bị di động; mạo danh cán bộ, công viên chức Nhà nước yêu cầu người dân cài đặt các ứng dụng giả mạo dịch vụ công như chính phủ, VNeID, bảo hiểm, thuế; đối tượng lừa đảo tiếp cận nạn nhân qua các phương tiện điện tử (gọi điện thoại, liên hệ qua tài khoản mạng xã hội, gửi email) để để trục lợi cá nhân, lừa đảo người nộp thuế:
    - Chúng sử dụng công nghệ cao, ẩn danh dưới số điện thoại giống hệt số điện thoại công khai của cơ quan Công an, Viện Kiểm sát để gọi điện thoại, nhắn tin, kết bạn Zalo, cung cấp đường dẫn trên mạng Internet và hướng dẫn người nộp thuế quyết toán thuế, hướng dẫn cài đặt các phần mềm giả mạo ứng dụng của cơ quan thuế, bảo hiểm xã hội,…
    - Giả mạo cơ quan chức năng để gọi điện hăm dọa, sử dụng chiêu trò lừa đảo nhằm chiếm đoạt tài sản của người nộp thuế.
    - Giả mạo website có giao diện gần giống website của cơ quan, doanh nghiệp từ hình ảnh đến nội dung để người dùng nhầm tưởng là website của đơn vị cung cấp, từ đó nhập các thông tin cần bảo mật như thông tin cá nhân, tài khoản ngân hàng,…

- Giả mạo cơ quan chức năng hỗ trợ dịch vụ công và yêu cầu cung cấp thông tin, gửi hình ảnh căn cước công dân, sau đó đối tượng gửi các đường dẫn truy cập website/ ứng dụng giả mạo và hướng dẫn giả mạo để chiếm quyền điều khiển điện thoại và thực hiện hành vi lấy hết tiền trong tài khoản ngân hàng.

- Đặc điểm chung là các đối tượng lừa đảo lợi dụng người dân chưa nắm bắt đầy đủ các thông tin liên quan đến việc cài đặt các ứng dụng dịch vụ công như thuế, bảo hiểm xã hội, VNeID, quy trình kích hoạt tài khoản định danh điện tử của một bộ phận người dân; tâm lý muốn nhanh chóng thực hiện, không muốn đến các trụ sở công quyền phiền phức nên đã làm theo chỉ dẫn của các đối tượng lừa đảo giả danh cán bộ.

3.7. Mạo danh nhân viên ngân hàng

- Các đối tượng lừa đảo liên hệ khách hàng qua điện thoại tự xưng là nhân viên ngân hàng hoặc tổ chức tín dụng để:
    - Thông báo tài khoản ngân hàng/ thông tin đăng nhập dịch vụ Ngân hàng trên Internet bị lộ thông tin hoặc cần xác nhận thông tin tài khoản ngân hàng, thông báo trúng thưởng,...
    - Thông báo hỗ trợ khách hàng vay vốn hoặc chuyển đổi hạn mức thẻ tín dụng sang tiền mặt với phí rẻ hoặc miễn phí….
- Điểm chung của hình thức này là yêu cầu khách hàng cung cấp thông tin đăng nhập, mật mã ngân hàng điện tử và cả mã xác thực OTP (nếu có), hoặc đối với người dùng thẻ tín dụng, đối tượng sẽ yêu cầu cung cấp toàn bộ thông tin có trên thẻ (gồm số thẻ, họ tên, ngày hết hạn và mã số xác thực ở mặt sau thẻ (CVV)).