Như lời cam kết của VietABank nhằm giữ tài khoản và thông tin cá nhân của Quý khách an toàn bảo mật. VietABank cung cấp một số lời khuyên hữu ích cho việc nhận dạng và ngăn chặn email lừa đảo:

1. Phòng tránh email gian lận

Lừa đảo và giả mạo

- Email lừa đảo và giả mạo trông giống với email chính thức của ngân hàng VietABank, và cố gắng đánh lừa Quý khách chuyển đến một website giả mạo để yêu cầu cung cấp thông tin về tài khoản, số điện thoại, chứng minh nhân dân, mật khẩu, ATM, PIN...

- Những cách thức để lừa đảo và giả mạo như sau:

- Đường dẫn (link) với tên gọi ngân hàng VietABank (hay website VietAbank, Internet Banking VietABank, VietABank EzMobile,...) nhưng không phải links chính thức của ngân hàng VietABank. Quý khách rê chuột vào link trong email lừa đảo, chương trình sẽ thể hiện link URL. Và quan trọng rằng đừng nhấp chuột vào link.
- Yêu cầu thông tin cá nhân.
- Thông báo nâng cấp hệ thống, an toàn bảo mật.
- Một lời đề nghị hấp dẫn.

2. Cách tự bảo vệ

2.1 Tuyệt đối không

- Mở tài khoản và đăng ký dịch vụ Ngân hàng điện tử cho người khác sử dụng.
- Tiết lộ tên đăng nhập (username), mật khẩu truy cập, mã SoftOTP của bất kỳ dịch vụ Ngân hàng điện tử, số thẻ, số tài khoản cho bất cứ ai qua bất kỳ kênh nào như điện thoại, email, mạng xã hội, ứng dụng, website, đường link lạ…
- VietABank 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.
- Chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng. VietABank 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 VietABank.

2.2 Quý khách nên

- ***Về cài đặt mật khẩu:***

  + Sử dụng mật khẩu đủ tin cậy là mật khẩu đủ độ dài (từ trên 8 ký tự), có sự kết hợp giữa chữ hoa với chữ thường, chữ số, và ký tự đặc biệt.

  + 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 1234567…

- ***Về bảo mật mật khẩu:***

  + Đổi mật khẩu, kích hoạt mã SoftOTP 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 06 tháng/lần) 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 VietABank EzMobile, Internet 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.

3. Các giải pháp bảo mật tại VietABank

- Sử dụng công nghệ bảo mật xác thực hai yếu tố thông qua thiết bị bảo mật tin nhắn SMSOTP và ứng dụng VietABank SoftOTP. Mỗi mã OTP sinh ra chỉ được sử dụng một lần duy nhất và không trùng lặp nên tin tặc không thể xâm nhập vào tài khoản của Quý khách để thực hiện giao dịch bất hợp pháp.
- Cơ chế tự động khóa tài khoản dịch vụ Ngân hàng điện tử: Sau 03 lần đăng nhập không thành công, VietABank sẽ tạm khóa tài khoản của Quý khách. Để kích hoạt lại tài khoản, khách hàng cần liên hệ với VietABank để được hướng dẫn.
- Cơ chế tự động khóa tính năng xác thực giao dịch bằng mã SoftOTP (Khách hàng sẽ không thể thực hiện giao dịch trong 24 giờ): Sau 05 lần nhập mã SoftOTP không thành công. Để kích hoạt lại tính năng này, khách hàng cần liên hệ với VietABank để được hướng dẫn.
- Tích hợp ứng dụng VietABank eToken cho các khách hàng sử dụng dịch vụ Internet Banking- ứng dụng xác thực được cài đặt vào thiết bị di động của người sử dụng nhằm giúp khách hàng xác thực các giao dịch và sử dụng các dịch vụ trên VietABank Internet Banking

4. Liên lạc với VietABank

- Khi gặp bất kỳ lỗi và sự cố trong quá trình sử dụng dịch vụ, Quý khách vui lòng liên hệ với Trung

tâm dịch vụ khách hàng 24/7 của VietABank theo số **1900 555 590**.

- 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, Quý khách cần liên hệ VietABank hoặc chủ động truy cập VietABank Internet Banking để tạm khóa dịch vụ ngân hàng số.
- 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 VietABank.

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.

eBanking VietABank sử dụng giao thức bảo mật tiêu chuẩn để mã hóa dữ liệu trên đường truyền. Mã hóa giúp tạo môi trường an toàn thông tin giữa trình duyệt với ngân hàng. Để giúp Quý khách đảm bảo vào website chính thức Internet banking của ngân hàng VietABank trước khi đăng nhập, Quý khách vui lòng kiểm tra trên thanh trình duyệt:

- Kiểm tra link: https://ebanking.vietabank.com.vn
- Chữ xanh lá cây/ có tô bóng nổi.
- Biểu tượng chìa khóa.