BNP PARIBAS

Dear our valued clients,
Kính gửi Quý khách hàng,

As summer time approaches, we want to remind you that **credit transfer scams are on the rise**, and no company, be it a large group or an SME, is safe. Vietnam is not immune, and we know that some companies have had recently to face cyber fraud.

Khi thời gian mùa hè đến gần, chúng tôi muốn nhắc nhở Quý khách rằng các vụ lừa đảo chuyển tiền tín dụng đang gia tăng và không có công ty nào, dù là một nhóm lớn hay một doanh nghiệp vừa và nhỏ, vẫn an toàn. Việt Nam không miễn nhiễm khỏi điều này và chúng tôi biết rằng gần đây một số công ty đã phải đối mặt với gian lận trên mạng

1. ***The Fake vendor scams*** (perpetrated by a fake supplier who requests a bank account to be amended) is the most dangerous scheme.
   Lừa đảo nhà cung cấp giả (bị tấn công bởi nhà cung cấp giả yêu cầu sửa đổi tài khoản ngân hàng) là kế hoạch nguy hiểm nhất
   Here are some tips/ đây là một số lời khuyên:
   - ☐ **Have call-back procedures in case of bank account change**, using safe contact details (not those contained in the notification or invoices). Double-check in case of tier one supplier. Beware: fraudsters may hack your vendor's email. Use alternative contact channel (phone in particular)
     Có các thủ tục gọi lại trong trường hợp thay đổi tài khoản ngân hàng, sử dụng các chi tiết liên lạc an toàn (không phải các chi tiết có trong thông báo hoặc hóa đơn). Kiểm tra lại trong trường hợp nhà cung cấp cấp một. Hãy coi chừng: những kẻ lừa đảo có thể hack email của nhà cung cấp của Quý khách. Sử dụng kênh liên lạc thay thế (cụ thể là điện thoại)
   - ☐ **Check the identity of anyone seeking information on your accounting data, invoices**... It could be a fraudster impersonating your client, an auditor, public administrations... to set up an attack on your main clients.
     Kiểm tra danh tính của bất kỳ ai đang tìm kiếm thông tin về dữ liệu kế toán, hóa đơn của Quý khách ... Đó có thể là một kẻ lừa đảo mạo danh khách hàng của Quý khách, kiểm toán viên, chính quyền công cộng ... để thiết lập một cuộc tấn công vào các khách hàng chính của Quý khách
   - ☐ To know more about **corporate best practices against vendor scam** or **invoice theft**, check on the following link some documents available on BNPP Vietnam website:
     Để biết thêm về các cách thực hiện tốt nhất của công ty chống lại hành vi lừa đảo của nhà cung cấp hoặc đánh cắp hóa đơn, hãy kiểm tra liên kết sau đây một số tài liệu có sẵn trên trang web BNPP Việt Nam

   http://vietnam.bnpparibas.com/en/corporates-institutions/notification/fraud-alert/

2. Generally, companies believe that they are protected against ***fake CEO scams***, but such frauds still sometimes succeed, often involving newcomers.

Thông thường, các công ty tin rằng họ được bảo vệ trước những trò gian lận của CEO giả, nhưng những vụ lừa đảo như vậy đôi khi vẫn thành công, thường liên quan đến người mới

Here are some tips/ đây là một số lời khuyên:

- ☐ Be sure to raise **awareness of all staff** authorized to make transfers, especially newcomers, including senior management.
  Hãy chắc chắn nâng cao nhận thức của tất cả các nhân viên được ủy quyền để thực hiện chuyển khoản, đặc biệt là người mới, bao gồm cả quản lý cấp cao
- ☐ Avoid orders and validation by **fax**.
  Tránh các đơn đặt hàng và xác nhận bằng fax
- ☐ Review your **payment procedures** (segregation of duties and limit amounts), especially in your subsidiaries abroad.
  Xem lại các quy trình thanh toán của Quý khách (phân tách nhiệm vụ và giới hạn số tiền), đặc biệt là trong các công ty con của Quý khách ở nước ngoài
- ☐ Raise also awareness against ***fake technician scams*** (fake bank or software vendor technician contacting to "help" you on your e-banking solution).
  Nâng cao nhận thức chống lại lừa đảo kỹ thuật viên giả (ngân hàng giả hoặc kỹ thuật viên nhà cung cấp phần mềm liên hệ để "giúp đỡ" Quý khách về giải pháp ngân hàng điện tử của Quý khách)
- ☐ To know more about **Fake CEO scam** or **Fake technician** scam, click on the attached documents
  Để biết thêm về lừa đảo CEO giả hoặc lừa đảo kỹ thuật viên giả, hãy nhấp vào tài liệu đính kèm

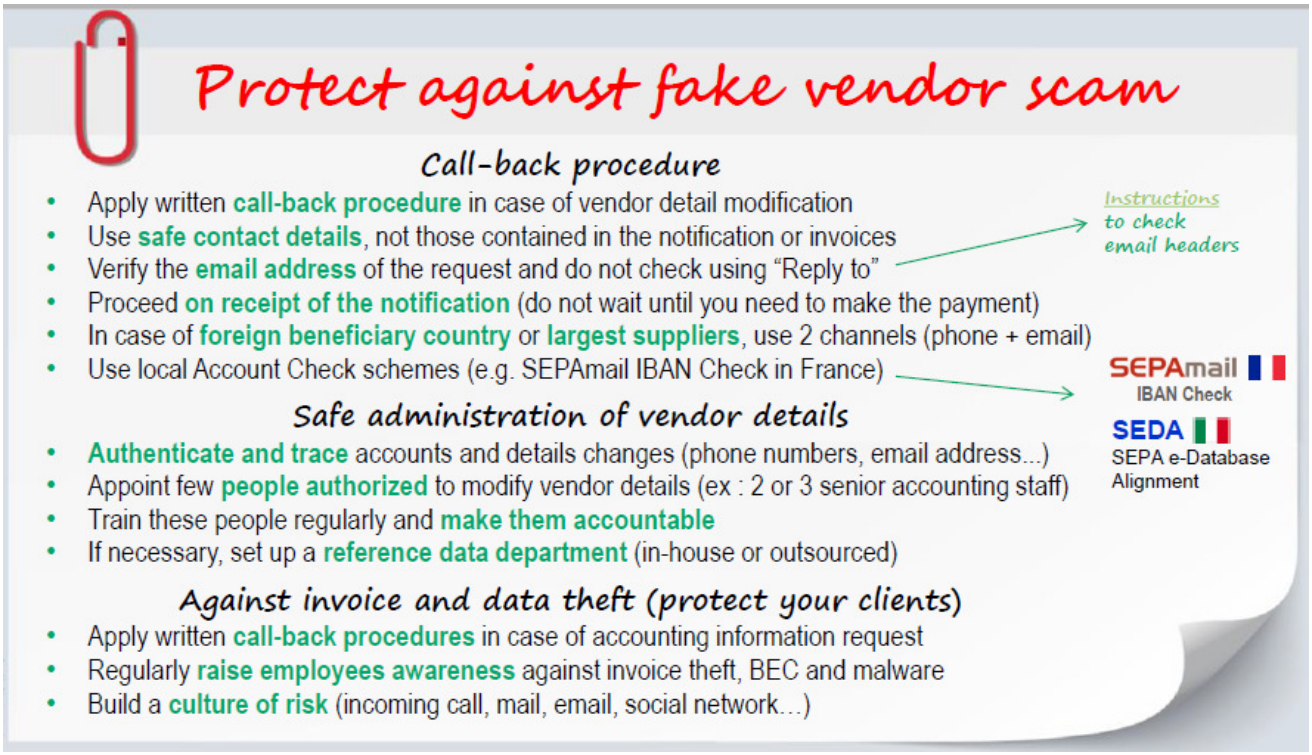
3. We are also currently seeing ***malware frauds*** on Internet tools.
   Chúng tôi hiện cũng đang thấy gian lận phần mềm độc hại trên các công cụ Internet
   Here are some tips/ đây là một số lời khuyên:
   - ☐ When using your Internet or mobile banking application, pay attention to requests for a validation code at an unusual time, unexplained connection failures, or any other **suspicious** behaviour: in such cases, please contact your Relationship Manager.
     Khi sử dụng Internet hoặc ứng dụng ngân hàng di động của Quý khách, hãy chú ý đến các yêu cầu mã xác thực vào thời điểm bất thường, lỗi kết nối không giải thích được hoặc bất kỳ hành vi đáng ngờ nào khác: trong những trường hợp như vậy, vui lòng liên hệ với Giám đốc quan hệ khách hàng phụ trách của Quý khách
   - ☐ Raise awareness against emails containing **attachments or links**, spreading malware. If in doubt, do not open the attachment; do not click on the link and check the origin of the email.
     Nâng cao nhận thức chống lại các email có chứa tệp đính kèm hoặc liên kết, phát tán phần mềm độc hại. Nếu nghi ngờ, không mở tệp đính kèm; không nhấp vào liên kết và kiểm tra nguồn gốc của email
   - ☐ Regularly **update your IT** systems: operating system (eg Windows, Mac OS X), Internet browser, anti-virus, firewall...
     Cập nhật thường xuyên các hệ thống CNTT của Quý khách: hệ điều hành (ví dụ: Windows, Mac OS X), trình duyệt Internet, chống vi-rút, tường lửa

☐ To know more about **malware fraud**, click on the attached document.
Để biết thêm về gian lận phần mềm độc hại, nhấp vào tài liệu đính kèm

You can always **contact** your **Relationship Manager** or your **Cash Management Officer** to make a personalized risk assessment, set up an awareness meeting and implement solutions to secure your flows.
*Quý khách luôn có thể liên hệ với **Giám đốc quan hệ khách hàng phụ trách** hoặc **Cán bộ quản lý tiền mặt** của Quý khách để thực hiện cá nhân hóa đánh giá rủi ro, thiết lập một cuộc họp nhận thức và thực hiện các giải pháp để đảm bảo an toàn luồngthanh toán của Quý khách*

On our website, you will find **training kits** presenting several fraud risks, warning signs and solutions to protect. We greatly recommend that your staffs, in particular in charge of invoices payment, are trained accordingly.
Trên trang web của chúng tôi, Quý khách sẽ tìm thấy các bộ dụng cụ đào tạo trình bày một số rủi ro gian lận, các dấu hiệu cảnh báo và giải pháp để bảo vệ. Chúng tôi đặc biệt khuyên các nhân viên của Quý khách, đặc biệt người phụ trách thanh toán hóa đơn, được đào tạo tương ứng.

We highly suggest as well that you check the **Fraudulent Change of Bank Account Details Awareness (click here)** which is an interactive animated online training prepared by the federation of financial institutions in France (in English and French). It is particularly adapted to the "Fake vendor scams".
Chúng tôi cũng khuyên Quý khách nên kiểm tra Nhận thức về Gian lận Thay đổi Chi tiết Tài khoản Ngân hàng (bấm vào đây), đây là khóa đào tạo hoạt hình trực tuyến tương tác được chuẩn bị bởi liên đoàn các tổ chức tài chính ở Pháp (bằng tiếng Anh và tiếng Pháp). Nó chuyên biệt tương thích với các trò lừa đảo nhà cung cấp.
* In particular/ *Đặc biệt*:



Best regards,
Trân trọng,

Your Relationship Manager/Transaction Banking Officer.
Giám đốc quan hệ khách hàng phụ trách / Cán bộ Ngân hàng giao dịch của Quý khách.