

HƯỚNG DẪN GIAO DỊCH AN TOÀN NGÂN HÀNG ĐIỆN TỬ VÀ THẺ

Để đảm bảo an toàn bảo mật, bảo vệ quyền và lợi ích của chính mình, khi thực hiện giao dịch trên các kênh Ngân hàng điện tử và giao dịch bằng thẻ của NH TNHH Indovina(IVB), Quý khách hàng vui lòng đọc kỹ và tuân theo các thông tin hướng dẫn sau đây

IVB trân trọng cảm ơn Quý khách hàng!

MỤC LỤC

I. HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN CÁC KÊNH NGÂN HÀNG ĐIỆN TỬ:	1
1. Nguyên tắc về bảo mật thông tin.....	1
2. Nguyên tắc về sử dụng dịch vụ an toàn.....	2
II. HƯỚNG DẪN GIAO DỊCH AN TOÀN VỚI THẺ IVB:.....	2
1. Nguyên tắc chung	2
2. Nguyên tắc bảo quản thẻ.....	3
3. Nguyên tắc khi giao dịch tại máy ATM	3
4. Nguyên tắc khi thanh toán bằng thẻ tại các đơn vị chấp nhận thẻ (ĐVCNT)	3
5. Nguyên tắc khi giao dịch thẻ để thanh toán trên Internet.....	3
III. CẢNH BÁO CÁC LOẠI HÌNH TẤN CÔNG TRỰC TUYẾN:	4
IV. CÁC GIẢI PHÁP BẢO MẬT TẠI IVB:	4
V. LIÊN LẠC VỚI IVB:.....	5

I. HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN CÁC KÊNH NGÂN HÀNG ĐIỆN TỬ:

1. Nguyên tắc về bảo mật thông tin

TUYỆT ĐỐI KHÔNG:

- Mở tài khoản và đăng ký dịch vụ Ngân hàng điện tử cho người khác sử dụng;
- Tiết lộ mã PIN, mật khẩu, tên truy cập (username) của bất kỳ dịch vụ Ngân hàng điện tử cho bất cứ ai qua bất kỳ kênh nào như điện thoại, email, đường link....
- Click vào các đường link lạ và khai báo thông tin cá nhân cho bất kỳ địa chỉ email đã gửi đến hoặc điện thoại gọi tới. Indovinabank không bao giờ chủ động yêu cầu Quý khách hàng khai báo cùng một lúc cả tên đăng nhập và mật khẩu truy cập của dịch vụ Ngân hàng điện tử qua điện thoại hoặc email;
- Cài đặt các phần mềm, công cụ tiện ích từ các trang web không tin cậy, không có bản quyền;
- Lưu lại tên và mật khẩu đăng nhập trên các trình duyệt web;
- Sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Ebanking;
- Chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng. IVB không bao giờ yêu cầu khách hàng chuyển tiền, nạp tiền vào số điện thoại để nhận thưởng bất kỳ chương trình khuyến mại nào của IVB.

QUÝ KHÁCH NÊN:

Sử dụng máy tính cá nhân/ điện thoại di động có cài đặt phần mềm diệt virus để truy cập dịch vụ Ngân hàng điện tử của IVB;

Chỉ dùng máy tính công cộng để truy cập, thực hiện giao dịch E-banking trong trường hợp cần thiết và sau đó phải sử dụng phương tiện an toàn để thay đổi ngay mật khẩu truy cập tài khoản đăng nhập

Bảo vệ bí mật mã khóa bí mật, OTP và bảo quản chứng thư số(PKI token) như bảo quản tiền mặt

- **Về cài đặt mật khẩu:**
 - + Sử dụng mật khẩu đủ tin cậy là mật khẩu đủ độ dài (từ 6 ký tự), có sự kết hợp giữa chữ hoa với chữ thường và chữ số.
 - + Không sử dụng mật khẩu có chứa thông tin mang tính cá nhân mà người khác dễ dàng suy đoán như ngày tháng năm sinh, số điện thoại, biển số xe, tên bản thân, tên của người thân như vợ chồng/con, dãy số liên tục đơn giản như 123456.
- **Về bảo mật mật khẩu:**
 - + Đổi mật khẩu truy cập các dịch vụ Ngân hàng điện tử lần đầu trong vòng 24h kể từ khi nhận được.
 - + Thay đổi mật khẩu thường xuyên (tối thiểu định kỳ 12 tháng/lần) hoặc khi bị lộ, nghi bị lộ để đảm bảo an toàn cho tài khoản.
 - + Tránh viết mật khẩu ra giấy hoặc ghi chép dưới hình thức khác.

+ Thay đổi mật khẩu truy cập dịch vụ IVB Ebanking(Internet banking/Mobile banking) ngay lập tức sau khi phát hiện ra mình vừa click vào các đường link nghi ngờ giả mạo hoặc vô tình trả lời thông tin cho người lạ gọi tới.

2. Nguyên tắc về sử dụng dịch vụ an toàn

- Để đăng nhập vào chương trình IVB Ebanking, Quý khách nên truy cập vào website chính thức của Indovinabank tại địa chỉ www.indovinabank.com.vn và chọn mục Ngân Hàng Trực Tuyến/Internet Banking hoặc tải ứng dụng IVB Mobile banking;
- 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 tuyệt đối không nhập mã OTP này vào bất kỳ trang web 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 hệ thống sau mỗi lần truy cập các dịch vụ Ngân hàng điện tử;
- Nên đăng ký sử dụng đồng thời dịch vụ ngân hàng qua tin nhắn IVB SMS Banking để nhận tin nhắn thông báo biến động số dư nhằm ngay lập tức biết được những giao dịch trên tài khoản, hạn chế rủi ro và tổn thất đến mức thấp nhất.

II. HƯỚNG DẪN GIAO DỊCH AN TOÀN VỚI THẺ IVB:

1. Nguyên tắc chung

- Khi nhận thẻ, Quý khách cần thực hiện:
 - + Kiểm tra các thông tin trên thẻ để đảm bảo đúng với các thông tin Quý khách 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 để kích hoạt thẻ.
 - + Không đặt mật khẩu có liên quan đến các thông tin cá nhân như: Ngày tháng năm sinh, số điện thoại, biển số xe...
 - + Không ghi mật khẩu lên thẻ hoặc gắn nơi để thẻ để tránh việc lộ thông tin và bị lợi dụng.
- Luôn bảo mật thẻ và PIN của thẻ trong mọi trường hợp:
 - + Không đưa thẻ của mình cho bất cứ người nào khác trừ những nhân viên của ngân hàng hoặc các nhân viên thu ngân của ĐVCNT được chỉ định để làm việc với Quý khách.
 - + Không tiết lộ các thông tin in trên hai mặt trước và sau thẻ cũng như số PIN cho bất cứ ai. Quý khách là người duy nhất được biết các thông tin đó.
- Khi thực hiện giao dịch sử dụng PIN, Quý khách 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 khách hàng.
- Đăng ký và sử dụng các dịch vụ ngân hàng điện tử của IVB (IVB Mobile banking, 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 để kiểm soát các giao dịch thanh toán online.
- Kiểm tra chi tiết sao kê thẻ tín dụng quốc tế. Trong trường hợp có thắc mắc, xin vui lòng thông báo cho Ngân hàng bằng văn bản trong vòng 45 ngày kể từ ngày thực hiện giao dịch.
- Chủ động thông báo ngay cho Ngân hàng những thay đổi của Quý khách về địa chỉ cư trú, địa chỉ gửi sao kê, thay đổi số điện thoại liên hệ, chữ ký.

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.
- Tránh làm xước bằng từ màu đen ở mặt sau của thẻ.
- Giữ thẻ cẩn thận và để thẻ ở vị trí có thể giúp Quý khách sớm phát hiện việc mất thẻ.

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 ngừng giao dịch và thông báo ngay cho IVB qua hotline 1900 588 879.
- Nên dùng tay che bàn phím khi nhập mật khẩu PIN.
- ATM sẽ nhả thẻ ra trước và đưa tiền ra sau, 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.
- 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 hoặc gọi 1900 588 879 để được hỗ trợ.

III. CẢNH BÁO CÁC LOẠI HÌNH TẤN CÔNG TRỰC TUYẾN:

Để Quý khách chủ động phòng ngừa rủi ro, giảm thiểu tổn thất, Indovinabank liệt kê ở đây một số loại hình tấn công trực tuyến mà tội phạm thường sử dụng hiện nay:

- *Lừa đảo tài chính quốc tế*: Trò lừa thường bắt đầu bằng một bức thư hoặc email có hình thức như được gửi trực tiếp tới người nhận nhưng thực tế đã được phát tán cho nhiều người để đưa ra đề xuất theo đó người nhận sẽ nhận được một khoản tiền lớn nhưng thực tế thì người nhận sẽ không thể nhận được.
- *Trộm danh tính*: là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính, chủ yếu là trộm thông tin thẻ tín dụng, tạo ra một món nợ lớn cho khách hàng.
- *Virus*: là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác. Virus thường phá hoại máy tính của nạn nhân bị lây nhiễm để lấy cắp các thông tin cá nhân nhạy cảm, mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển nhằm có lợi cho người phát tán virus. Gần đây, hình thức virus qua email khá phổ biến, xâm nhập vào các thư điện tử và thường xuyên nhân bản để phát tán virus đến những người trong danh bạ của khách hàng.
- *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 bằng Internet.

IV. CÁC GIẢI PHÁP BẢO MẬT TẠI IVB:

- Sử dụng công nghệ bảo mật xác thực hai yếu tố thông qua mật khẩu đăng nhập và thiết bị bảo mật tin nhắn OTP hoặc chữ ký số.
- Cơ chế tự động khóa tài khoản: Sau 05 lần đăng nhập không thành công, IVB sẽ tạm khóa tài khoản của Quý khách. Để kích hoạt lại tài khoản, khách hàng cần liên hệ với Chi nhánh/Phòng giao dịch

gần nhất của Indovinabank để được hướng dẫn.

- Dịch vụ 3D secure: Cung cấp thêm một lớp bảo vệ bằng mật mã yêu cầu khách hàng phải thực hiện mới được chấp thuận khi giao dịch trên internet. Dịch vụ 3D secure chỉ được áp dụng được khi khách thực hiện giao dịch trên các trang web có xác thực của Visa/Master.
- 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 vui lòng liên hệ với Trung tâm dịch vụ khách hàng 24/7 của IVB theo số hoặc 1900 588 879 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 ngân hàng điện tử.
- Khi có bất kỳ sự thay đổi về 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 thực hiện.
- Khi nghi ngờ địa chỉ email, số điện thoại đang sử dụng cho dịch vụ ngân hàng điện tử bị lợi dụng.
- 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 điện tử của IVB.

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 đều hiển thị là đầu số 1900 588 879

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

Ngân hàng điện tử của IVB – Cùng phát triển bền vững