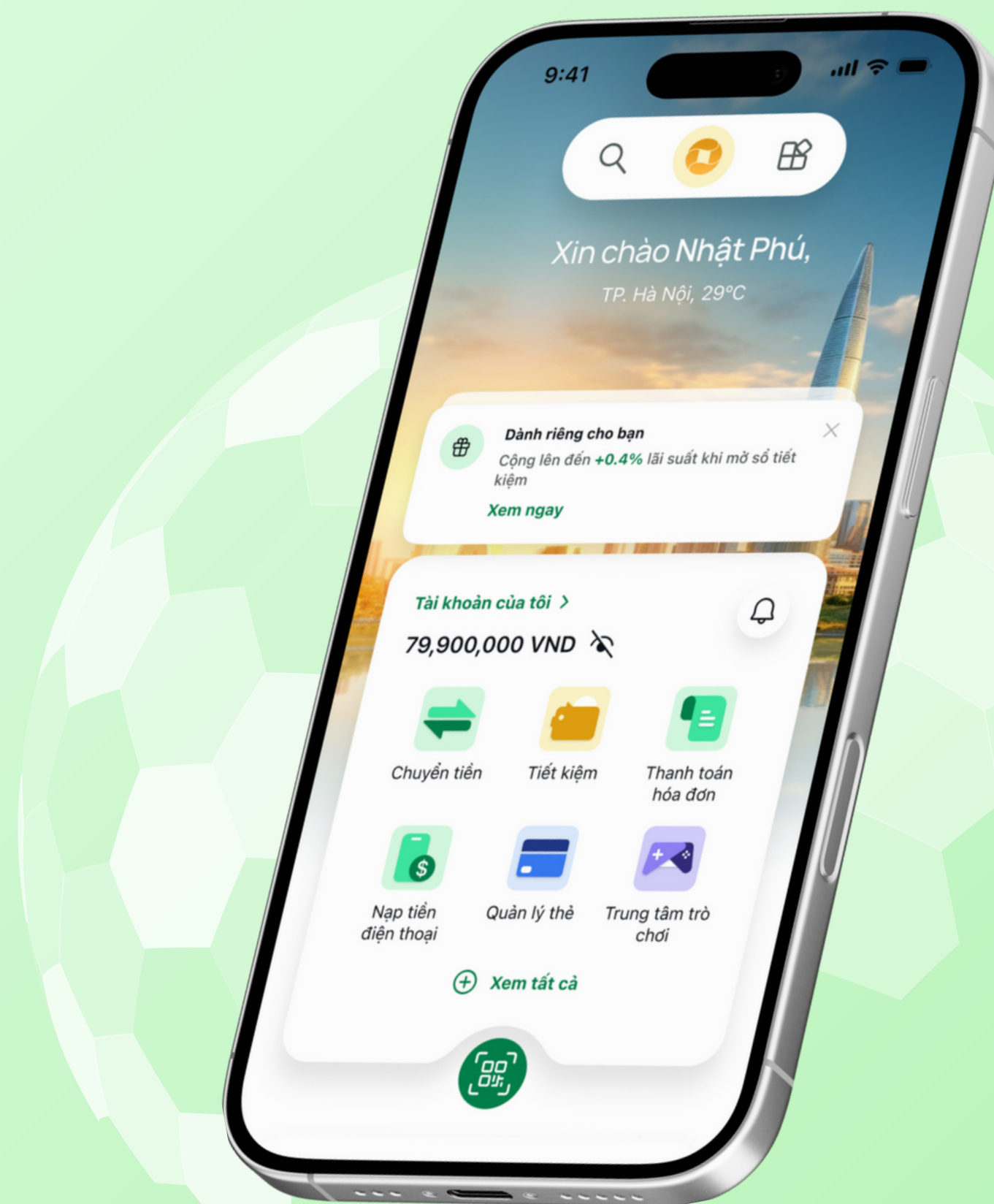


Hướng dẫn Giao dịch an toàn trên **OCB OMNI**



Để nâng cao an toàn khi sử dụng dịch vụ trên ứng dụng OCB OMNI, Quý khách vui lòng lưu ý và thực hiện nội dung sau đây:

I. CÁC NGUYÊN TẮC BẢO MẬT



Thiết lập mã PIN, Smart OTP, mật khẩu có độ khó cao, tránh sử dụng thông tin cá nhân dễ đoán như ngày sinh, số điện thoại, tên riêng và không chia sẻ cho bất kỳ ai (kể cả nhân viên ngân hàng), nên thay đổi định kỳ để bảo vệ tài khoản



Không sử dụng máy tính dùng chung hoặc kết nối mạng WiFi công cộng không bảo mật, ưu tiên sử dụng mạng di động 4G/5G hoặc WiFi gia đình



Không lưu tên đăng nhập, mật khẩu, mã PIN trên trình duyệt web hay các thiết bị dùng chung.



Đăng xuất và đóng ứng dụng OCB OMNI sau khi hoàn thành giao dịch



Không sử dụng điện thoại đã bị phá khóa để cài ứng dụng OCB OMNI và chỉ cài đặt ứng dụng từ nguồn chính thống như App Store hoặc Google Play, tránh phần mềm lạ hoặc không có bản quyền



Thông báo ngay khi phát hiện giao dịch bất thường, mất thiết bị có lưu thông tin đăng nhập hoặc nghi ngờ bị lừa đảo, tấn công mạng, hoặc vô tình nhấp vào link lạ



Sử dụng các phương thức xác thực có độ bảo mật cao như Smart OTP hoặc sinh trắc học, phù hợp với nhu cầu và hạn mức giao dịch



Thường xuyên cập nhật hệ điều hành và ứng dụng, cài đặt bản vá bảo mật, sử dụng phần mềm chống mã độc và dữ liệu nhận diện virus mới nhất

II. NHẬN BIẾT VÀ PHÒNG TRÁNH RỦI RO LỪA ĐẢO TRỰC TUYẾN

Các hình thức lừa đảo trực tuyến ngày càng tinh vi, một số thủ đoạn thường gặp:

Giả mạo cơ quan nhà nước



Đối tượng gửi đường link hoặc website giả mạo yêu cầu cài ứng dụng của cơ quan nhà nước như VNeID, ứng dụng ngành thuế... để đánh cắp thông tin, kiểm soát thiết bị từ xa và chuyển tiền trong tài khoản

Đe dọa liên quan pháp luật



Đối tượng dựng lên các kịch bản giả về tai nạn giao thông, rửa tiền, buôn lậu...yêu cầu cung cấp thông tin, cài ứng dụng hoặc chuyển tiền theo chỉ dẫn

Giả mạo ngân hàng



Đối tượng giả mạo website, ứng dụng, fanpage hoặc SMS giống ngân hàng, gửi link giả, hoặc mạo danh nhân viên ngân hàng để lấy thông tin bảo mật (thông tin đăng nhập, mã OTP...) và chuyển tiền trong tài khoản

Giả mạo doanh nghiệp, tổ chức khuyến mại



Đối tượng thông báo trúng thưởng, nhận quà, mã ưu đãi... và yêu cầu cung cấp thông tin ngân hàng hoặc chuyển khoản để hoàn tất thủ tục

Chiếm quyền tài khoản mạng xã hội



Đối tượng chiếm đoạt tài khoản mạng xã hội của bạn bè, người thân (Facebook, Zalo...) rồi nhắn tin vay tiền, nhờ chuyển khoản gấp

III. XỬ LÝ SỰ CỐ



Khi nghi ngờ lừa đảo hoặc phát hiện có dấu hiệu bị lộ thông tin bảo mật tài khoản ngân hàng, Quý khách vui lòng thông báo ngay cho OCB qua hotline **19001846** hoặc chi nhánh/PGD gần nhất

Cập nhật phiên bản mới để trải nghiệm OCB OMNI ngay!



Tải về trên
App Store



TẢI TRÊN
Google Play

