HƯỚNG DẪN GIAO DỊCH AN TOÀN
trên ngân hàng số VCB Digibank và VCB DigiBiz

07 NGUYÊN TẮC ĐẢM BẢO AN TOÀN

Để đảm bảo an toàn khi giao dịch online trên ngân hàng số, Quý khách vui lòng thực hiện theo các nguyên tắc sau đây:

01 **Tuyệt đối không tiết lộ thông tin định danh cá nhân** (Tên đăng nhập; Mật khẩu và Mã khóa bí mật dùng một lần – OTP) cho bất cứ ai khác. Không nên viết mật khẩu ra giấy hoặc ghi chép/lưu dưới bất kỳ hình thức nào.

02 **Tuyệt đối không tải và sử dụng ứng dụng không rõ nguồn gốc** (chỉ sử dụng ứng dụng đã được kiểm định rõ ràng trên chợ ứng dụng App Store và Google Play Store).

03 Nếu sử dụng dịch vụ trên website, **Quý khách chỉ truy cập vào dịch vụ thông qua website chính thức của Vietcombank** (tuyệt đối không thực hiện đăng nhập dịch vụ thông qua các đường link được gắn trong tin nhắn SMS, email, Zalo, Viber ...).

04 **Chỉ đăng nhập qua các thiết bị đáng tin cậy.** Không sử dụng các thiết bị đi động đã bị phá khóa hoặc can thiệp hệ điều hành (root, jailbreak ...) để sử dụng dịch vụ.

05 **Không nên sử dụng các thông tin cá nhân cơ bản** (ngày tháng năm sinh, số điện thoại, tên...) **để đặt mật khẩu**. Nên đổi mật khẩu theo định kỳ tối thiểu ba tháng một lần hoặc khi bị lộ/nghi ngờ bị lộ.

06 Trường hợp không thực hiện giao dịch trên ngân hàng số nhưng vẫn nhận được thông báo từ Ngân hàng về: *Mã OTP, thay đổi số dư bất thường, kích hoạt ứng dụng trên thiết bị khác, liên kết ví điện tử..* **Quý khách tuyệt đối không cung cấp mã OTP** và thông báo ngay cho Ngân hàng.

07 Hãy luôn bình tĩnh, tỉnh táo khi nhận được các yêu cầu cung cấp thông tin/yêu cầu chuyển tiền. **Thực hiện xác minh, kiểm chứng thông tin qua các kênh chính thống** (*ví dụ: Tổng đài chính thức của bên yêu cầu) và kiểm chứng thông tin về website/đường link tại Cổng đánh giá tín nhiệm mạng của Bộ thông tin và Truyền thông (tinnhiemmang.vn*).

CẢNH BÁO CÁC LOẠI HÌNH LỪA ĐẢO TRỰC TUYẾN

Đối tượng lừa đảo sử dụng các thủ đoạn tinh vi để nghị khách hàng thực hiện theo hướng dẫn để đánh cắp thông tin dịch vụ ngân hàng, từ đó truy cập dịch vụ và chiếm đoạt tiền trong tài khoản hoặc yêu cầu khách hàng tự chuyển tiền.

Một số thủ đoạn phổ biến:

- **Giả mạo cơ quan có thẩm quyền** *(công an, tòa án, cơ quan thuế..)* **gửi đường link/website giả mạo dịch vụ công để khách hàng cài đặt các ứng dụng giả mạo** *(ứng dụng VNeID, ứng dụng của Tổng cục thuế..)*, từ đó chiếm quyền điều khiển thiết bị, ngầm đánh cắp thông tin bảo mật dịch vụ ngân hàng và thực hiện hành vi chuyển tiền trong tài khoản của khách hàng.
- **Giả mạo cơ quan có thẩm quyền** *(tòa án, công an..)* **đe dọa khách hàng có liên quan đến các hành vi phạm pháp** *(gây tai nạn giao thông, liên quan đường dây rửa tiền, buôn lậu, nợ cước viễn thông quốc tế..)* và yêu cầu khách hàng thực hiện theo hướng dẫn *(mở tài khoản mới, cung cấp thông tin, cài đặt ứng dụng, chuyển tiền tới tài khoản chỉ định..)*.
- **Giả mạo Website/Fanpage/Tin nhắn SMS của ngân hàng** và gửi đường link giả mạo để khách hàng nhập thông tin.
- **Giả mạo nhân viên ngân hàng liên hệ khách hàng để nghị hỗ trợ** *(hỗ trợ giao dịch chuyển tiền bị lỗi, hỗ trợ xử lý tra soát..)* sau đó yêu cầu khách hàng cung cấp các thông tin bảo mật để thực hiện hành vi chiếm đoạt tài sản.
- **Gửi bưu phẩm có nội dung tạo lòng tin cho khách hàng** *(thông báo trúng thưởng, cung cấp các mã khuyến mãi..)* và kèm theo các yêu cầu, hướng dẫn khách hàng cung cấp thông tin bảo mật của dịch vụ.
- **Đánh cắp thông tin truy cập trên các nền tảng mạng xã hội** (Facebook, Zalo...) của bạn bè, người thân của khách hàng, qua đó liên lạc với khách hàng để đề nghị chuyển tiền hỗ trợ, cho vay.

Quý khách hàng lưu ý

Vietcombank không gửi đường link đăng nhập dịch vụ ngân hàng số cho khách hàng dưới mọi hình thức, **tất cả các đường link đăng nhập gửi đến khách hàng đều là giả mạo.**

Vietcombank không liên hệ yêu cầu khách hàng cung cấp thông tin bảo mật dưới mọi hình thức, **mọi yêu cầu cung cấp thông tin bảo mật dịch vụ đều là giả mạo.**

Quý khách hãy nâng cao cảnh giác đối với các yêu cầu qua kênh trực tuyến và nền tảng mạng xã hội. Đồng thời, báo cho cơ quan Công an/Cơ quan chức năng nơi gần nhất nếu thấy dấu hiệu nghi ngờ.

KHI XẢY RA TÌNH HUỐNG KHẨN CẤP

Trường hợp nghi ngờ hoặc phát hiện có dấu hiệu bị lừa đảo, bị tin tặc tấn công, Quý khách hãy thực hiện theo thứ tự ưu tiên như sau:

1. **KHÓA DỊCH VỤ HOẶC ĐỔI MẬT KHẨU DỊCH VỤ NGAY LẬP TỨC:**
   - **Đối với VCB Digibank:** Soạn tin nhắn theo cú pháp **VCB KHOA DIGIBANK** gửi **6167**
   - **Đối với VCB DigiBiz:** Đổi mật khẩu đăng nhập bằng cách vào mục **Tiện ích chọn Đổi mật khẩu.**
2. **LIÊN HỆ NGAY TỚI NGÂN HÀNG**
   Theo số hotline 1900545413, hoặc đến ngay các điểm giao dịch ngân hàng để được trợ giúp (nếu trong giờ hành chính).
3. **KHÔI PHỤC CÀI ĐẶT GỐC (FACTORY RESET)**
   Đối với thiết bị trường hợp phát hiện/nghi ngờ cài đặt ứng dụng giả mạo.
4. **TRÌNH BÁO VỚI CƠ QUAN CÔNG AN NƠI GẦN NHẤT.**

Hãy thường xuyên cập nhật đầy đủ các thông tin về hướng dẫn giao dịch an toàn trên website của Vietcombank