VPBank
Ngân Hàng Việt Nam Thịnh Vượng

CÁC HÌNH THỨC LỪA ĐẢO ONLINE VÀ CÁCH THỨC PHÒNG TRÁNH

CẢNH BÁO NGUY CƠ BỊ LỪA ĐẢO ONLINE

CỔNG THÔNG TIN ĐIỆN TỬ

BỘ CÔNG AN

GIỚI THIỆU | TIN TỨC SỰ KIỆN | VĂN BẢN | DỊCH VỤ CÔNG | BỘ

Cảnh báo về chiến dịch tấn công mạng lợi dụng dịch bệnh COVID-19

Thời gian gần đây, tình hình dịch bệnh COVID-19 đang có diễn biến phức tạp tại nhiều quốc gia, một số nhóm tin tặc đã lợi dụng tình hình này để phát động, tiến hành chiến dịch tấn công mạng có chủ đích vào các cơ

Cảnh báo về chiến dịch tấn công mạng lợi dụng dịch bệnh COVID-19

Công an Cửa khẩu Cảng hàng không quốc tế Nội Bài: Chủ động các phương án phòng, chống dịch COVID-19 trong ngày đầu dừng cấp thị thực cho du khách từ vùng dịch

Tuổi trẻ Văn phòng Bộ Công an đồng hành cùng cán bộ, chiến sỹ Công an nơi tuyến đầu phòng, chống dịch COVID-19

Những chiến sỹ chống

Nhấp chuột, mất tiền

Chị Y (ngụ TP. Hồ Chí Minh, kinh doanh online) cho biết, vừa bị đối tượng lừa lấy tài khoản internet banking. Đối tượng này cho biết đang ở nước ngoài, qua fanpage của chị Y, người này đặt mua nhiều loại bánh mứt, đặc sản ngoại để gửi cho gia đình ở Đồng Nai. Tổng đơn hàng hơn 4,2 triệu đồng. "Tôi rất cẩn thận nên đã vào facebook của người mua, xem nhiều comment (bình luận) đúng là người này ở nước ngoài thật nên khá tin tưởng" - chị Y nói.

Khi chị Y yêu cầu chuyển tiền trước, người mua gửi một đường link giả Western Union và một mã giao dịch, đề nghị chị Y nhấp chuột để nhận tiền. Theo chị Y, website này có giao diện, hotline khá giống với một ngân hàng tại Việt Nam. Đối tượng còn gọi điện thoại từ 1 số máy nước ngoài, hối thúc chị nhanh chóng đăng nhập vì người này đang ở NH, sắp đến giờ làm nên không chờ được lâu.

"Sợ mất khách hàng "ngon", tôi không có thời gian suy nghĩ nên nhấp vào link, khai báo tên đăng nhập, mật khẩu, nhập cả mã OTP. Ngay lập tức, tôi nhận được thông báo hủy mã OTP đang sử dụng, đồng thời mã OTP của tôi đã được kích hoạt trên một điện thoại khác. Sau đó 34 triệu đồng trong tài khoản cũng biến mất" - chị Y nói.

Mai Thế Dũng giả bị can để lừa đảo

Còn trường hợp ông T.V.D (ngụ P.Yên Thế, TP.Pleiku, Gia Lai) bị chiếm đoạt quyền sử dụng Gmail rồi còn bị gọi điện thoại "hù dọa", cuối cùng mất gần 3 tỷ đồng cho chúng.

Các đối tượng chiếm đoạt quyền sử dụng Gmail của ông D., nhưng vẫn để chủ tài khoản truy cập bình thường. Ông D. vẫn dùng Gmail để làm việc mà không biết có người đang theo dõi từng thư đến, thư đi. Qua theo dõi Gmail của ông D, các đối tượng biết ông D. có một khoản tiền lớn trong tài khoản ngân hàng.

CÁC HÌNH THỨC LỪA ĐẢO

Mục tiêu

Lừa đảo qua điện thoại

Kẻ lừa đảo giả mạo cơ quan chức năng, tổ chức tài chính để lừa người dùng nộp tiền hoặc cung cấp thông tin tài khoản ngân hàng.

Lừa đảo trên mạng xã hội Zalo/Facebook

Kẻ lừa đảo gửi tin nhắn trúng thưởng hoặc hỏi mua hàng, sau đó yêu cầu cung cấp thông tin tài khoản hoặc chuyển phí để nhận quà.

Lừa đảo qua các trang web hoặc email

Kẻ lừa đảo gửi đường link của trang web giả mạo ngân hàng hoặc dịch vụ chuyển tiền quốc tế đến người bị hại. Khi nạn nhân nhập thông tin như số tài khoản, mật khẩu, OTP, toàn bộ số tiền trong tài khoản của họ sẽ bị chuyển đi

CÁC TÌNH HUỐNG THỰC TẾ

Lừa đảo qua điện thoại

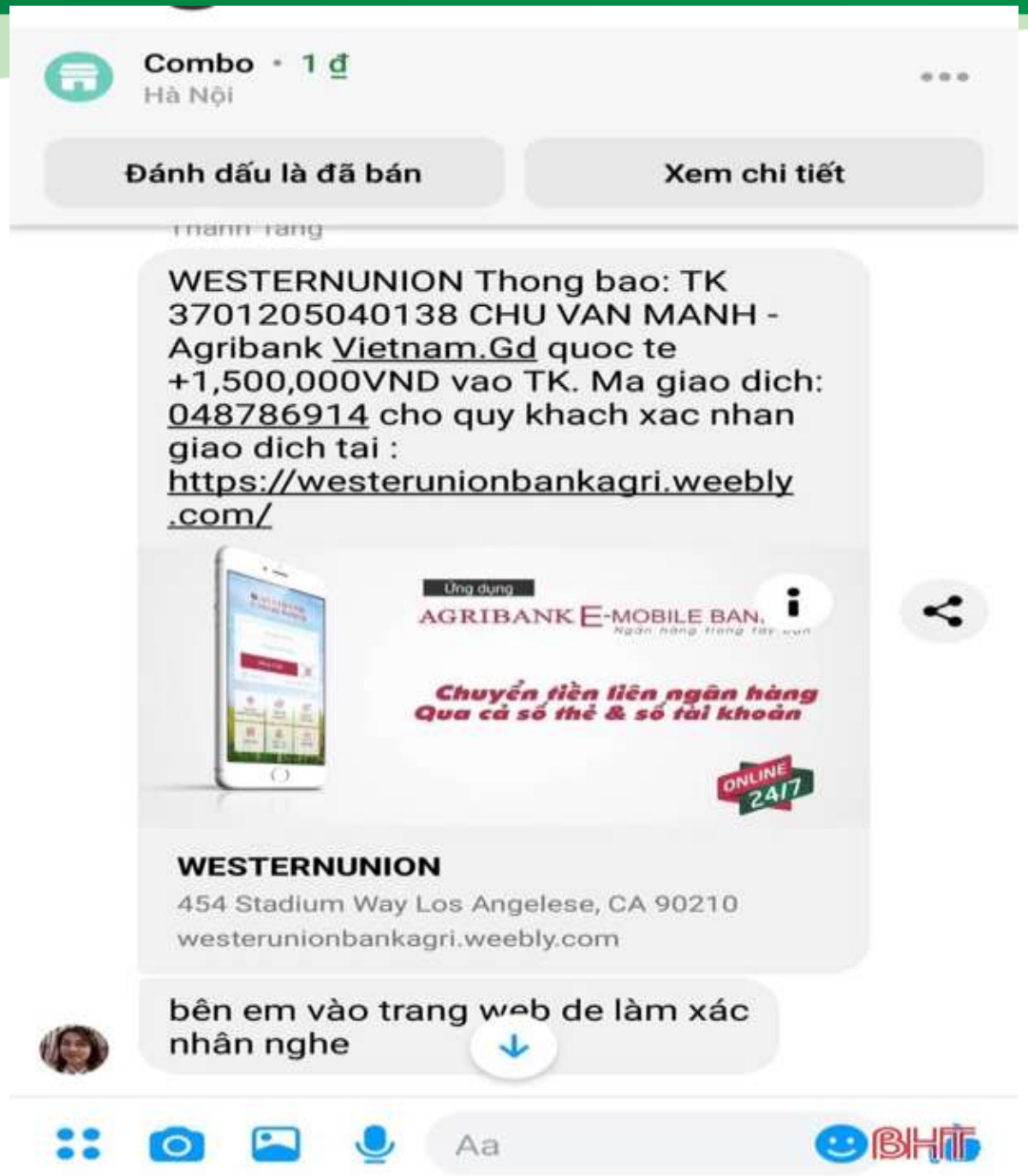
Bước 1: Kẻ lừa đảo gọi điện mạo danh cán bộ trong các cơ quan tư pháp như: Công an, Viện kiểm sát, Tòa án gọi điện cho nạn nhân nói rằng họ bị kiện vì nợ tiền hoặc có liên quan đến vụ án đang giải quyết Hoặc có thể giả mạo nhân viên nhà mạng, công ty điện lực thông báo SĐT đang nợ tiền cước, tiền điện.

Bước 2: Yêu cầu người dân chuyển một số tiền vào một tài khoản do các đối tượng này cung cấp để điều tra hoặc nộp tiền dịch vụ chưa thanh toán vào số tài khoản.

Khuyến nghị từ VPBank

- **Cảnh giác** với các cuộc gọi tự xưng từ các cơ quan công an, viện kiểm sát, ngân hàng.
- Gọi lên tổng đài của nhà mạng, công ty điện lực để **xác minh thông tin** và số tài khoản của Nhà cung cấp dịch vụ.

CÁC TÌNH HUỐNG THỰC TẾ



Tình huống 1:

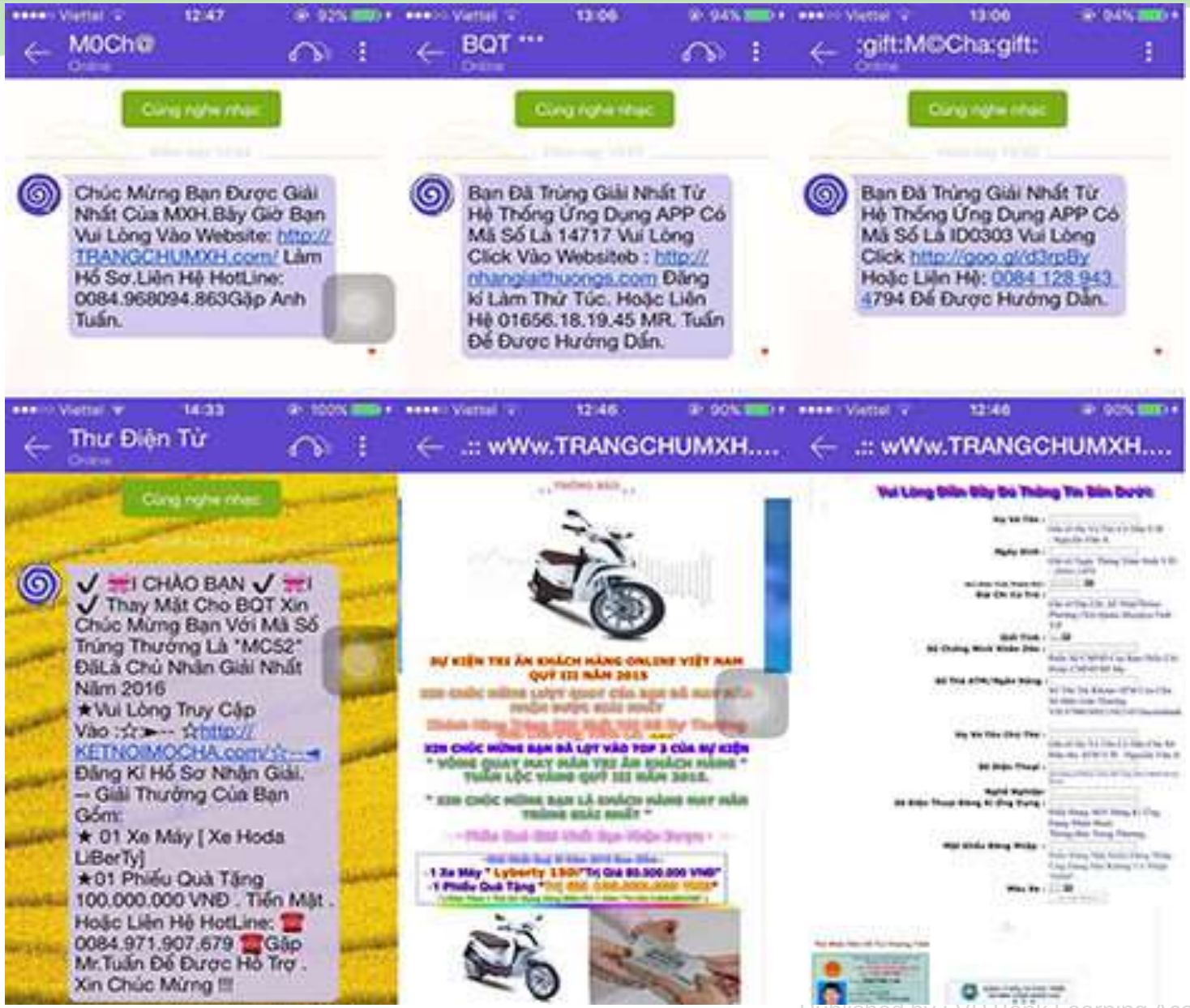
Một khách quen thường đặt mua hoa tại cửa hàng hoa của bà H. Họ mua đơn hàng hoa với giá 3.2tr. Ở bước chuyển tiền, người này nói đang ở Mỹ và chuyển khoảng qua. Sau bước đăng nhập, một mã OTP được gửi về đt bà H. Sau khi nhập, tk bị trừ 50tr ngay lập tức. Quá hoảng loạn, bà H hỏi lại người này thì họ bảo bà chụp màn hình tin nhắn trừ tiền của ngân hàng để xem lý do. Ngay lúc chụp ảnh màn hình, một mã OTP khác được gửi về đt của bà H và 50tr đồng tiếp theo lại được chuyển về tài khoản của kẻ lừa đảo. Người này tiếp tục bảo bà nhập OTP vào trang web nếu không tài khoản sẽ bị đóng băng. Cuối cùng tổng cộng bà bị lừa mất 150tr. Bà cho biết đây là khách quen nên hoàn toàn tin tưởng. Tuy nhiên sau này bà mới biết Facebook của người này đã bị hacker tấn công

CÁC TÌNH HUỐNG THỰC TẾ

Tình huống 2:

Tặng quà từ nước ngoài: Giả mạo người nước ngoài sau khi nói chuyện một thời gian sẽ đề nghị tặng nạn nhân một món quà nhưng để nhận món quà đó thì nạn nhân phải chi một khoản tiền để thanh toán phí hải quan và phí vận chuyển. Món quà thường được nói là có giá trị lớn để mức phí hải quan cao khiến nạn nhân không nghi ngờ mà chuyển một số tiền lớn cho đối tượng lừa đảo. Sau khi chuyển tiền thì đối tượng sẽ chặn tài khoản nạn nhân và tiếp tục lừa đảo đối tượng khác.

CÁC TÌNH HUỐNG THỰC TẾ

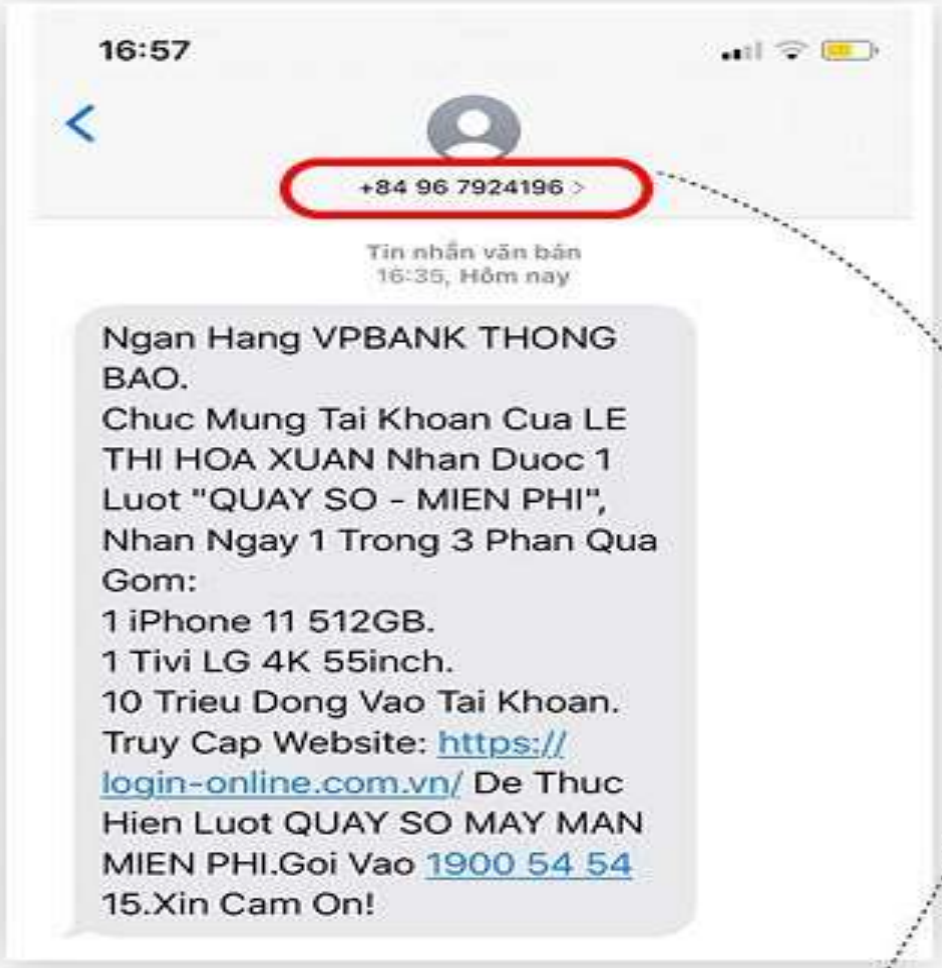


Tình huống 3:

Bạn dùng tài khoản MXH để comment một nội dung bài viết trên mạng liên quan đến minigame. Kẻ gian tạo nick giả mạo admin của group, sử dụng tên và avatar của Group để add nick zalo, Facebook của các thành viên trong group. Sau đó lừa các thành viên là đã thắng minigame, phần thưởng là tài khoản quảng cáo trên MXH hay hiện vật, tiền mặt, … Yêu cầu thành viên đó cung cấp thẻ tín dụng và mã OTP để liên kết tạo tài khoản quảng cáo trên MXH hoặc để nhận phần thưởng. Sau đó kẻ gian dùng thông tin thẻ tín dụng lừa được để liên kết thẻ tín dụng và tài khoản của mình để chiếm đoạt tiền của nạn nhân


Viettel
16:02
42%
VPBANK
15:53, Hôm nay
QK dang giao dich tren VPBank Dream.KHONG gui OTP cho bat cu ai, BAO GOM NGAN HANG.Ma OTP 972477 hieu luc trong 3phut.LH 1900545415
Tin nhắn văn bản

TIN NHẮN **GIẢ MẠO**



Gửi từ đầu số máy lạ

TIN NHẮN **NGÂN HÀNG**

Hiển thị đầu số gửi là tên của ngân hàng

CÁC TÌNH HUỐNG THỰC TẾ

Lừa đảo trên mạng xã hội (tin nhắn, zalo, facebook)

Bước 1: Kẻ lừa đảo gửi tin nhắn cho nạn nhân đính kèm trang web giả mạo yêu cầu đăng nhập tài khoản ngân hàng hoặc yêu cầu cung cấp số thẻ tín dụng

Bước 2: Nạn nhân nhập số tài khoản, mật khẩu và mã OTP được gửi về điện thoại

Bước 3: Nạn nhân bị mất tiền trong tài khoản

Khuyến nghị từ VPBank

- Không mở và đăng nhập tài khoản ngân hàng trên các đường link lạ.
- Không cung cấp mật khẩu dùng 1 lần (OTP) cho bất cứ ai kể cả ngân hàng, công an.
- Xác minh lại người nhận trước khi cung cấp thông tin

CÁC TÌNH HUỐNG THỰC TẾ

Lừa đảo qua website

Bước 1: Kẻ tấn công gửi tin nhắn/email có chứa liên kết đến trang web giả mạo có chứa mã độc. Hoặc người dùng vô tình nhấp vào các popup quảng cáo khi truy cập Internet.

Bước 2: Trang web giả mạo hiện lên yêu cầu người dùng đăng nhập tài khoản mạng xã hội Facebook/Zalo/Gmail hay tài khoản ngân hàng.

Bước 3: Toàn bộ thông tin đăng nhập sẽ bị đánh cắp. Kẻ tấn công dùng thông tin này để thực hiện các hành vi lừa đảo khác.

Khuyến nghị

Thiết lập bảo mật 2 lớp cho các tài khoản mạng xã hội

Không click vào các đường link lạ, các quảng cáo và truy cập vào các website độc hại

CÁCH THỨC PHÒNG TRÁNH

HÃY THỰC HIỆN

- **GIỮ BÍ MẬT** các thông tin bảo mật Ngân hàng điện tử bao gồm tên đăng nhập/mật khẩu đăng nhập/mã mở khóa Smart OTP.
- **NÊN THỰC HIỆN** giao dịch điện tử trên các website mua bán hàng hóa chính thức, có độ bảo mật cao.
- **NÊN XÁC THỰC** người đề nghị thực hiện giao dịch khi nhận được yêu cầu chuyển tiền, nạp tiền.

TUYỆT ĐỐI KHÔNG

- **KHÔNG** cung cấp thông tin bảo mật như tên đăng nhập/mật khẩu đăng nhập/mã mở khóa Smart OTP và nội dung các tin nhắn thông báo từ VPBank cho bất kì ai, kể cả người tự xưng là công an, cơ quan điều tra, nhân viên ngân hàng,...
- **KHÔNG** cung cấp thông tin, đưa thông tin giao dịch lên mạng, đặc biệt là những giao dịch bán hàng online, vì sẽ tạo điều kiện cho kẻ lừa đảo.
- **KHÔNG** cài đặt các phầm mềm crack, can thiệp vào thiết bị, hệ điều hành.
- **KHÔNG** nhập mật khẩu đăng nhập/mã OTP trên các trang mạng không rõ nguồn gốc, hoặc đường link lạ.
- **KHÔNG** thực hiện giao dịch trên các thiết bị công cộng, tiềm ẩn rủi ro cao, hay lưu thông tin tự động đăng nhập ngân hàng điện tử tại bất kì đâu.