

PHÒNG TRÁNH LỪA ĐẢO TÀI CHÍNH

1. Đặc điểm của lừa đảo qua điện thoại (Voice Phising)

1) Mạo danh cơ quan

Tội phạm lừa đảo sẽ giả danh kiểm sát, cảnh sát, viện giám sát tài chính, công ty tài chính.

2) Áp lực về mặt tâm lý

gây áp lực về mặt tâm lý của người bị hại như thông báo bị lộ thông tin cá nhân, liên quan đến vụ án lừa đảo, con cái bị bắt cóc, v.v...

3) Làm giả số điện thoại gọi đến

làm giả để số điện thoại gọi đến là số điện thoại của cơ quan hành chính và công ty tín dụng.

4) Nói tiếng Hàn một cách thành thạo

Giống thời kỳ đầu gây ra lừa đảo bằng giọng nói, tội phạm lừa đảo gần như không sử dụng tiếng Hàn một cách lắp bắp mà sử dụng tiếng Hàn thông thạo để tấn công nạn nhân

5) Trực tiếp rút tiền chuyển khoản

tìm được thông tin giao dịch tài chính của người bị hại (số tài khoản, số thẻ tín dụng, thông tin internet banking, thông tin telebanking, v.v.v...) để trực tiếp rút tiền.

6) Sở tài khoản chuyên dụng để lừa đảo

sử dụng sổ gửi tiền khi vay tiền hoặc tìm việc, làm mỗi như trước đó hoặc sổ tài khoản đứng tên người nước ngoài để dùng trong hành vi lừa đảo

2. Cách phòng ngừa lừa đảo Voice phishing

1) Đừng trả lời bất cứ yêu cầu nào về thông tin giao dịch tài chính

Tuyệt đối không được trả lời trong các trường hợp hỏi thông tin qua điện thoại với các lý do như bị lộ thông tin cá nhân, liên quan đến vụ án tội phạm, v.v.v... hoặc yêu cầu nhập các thông tin cá nhân vào trang web internet.

2) Nếu bị dụ dỗ đến máy ATM (máy gửi và rút tiền mặt tự động) thì 100% đó là lừa đảo Voice phishing

Trong trường hợp tội phạm lừa đảo bảo sẽ sử dụng máy ATM để hoàn trả lại thuế, phí bảo hiểm, v.v... hoặc nói sẽ xử lý an toàn cho tài khoản để dẫn dụ bạn đến máy ATM thì tuyệt đối không làm theo những gì chúng yêu cầu.

3) Trường hợp có người biết trước thông tin cá nhân, thông tin giao dịch tài chính và tiếp cận bạn thì cần xác nhận sự thật của nội dung đó có đúng hay không

Gần đây việc biết trước các thông tin cá nhân, giao dịch tài chính để tiếp cận xảy ra rất nhiều do đó trong trường hợp này, cần phải trực tiếp liên hệ đến cơ quan hay liên hệ đến số điện thoại đại diện của công ty tài chính đó để kiểm tra xem nội dung của điện thoại, tin nhắn điện thoại, tin nhắn internet có đúng hay không

4) Nếu đã bị thiệt hại thì phải yêu cầu đình chỉ thanh toán ngay lập tức

Nếu đã bị thiệt hại thì phải yêu cầu đình chỉ thanh toán đối với tài khoản lừa đảo một cách nhanh chóng thông qua tổng đài sở cảnh sát (☎112) hay tổng đài công ty tài chính.

5) Số điện thoại gọi đến(điện thoại) có khả năng là giả nên cần lưu ý

Dù đã gia nhập vào hệ thống chỉ định trước số điện thoại telebanking (là hệ thống chỉ có số điện thoại được chỉ định đã đăng

ký trước mới có thể sử dụng dịch vụ telebanking) thì thông qua sự chuyển đổi internet cũng có khả năng làm giả số gọi đến, vì thế những người bị hại không được bị mê hoặc với các lời nói của bọn lừa đảo như “không có ai có thể sử dụng tele banking ngoài bản thân người đăng ký gia nhập tại hệ thống chỉ định số điện thoại trước nên khách hàng có thể yên tâm”

3. Lưu ý đặc biệt về thông tin cá nhân

- 1) Đừng cho người khác biết thông tin cá nhân(Số tài khoản, số điện thoại, họ tên, số hộ chiếu, số người nước ngoài)
- 2) Đừng cho người khác biết thông tin cá nhân của bạn nếu không có đồng ý của người đó
- 3) Khi cung cấp thông tin cá nhân thì hãy suy nghĩ kỹ. Đặc biệt là Hàn Quốc không có chỗ đổi tiền chính thức nên bắt buộc phải đổi tiền tại ngân hàng.