Kính thưa Quý Khách hàng,

Ngân hàng TMCP Ngoại thương Việt Nam (Vietcombank) xin cảm ơn Quý Khách hàng đã tin tưởng và sử dụng dịch vụ của Vietcombank.

Trong thời gian gần đây, Vietcombank đã ghi nhận một số trường hợp khách hàng chuyển tiền không đúng người hưởng do bị "hack email" (*nghĩa là* Tin tặc (Hacker) xâm nhập trái phép email của khách hàng hoặc đối tác để thay đổi thông tin người hưởng trên các chứng từ giao dịch) và yêu cầu Vietcombank hỗ trợ đòi tiền từ ngân hàng nước ngoài. Tuy nhiên, khả năng đòi được tiền đối với giao dịch bị hack email là rất thấp do Hacker thường rút tiền ra khỏi tài khoản ngay khi nhận được tiền hoặc do thủ tục đòi tiền rất phức tạp của ngân hàng nước ngoài.

Nhằm hỗ trợ Quý Khách hàng phòng ngừa rủi ro bị hack email trong giao dịch với đối tác nước ngoài, Vietcombank xin lưu ý một số nội dung như sau:

- **Các dấu hiệu nhận biết giao dịch lừa đảo**:
  - Hợp đồng và các giao dịch liên quan đến thực hiện hợp đồng (thông báo giao hàng, hóa đơn đòi tiền, thương lượng…) đều thực hiện qua email. Bên xuất khẩu và bên nhập khẩu không xác nhận giao dịch bằng các hình thức liên lạc khác.
  - Đối tượng Hacker hướng tới chủ yếu là các doanh nghiệp vừa và nhỏ, các công ty có tính bảo mật và an toàn trong hệ thống quản trị mạng chưa cao hoặc thiếu các qui định về an toàn khi sử dụng email.
  - Người hưởng không phải bên xuất khẩu.
  - Thông tin thanh toán đột ngột thay đổi.
  - Bên xuất khẩu không đề cập đến thay đổi thông tin người hưởng nhưng trên hóa đơn đòi tiền lại ghi thông tin người hưởng khác với thông tin trên hợp đồng.
  - Địa chỉ quốc gia của người hưởng khác với địa chỉ quốc gia của ngân hàng hưởng.
- **Các hình thức lừa đảo phổ biến**:
  - Hacker sửa nội dung hợp đồng ký qua email.
  - Hacker giả mạo email để thay đổi thông tin người hưởng: sử dụng đúng email của bên xuất khẩu hoặc email tương tự nhưng tên miền khác.
  - Hacker sửa thông tin người hưởng trên hóa đơn hoặc chèn thông tin người hưởng giả trên hóa đơn.
- **Các thị trường Hacker thường yêu cầu chuyển tiền đến**
  - Trung Quốc, Hồng Kông, Malaysia, Mỹ…
  - Các quốc gia ở châu Âu, đặc biệt là Anh do tại thị trường này, các ngân hàng thực hiện ghi có cho khách hàng theo số tài khoản mà không kiểm tra tên tài khoản.
- **Biện pháp phòng ngừa**

- Xem xét cẩn thận tất cả email. Cảnh giác với các email yêu cầu chuyển khoản để xác định xem yêu cầu này có khác thường không.
- Xác minh bất kỳ thay đổi nào trong chỉ thị thanh toán của đối tác. Trường hợp nghi ngờ giả mạo, Quý Khách hàng cần liên hệ ngay với đối tác bằng kênh thông tin tin cậy khác để xác thực thông tin.
- Với các đối tác mới làm ăn, Quý Khách hàng có thể tham khảo thông tin từ các Ngân hàng hoặc các tổ chức đánh giá tín nhiệm quốc tế (một số trang thông tin cung cấp đánh giá tín nhiệm của Doanh nghiệp nước ngoài như: http://www.dnb.com; http://dnbvietnam.com/vi/ cung cấp dịch vụ tra cứu đối với thông tin thương mại của hàng triệu Doanh nghiệp trên toàn cầu).

Trong quá trình sử dụng dịch vụ, nếu cần thêm thông tin hoặc cần hỗ trợ, Quý Khách hàng vui lòng liên hệ với bất kì Chi nhánh nào trong hệ thống Vietcombank**.**

Vietcombank luôn mong muốn mang lại sự an toàn khi cung cấp dịch vụ cho Quý Khách hàng.

Dear valued Customers,

Joint Stock Commercial Bank for Foreign Trade of Vietnam (Vietcombank) would like to send greetings and thank you for using our service.

It has been recorded by Vietcombank that several customers whose emails or whose trading partners' emails had been hacked (*It means that* Hackers hack into emails of customers or their trading partners to change the beneficiary's information on documents) transferred money to incorrect beneficiaries and required Vietcombank to help to claim from foreign banks. However, the possibility of claiming money back is very low. The reason is that Hackers usually withdraw money from their account immediately when money is credited to their account or foreign banks' procedure of claiming money back is too complicated.

In order to support Customers to prevent risks of email hacking, Vietcombank would like to announce as follows:

- **Early warning signs of fraud**
  - Contracts and related transactions (Delivery Notice, Invoice, negotiations…) are processed via email. Exporters and importers do not confirm transactions by other methods of communication.
  - Hackers mainly aim at SMEs and businesses with their low-security IT system and lack of email rules and regulations.
  - The beneficiary is not the exporter.
  - Payment instructions are suddenly changed.
  - The beneficiary on the invoice is different from that on the contract whereas the exporter does not inform of the change in the beneficiary.
  - The country of the beneficiary is different from that of the beneficiary's bank.

- **Common fraud techniques**
  - Hackers modify contracts signed via email.
  - Hackers use fake email to change beneficiary's information: email of the exporter or similar emails with other domains.
  - Hackers modify beneficiary's information on the invoice or insert fake beneficiary's information on the invoice.
- **Markets aimed at by hackers to transfer money**
  - China, Hong Kong, Malaysia, U.S.A…
  - Countries in Europe, especially England because in this country, banks credit to customers' accounts without checking their name.
- **Preventive measures**
  - Consider all emails with great care. Be cautious about emails of transferring request to determine if they are unusual.
  - Verify any changes in payment instructions. In case of suspicion, please contact trading partners to confirm in other methods of communication.
  - For new partners, please refer to banks or credit reference agencies (for example, http://www.dnb.com; http://dnbvietnam.com/vi/ are commonly used to provide a range of credit reference and research services of millions of businesses all over the world).

If you have any questions or need further assistance, do not hesitate to visit Vietcombank branches.

Vietcombank always hope to bring security to our valued customers' transactions.

Sincerely./.