HƯỚNG DẪN GIAO DỊCH AN TOÀN NGÂN HÀNG TRỰC TUYẾN VÀ THẺ

Để đảm bảo an toàn bảo mật thông tin, bảo vệ quyền và lợi ích của Quý Khách hàng khi sử dụng các dịch vụ Ngân hàng trực tuyến và Thẻ của Ngân hàng TNHH Indovina (IVB), Quý Khách hàng vui lòng đọc kỹ và tuân thủ các hướng dẫn sau đây:

I. HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN CÁC KÊNH NGÂN HÀNG TRỰC TUYẾN

1. Nguyên tắc về bảo mật thông tin:

TUYỆT ĐỐI KHÔNG:

- Mở tài khoản và đăng ký dịch vụ Ngân hàng trực tuyến cho người khác sử dụng
- Viết tên đăng nhập và mật khẩu ra giấy hoặc lưu tự động trên trình duyệt web hoặc lưu dưới bất kỳ hình thức không an toàn nào để tránh lộ thông tin.
- Cung cấp thông tin Ngân hàng trực tuyến (tên truy cập/mật khẩu truy cập/mật khẩu OTP/mã OTP, mã PIN, Soft Token…) cho bất kỳ ai dưới mọi hình thức (điện thoại, email, mạng xã hội, ứng dụng, đường link, lời nói),….
- Đăng nhập/ khai báo thông tin cá nhân/ nhập OTP trên các đường dẫn lạ/ website không rõ nguồn gốc, đặc biệt là:
  - Các đường dẫn đính kèm trong các email nghi ngờ là giả mạo, tin nhắn SMS, ứng dụng mạng xã hội.
  - Các cuộc điện thoại gọi tới yêu cầu Quý Khách hàng làm theo hướng dẫn truy cập vào các trang web lạ hoặc cài đặt ứng dụng không rõ nguồn gốc.

  IVB không bao giờ chủ động yêu cầu Quý Khách hàng cung cấp tên đăng nhập và mật khẩu truy cập dịch vụ Ngân hàng trực tuyến qua điện thoại, email hoặc bất cứ hình thức nào. Mọi yêu cầu cung cấp thông tin bảo mật dịch vụ đều là giả mạo.
- Cài đặt các phần mềm lạ, phần mềm không có bản quyền, phần mềm không rõ nguồn gốc.
- Sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Ngân hàng trực tuyến, phần mềm tạo OTP.
- Rời khỏi hoặc để người khác sử dụng máy tính, thiết bị di động, thiết bị xác thực cho đến khi đăng xuất thành công ra khỏi dịch vụ.
- Sử dụng máy tính công cộng để truy cập, thực hiện giao dịch; sử dụng mạng Wifi công cộng khi sử dụng dịch vụ Ngân hàng trực tuyến.
- Chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng. IVB không bao giờ yêu cầu Quý Khách hàng chuyển tiền, nạp tiền vào số điện thoại để nhận thưởng bất kỳ chương trình khuyến mại nào của IVB.
- Làm theo hướng dẫn của các tin nhắn yêu cầu chuyển tiền để phục vụ công tác điều tra (buôn lậu ma túy, rửa tiền,...) để chứng minh sự trong sạch hoặc chuyển tiền để chứng minh khoản vay, hỗ trợ nâng cấp SIM, hỗ trợ cài đặt sinh trắc học… do đây là các cuộc gọi lừa đảo.

NÊN LÀM:

Về thiết lập mật khẩu và mã PIN:

- Thiết lập mật khẩu mạnh**:** Dài tối thiểu 08 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Mật khẩu truy cập dịch vụ: không dùng chung/giống các mật khẩu sử dụng của các dịch vụ khác: mật khẩu máy tính, facebook, email, zalo, viber,….
- Không sử dụng mật khẩu truy cập mà người khác dễ đoán như: thông tin cá nhân như ngày tháng năm sinh, số điện thoại, căn cước công dân, biển số xe, chứng minh nhân dân, tên bản thân, tên của người thân như vợ chồng/con, dãy số liên tục đơn giản như 123456, …
- Thiết lập và sử dụng mã PIN (Personal Identification Number) an toàn: Khi thiết lập mã PIN cho ứng dụng hoặc mã PIN Soft OTP, không sử dụng các dãy số liên tiếp, số lặp lại hoặc thông tin cá nhân dễ đoán.

Về bảo mật mật khẩu và mã PIN:

- Đổi mật khẩu truy cập các dịch vụ Ngân hàng trực tuyến lần đầu trong vòng 24h kể từ khi nhận được và thay đổi mật khẩu thường xuyên (tối thiểu định kỳ 06 tháng/lần).
- Đổi ngay lập tức sau khi phát hiện ra mình vừa click vào các đường dẫn (link) nghi ngờ giả mạo hoặc vô tình trả lời thông tin cho người lạ gọi tới hoặc khi bị lộ, nghi ngờ bị lộ để đảm bảo an toàn cho tài khoản.
- Tuyệt đối không chia sẻ mã PIN cho bất cứ ai dưới bất kỳ hình thức nào.

2. Nguyên tắc về sử dụng dịch vụ an toàn:

- Chỉ tải và đăng nhập ứng dụng IVB Mobile Banking, IVB Biz+ đã được xác nhận trên App Store hoặc Google Play và địa chỉ chính thức Internet Banking trên website: www.indovinabank.com.vn.

Logo IVB Indovina Bank trên App store

Logo IVB Indovina Bank trên Google Play

- Chỉ đăng nhập qua các thiết bị đáng tin cậy. Sử dụng máy tính/thiết bị di động có cài đặt đầy đủ các các bản vá lỗ hổng bảo mật của hệ điều hành và phần mềm ứng dụng IVB Mobile Banking, IVB Biz+; xem xét và cập nhật thường xuyên các phần mềm chống virus, tường lửa. Thường xuyên xóa lịch sử trình duyệt web (history), bộ nhớ đệm, vùng lưu dữ liệu tạm thời

của một thiết bị (cache) và các tệp do các trang web mà Quý Khách hàng truy cập tạo ra (cookie) của trình duyệt web.

- Để sử dụng dịch vụ Ngân hàng trực tuyến, Quý Khách hàng truy cập vào website chính thức của IVB tại địa chỉ www.indovinabank.com.vn và chọn mục "Đăng Nhập Ngân Hàng Trực Tuyến" hoặc tải ứng dụng IVB Mobile Banking/ IVB Biz+ trên App Store hoặc Google Play.
- Khi nhận được tin nhắn OTP từ IVB, cần kiểm tra kỹ nội dung tin nhắn, bao gồm: loại giao dịch, số tiền giao dịch, kênh giao dịch. Nếu nội dung tin nhắn không khớp đúng với giao dịch đang thực hiện, Quý Khách hàng tuyệt đối không nhập mã OTP này vào bất kỳ thiết bị nào hoặc tiết lộ cho bất kỳ ai.
- Khi hệ thống đang xử lý giao dịch, không thoát khỏi màn hình giao dịch và chờ thông báo kết quả từ hệ thống trước khi thực hiện các giao dịch khác.
- Luôn nhớ Đăng xuất/ Thoát khỏi thiết bị sau mỗi lần truy cập các dịch vụ Ngân hàng trực tuyến.
- Nên đăng ký sử dụng dịch vụ ngân hàng qua tin nhắn IVB SMS Banking và bật popup thông báo trên thiết bị di động để nhận thông báo biến động số dư giúp Quý Khách hàng biết được ngay lập tức những giao dịch trên tài khoản, hạn chế rủi ro và tổn thất đến mức thấp nhất.
- Trường hợp không thực hiện giao dịch nhưng vẫn nhận được thông báo từ IVB về: Mã OTP; Thay đổi số dư bất thường; Kích hoạt ứng dụng trên thiết bị khác; Liên kết ví điện tử, … Quý Khách hàng thông báo ngay cho IVB và không cung cấp các thông tin trên cho bất cứ ai và dưới bất kỳ hình thức nào.

II. HƯỚNG DẪN GIAO DỊCH AN TOÀN VỚI THẺ IVB

1. Nguyên tắc chung:

Khi nhận thẻ, Quý Khách hàng cần thực hiện:

- Kiểm tra tên trên thẻ đúng với tên Quý Khách hàng đã đăng ký.
- Đổi ngay mã số cá nhân (PIN) đối với các thẻ ghi nợ (ATM) mà Ngân hàng cung cấp tại máy ATM.
- Không đặt mật khẩu có liên quan đến các thông tin cá nhân như: Ngày tháng năm sinh, số điện thoại, biển số xe, căn cước công dân, ...
- Không ghi mật khẩu lên thẻ hoặc gần nơi để thẻ để tránh việc lộ thông tin và bị lợi dụng.

Luôn bảo mật thẻ và PIN, các mã số xác nhận của thẻ trong mọi trường hợp:

- Không đưa thẻ của mình cho bất cứ người nào khác trừ nhân viên của Ngân hàng hoặc các nhân viên thu ngân của ĐVCNT được chỉ định để làm việc với Quý Khách hàng.
- Không tiết lộ các thông tin in trên hai mặt trước và sau thẻ cũng như số PIN, các mã số xác nhận cho bất cứ ai. Quý Khách hàng là người duy nhất được biết các thông tin đó.
- Không tiết lộ thông tin giao dịch cho bất cứ ai.

Khi thực hiện giao dịch sử dụng PIN, Quý Khách hàng nên lưu ý:

- Đảm bảo không ai nhìn thấy số PIN khi thực hiện giao dịch (bằng cách che bàn phím);
- Nên đổi số PIN thường xuyên.

- Nếu nhập sai PIN 03 lần liên tiếp, thẻ sẽ bị khóa trong ngày giao dịch để đảm bảo an toàn tuyệt đối cho Quý Khách hàng.

Đăng ký và sử dụng các dịch vụ Ngân hàng trực tuyến của IVB (IVB Mobile Banking, IVB Biz+, SMS Banking...) để đảm bảo:

- Được thông báo các biến động liên quan đến tài khoản cá nhân hoặc hạn mức thẻ ngay khi một giao dịch thẻ được thực hiện.
- Chủ động khóa/ mở tính năng chi tiêu trên Internet đối với thẻ tín dụng quốc tế/ thẻ ghi nợ quốc tế/ thẻ ghi nợ nội địa để kiểm soát các giao dịch thanh toán online.

2. Nguyên tắc bảo quản thẻ:

- Không bẻ cong thẻ, gấp thẻ.
- Không để thẻ gần những thiết bị điện tử có thể phát sóng, từ tính mạnh có thể làm hỏng dữ liệu trên thẻ.
- Giữ thẻ cẩn thận và thường xuyên kiểm tra giúp Quý Khách hàng sớm phát hiện khi thẻ bị thất lạc.

3. Nguyên tắc khi giao dịch tại máy ATM:

- Quan sát kỹ máy ATM trước khi thực hiện giao dịch, đặc biệt tại các vị trí: khe đọc thẻ, bàn phím, camera. Nếu nhận thấy máy ATM có các thiết bị lạ hoặc có bất kỳ dấu hiệu bất thường nào, Quý Khách hàng ngừng giao dịch và thông báo ngay cho:
  - Tại ATM của IVB: Liên hệ ngay số hotline 1900 588 879.
  - Tại ATM của Ngân hàng khác: Liên hệ ngay số hotline dán trên máy ATM đó.

  Đồng thời, Quý Khách hàng nên đến Chi nhánh/ Phòng giao dịch gần nhất của IVB để thực hiện đổi thẻ mới nhằm ngăn ngừa rủi ro lộ lọt thông tin.
- Nên dùng tay che bàn phím khi nhập mật khẩu PIN.
- Quý Khách hàng thao tác sử dụng thẻ theo đúng hướng dẫn tại ATM, ATM sẽ nhả tiền ra trước và đưa thẻ ra sau, Quý Khách hàng nên đợi máy chi tiền ra, không nên bỏ đi ngay để tránh trường hợp máy ATM nhả tiền chậm và người khác có thể lấy được số tiền này.

4. Nguyên tắc khi thanh toán bằng thẻ tại các Đơn vị chấp nhận thẻ (ĐVCNT):

- Chú ý kiểm tra các thông tin trên hóa đơn thanh toán thẻ, đảm bảo các thông tin chính xác, đầy đủ. Chỉ ký nhận thanh toán khi đồng ý về tất cả các thông tin trên hóa đơn.
- Đảm bảo tất cả các giao dịch bằng thẻ tại các ĐVCNT phải được tiến hành trước mắt Quý Khách hàng.
- Đảm bảo được nhận lại thẻ sau khi thực hiện xong giao dịch tại các ĐVCNT.
- Giữ lại các hóa đơn thanh toán thẻ và các chứng từ có liên quan để phục vụ việc tra soát khiếu nại sau này (nếu có).

5. Nguyên tắc khi giao dịch thẻ để thanh toán trên Internet:

- Chỉ sử dụng thông tin thẻ để thanh toán tại các website do Visa/Master chứng thực (ghi chữ "Verified by Visa/Master") và có xác thực thêm mật khẩu OTP của dịch vụ 3D Secure, không nên sử dụng máy tính công cộng khi thực hiện các giao dịch thanh toán online.
- Đọc kỹ các chính sách của đơn vị trước khi đồng ý thanh toán.
- Luôn nhớ Thoát/Đăng xuất khỏi website sau khi kết thúc giao dịch.

- Sau khi thực hiện xong giao dịch thanh toán online, chủ động khóa tính năng chi tiêu Internet của thẻ bằng cách sử dụng dịch vụ mở khóa thẻ trực tuyến qua kênh IVB Ebanking/IVB Mobile Banking/ IVB Biz+ hoặc gọi 1900 588 879 để được hỗ trợ.

III. CẢNH BÁO CÁC LOẠI HÌNH LỪA ĐẢO TRỰC TUYẾN VÀ THẺ

Để Quý Khách hàng chủ động phòng ngừa rủi ro, giảm thiểu tổn thất, IVB liệt kê ở đây một số thủ đoạn phổ biến mà tội phạm thường sử dụng hiện nay:

- 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/ phần mềm ứng dụng ngân hàng số/ Fanpage/ tin nhắn SMS của ngân hàng và gửi đường link giả mạo để khách hàng nhập thông tin. Hoặc giả mạo nhân viên ngân hàng liên hệ khách hàng đề 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.
- Giả mạo doanh nghiệp, tổ chức thông báo khách hàng trúng thưởng khuyến mại, nhận mã khuyến mại… và yêu cầu khách hàng cung cấp thông tin bảo mật dịch vụ ngân hàng hoặc chuyển tiền.
- 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
- **Skimming:** là một phương thức ăn cắp thông tin tài khoản của thẻ khi giao dịch tại ATM. Kẻ xấu sử dụng những thiết bị điện tử rất tinh vi để đánh cắp thông tin trong thẻ ATM và ghi lại mã PIN của khách hàng, để có thể thực hiện thẻ giả và rút tiền của khách hàng từ ATM.
- **Phishing:** sử dụng như một tên website giả mạo để đánh lừa khách hàng đăng nhập vào để từ đó lợi dụng, xâm phạm tài chính và thông tin của khách hàng.
- **Hacking:** truy cập bất hợp pháp vào máy tính khách hàng đánh cắp thông tin cá nhân, thông tin truy cập cho mục đích sử dụng bất hợp pháp.
- **Lừa đảo bằng Deepfake/ AI:** Đây là hình thức cực kỳ nguy hiểm và bùng nổ mạnh mẽ. Kẻ gian sao chép giọng nói (Voice cloning) hoặc khuôn mặt (Deepfake video) của người thân, bạn bè hoặc đối tác để gọi video call mượn tiền, yêu cầu chuyển khoản gấp,..

IV. CÁC GIẢI PHÁP BẢO MẬT TẠI IVB

- Để đảm bảo an toàn khi thực hiện giao dịch Ngân hàng trực tuyến, ngoài mật khẩu khi đăng nhập, Quý Khách hàng xác thực bổ sung như: OTP qua tin nhắn, Soft OTP và/ hoặc chữ ký

số. Cơ chế này đảm bảo rằng ngay cả khi mật khẩu bị lộ, giao dịch vẫn không thể thực hiện nếu thiếu bước xác thực thứ hai - giúp bảo vệ tài khoản Quý khách hàng một cách toàn diện.

- Xác thực Sinh trắc học: đối chiếu dữ liệu sinh trắc học khuôn mặt để đảm bảo chính Quý Khách hàng khi thực hiện các giao dịch chuyển tiền trực tuyến trên 10 triệu đồng theo quy định của Ngân hàng Nhà nước.
- Cơ chế tự động khóa tài khoản: Sau 05 lần đăng nhập không thành công, IVB sẽ tạm khóa tài khoản của Quý Khách hàng. Để kích hoạt lại tài khoản, Quý Khách hàng cần liên hệ với Chi nhánh/ Phòng giao dịch gần nhất của IVB để được hướng dẫn.
- Giải pháp 3D Secure: Cung cấp thêm một lớp bảo vệ bằng mật mã yêu cầu Quý Khách hàng phải thực hiện mới được chấp thuận khi giao dịch trên Internet. Giải pháp 3D Secure được áp dụng được khi Quý Khách hàng thực hiện giao dịch trên các trang web có xác thực của Visa/ Master.
- Từ ngày 01/03/2026, theo Thông tư 77/2025/TT-NHNN, ứng dụng Mobile Banking sẽ tự động dừng hoạt động nếu phát hiện thiết bị di động không an toàn, đã bị root/jailbreak, hoặc cài phần mềm độc hại. Biện pháp này nhằm tăng cường bảo mật, bảo vệ tài sản Quý Khách hàng trước tội phạm công nghệ cao.
- Các giải pháp khác được thực hiện đồng bộ trong các khâu thiết kế và vận hành dịch vụ dựa trên nền tảng công nghệ hiện đại, tiên tiến và các chế độ cảnh báo rủi ro đáp ứng các thông lệ quốc tế.

V. LIÊN LẠC VỚI IVB

Quý Khách hàng vui lòng liên hệ với IVB trong các trường hợp sau đây:

- Khi gặp bất kỳ lỗi và sự cố trong quá trình sử dụng dịch vụ;
- Nếu bị mất điện thoại hoặc có bất kỳ sự thay đổi nào về số điện thoại đã đăng ký sử dụng gắn với dịch vụ;
- Khi có bất kỳ sự thay đổi về căn cước công dân, địa chỉ email, số điện thoại, địa chỉ cư trú, địa chỉ nhận sao kê thẻ, chữ ký;
- Khi thẻ bị mất cắp, thất lạc hoặc phát hiện các giao dịch thẻ không do Quý Khách hàng thực hiện;
- Khi nghi ngờ địa chỉ email, số điện thoại đang sử dụng bị lợi dụng cho dịch vụ bất hợp pháp;
- Vô tình click vào các đường link nghi ngờ giả mạo hoặc trả lời thông tin qua điện thoại với đối tượng nghi ngờ mạo danh;
- Khi có bất cứ băn khoăn, thắc mắc hay lo ngại nào về dịch vụ và cách sử dụng dịch vụ thẻ, Ngân hàng trực tuyến của IVB;
- Chủ động khoá dịch vụ và đổi mật khẩu của dịch vụ trên Internet Banking hoặc IVB Mobile Banking, IVB Biz+;
- Bị mất hoặc hư hỏng thiết bị tạo mã OTP/ nhận SMS OTP;
- Phát hiện bị lừa đảo hoặc nghi ngờ bị lừa đảo (Ví dụ: Nhận được các cuộc gọi mạo danh yêu cầu chuyển tiền để phục vụ điều tra, cài đặt ứng dụng sinh trắc học giả mạo, nộp tiền nâng cấp SIM,...);

- Bị tin tặc hoặc nghi ngờ bị tin tặc tấn công (Ví dụ: Bất ngờ nhận được mã OTP, thông báo kích hoạt thiết bị khác, thông báo liên kết ví điện tử hoặc biến động số dư dù không thực hiện giao dịch,…)

Thông tin liên hệ:

- Nếu cần bất kỳ sự hỗ trợ nào trong quá trình sử dụng Dịch vụ, Quý Khách hàng vui lòng liên hệ:
  - Trung tâm Dịch vụ Khách hàng IVB 24/7: **1900 588 879**
  - Email: **support@indovinabank.com.vn**
  - Hoặc **các điểm giao dịch của IVB** trên toàn quốc.
- Trong mọi trường hợp, số điện thoại duy nhất của Trung tâm Dịch vụ Khách hàng IVB 24/7 gọi đến điện thoại của Quý Khách hàng đều hiển thị là đầu số 1900 588 879

Trân trọng cảm ơn Quý Khách hàng đã luôn tin tưởng lựa chọn và sử dụng các dịch vụ của IVB!