

HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN BIDV - EBANKING

Kính gửi Quý khách hàng,

Thời gian vừa qua, xuất hiện một số kẻ gian lợi dụng sơ hở của khách hàng để đánh cắp thông tin tài khoản ngân hàng điện tử nhằm chiếm đoạt tài sản khách hàng. Vì vậy, để bảo vệ thông tin và tài sản, giúp khách hàng tránh được những rủi ro cũng như an tâm khi sử dụng các tiện ích dịch vụ ngân hàng, BIDV khuyến nghị Quý khách hàng lưu ý một số nội dung sau:

DẤU HIỆU LỪA ĐẢO

1. Bất ngờ nhận được cuộc gọi, tin nhắn, email, tin trên mạng xã hội thông báo trúng thưởng, nhờ nhận tiền từ nước ngoài chuyển về... kèm theo hướng dẫn nhận giải thưởng bằng cách cung cấp mật khẩu, mật khẩu sử dụng một lần – còn gọi là mã xác thực giao dịch (OTP), sau đó kẻ gian sẽ lợi dụng OTP và mật khẩu để chuyển tiền.
2. Bất ngờ nhận được cuộc gọi, tin nhắn tự xưng là cán bộ ngân hàng hoặc cán bộ điều tra trong đó có yêu cầu cung cấp các thông tin cá nhân về tài khoản ngân hàng, hoặc cung cấp thông tin vì trách nhiệm, đe dọa nào đó.
3. Bất ngờ nhận được cuộc gọi xưng là bạn bè, người thân, họ hàng lâu ngày không gặp đang gặp khó khăn cần được giúp đỡ gấp bằng việc mua hộ mã thẻ cào, chuyển tiền vào số tài khoản do người đó cung cấp.

NHỮNG VIỆC KHÔNG LÀM

1. KHÔNG cung cấp tên, mật khẩu truy cập dịch vụ ngân hàng điện tử, không cung cấp OTP, không chia sẻ các thiết bị lưu trữ các thông tin này, thông tin thẻ, mã số PIN cho bất kỳ đối tượng nào dưới bất kỳ hình thức nào, kể cả nhân viên ngân hàng hoặc nhân viên gọi đến tự xưng là cán bộ hỗ trợ khách hàng của BIDV.
2. KHÔNG cung cấp các thông tin cá nhân có liên quan đến tài khoản và dịch vụ Ngân hàng điện tử như: Họ tên khách hàng, số CMND, số tài khoản, địa chỉ email, số điện thoại đăng ký dịch vụ, nội dung tin nhắn theo yêu cầu của bất kỳ ai **trừ khi** quý khách hàng đã chủ động gọi điện đến hai số điện thoại hỗ trợ của BIDV (**1900 9247 và 04 22200588**) để yêu cầu trợ giúp hoặc đăng ký dịch vụ.
3. KHÔNG truy cập các trang web không đáng tin cậy, KHÔNG nhập thông tin cá nhân và thông tin dịch vụ ngân hàng điện tử vào bất kỳ trang web hay ứng dụng không chính thức của BIDV.
4. KHÔNG lưu lại tên đăng nhập và mật khẩu trên các trình duyệt web, trên các thiết bị sử dụng chung (nhiều người sử dụng), trên máy tính công cộng...
5. KHÔNG cài đặt các phần mềm, công cụ tiện ích từ các trang web không tin cậy, không có bản quyền. Xóa các tiện ích mở rộng không rõ nguồn gốc hoặc khả nghi trên các trình duyệt hiện có.

6. KHÔNG sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Internet Banking – Mobile Banking, phần mềm tạo OTP.

NHỮNG VIỆC NÊN LÀM

1. Để đề phòng truy cập vào trang web giả mạo, Quý khách đảm bảo đăng nhập đúng địa chỉ trang web của BIDV bằng cách gõ trực tiếp nội dung www.bidv.com.vn hoặc www.bidvsmartbanking.vn trên thanh địa chỉ của trình duyệt. Sau đó, quý khách có thể đăng nhập dịch vụ ngân hàng điện tử, khai báo thông tin hoặc tải các ứng dụng xuất phát từ các trang web này. Quý khách không đăng nhập vào trang web dịch vụ ngân hàng điện tử từ các liên kết/địa chỉ truy cập có sẵn trong email hoặc các trang web không phải của BIDV.

2. Khi Quý khách bị mất điện thoại, chuyển nhượng sim điện thoại cho người khác hoặc nhận thấy có các giao dịch bất thường liên quan đến tài khoản hãy **thông báo ngay** đến ngân hàng theo một trong các số điện thoại: **1900 9247; 04 22200588** hoặc các địa điểm giao dịch BIDV gần nhất để thay đổi thông tin hoặc tạm khóa các dịch vụ Quý khách đăng ký với Ngân hàng có liên quan đến số điện thoại.

3. Cài đặt, sử dụng phần mềm diệt vi rút trên thiết bị cá nhân sử dụng để giao dịch Internet Banking.

4. Chỉ dùng máy tính công cộng để truy cập, thực hiện giao dịch Internet Banking trong trường hợp thật sự cần thiết và sau đó phải sử dụng phương tiện an toàn để thay đổi ngay mật khẩu. Quý khách nên cài đặt, sử dụng, cập nhật hệ điều hành và trình duyệt mới nhất, được nhà sản xuất hỗ trợ để tránh phải đối mặt với nguy cơ máy tính sử dụng bị lây nhiễm virus, các phần mềm gián điệp... khi giao dịch Ngân hàng điện tử.

5. Bảo vệ bí mật mật khẩu, OTP và không chia sẻ các thiết bị lưu trữ các thông tin này. Cách thiết lập mật khẩu và thay đổi mật khẩu tài khoản truy cập theo định kỳ tối thiểu 03 tháng một lần, hoặc khi bị lộ, nghi bị lộ.

6. Thoát khỏi ứng dụng Internet Banking – Mobile Banking khi không sử dụng.

7. Trường hợp Quý khách thường xuyên giao dịch với giá trị cao trên Internet Banking, quý khách có thể lựa chọn hình thức bảo mật cao là hardware token; kích hoạt xác thực bằng vân tay nếu điện thoại Quý khách hỗ trợ tính năng này.

8. Đăng ký sử dụng dịch vụ nhận tin nhắn báo biến động số dư tài khoản, giao dịch thẻ (BSMS) để tăng tính an toàn cho tài khoản và thẻ.

9. Đọc và thực hiện đúng các quy định về Hướng dẫn giao dịch an toàn để đảm bảo sử dụng các dịch vụ ngân hàng điện tử/thẻ đúng cách, an toàn, bảo mật

10. Liên hệ ngay đến BIDV (qua điện thoại, email, facebook) để xác minh thông tin khi nhận được cuộc gọi thông báo trúng thưởng, có giao dịch nghi ngờ từ tài khoản/thẻ hoặc để được hỗ trợ khi có bất khoản, vướng mắc cần trao đổi thông tin với BIDV. Các

kênh hỗ trợ và chăm sóc khách hàng chính thức của BIDV:

- Qua các số điện thoại: **1900 9247** hoặc **04 22200588**
- Qua email: **bidv247@bidv.com.vn**
- Qua trang facebook: <https://www.facebook.com/BIDVbankvietnam/>

Quý khách lưu ý:

Thông qua các kênh hỗ trợ và chăm sóc khách hàng chính thức của BIDV, để hỗ trợ xử lý yêu cầu của khách hàng cũng như tư vấn và cung cấp một số sản phẩm dịch vụ ngân hàng, Quý khách hàng có thể cần cung cấp một số thông tin cá nhân để định danh khách hàng cho BIDV như: Họ tên khách hàng, ngày tháng năm sinh, số CMND, số tài khoản, địa chỉ email, số điện thoại đăng ký dịch vụ, thông tin về lịch sử giao dịch của tài khoản, tên đăng nhập dịch vụ... (Riêng qua kênh facebook hiện BIDV không yêu cầu cung cấp các thông tin liên quan đến tài khoản cá nhân).

BIDV kính chúc Quý khách có những trải nghiệm dịch vụ an toàn và hiệu quả!