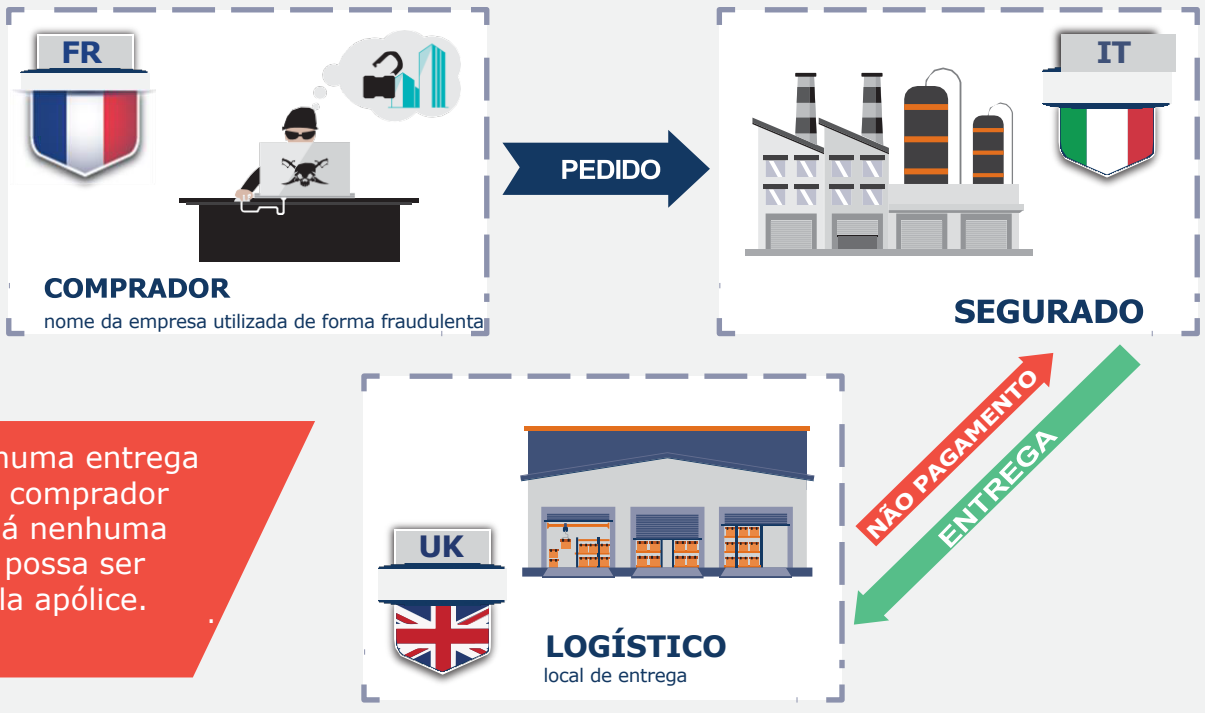
ALERTA DE FRAUDE DE IDENTIDADE CORPORATIVA

A fraude de identidade corporativa é um "negócio em expansão" no mundo do B2B e representa um grande perigo com seu amplo alcance e natureza evolutiva. Isso significa que as empresas precisam tomar medidas proativas para proteger seus ativos e sua identidade contra esta ameaça.

O uso da identidade corporativa representa um sério risco operacional como o fraudador usa a identidade de uma empresa para apoiar várias atividades ilegais. Nas últimas semanas, a Coface foi informada de vários esquemas de roubo de identidade e recomenda uma maior vigilância.

Na prática, os fraudadores utilizam a identidade comercial de uma empresa real, de preferência com um bom histórico de pagamento e reputação, para adquirir bens e serviços de nossos clientes/parceiros.
O recente esquema de fraude que enfrentamos pode ser descrito como no exemplo abaixo:

Fraude de identidade corporativa:



Como nenhuma entrega foi feita ao comprador real, não há nenhuma dívida que possa ser coberta pela apólice.

Como funciona? Os fraudadores são muito bem organizados, criam linhas telefônicas dedicadas e endereços de e-mail, reproduzem formulários de pedidos, compram certificados de incorporação e financiam um registro comercial para tornar-se um comprador de uma empresa.

É por isso que algumas precauções devem ser tomadas ao receber um formulário de pedido, especialmente quando este pedido vem do exterior e de um novo comprador.

Na verdade, um formulário de pedido falso nunca é perfeito. Vale a pena levar alguns minutos para verificá-lo para ver se ele pode ser fraudulento. Quando seu departamento de compras ou vendas recebe um formulário de pedido, é sempre bom de revisá-lo de acordo com a seguinte lista de verificação para evitar qualquer risco de fraude:

- Compare o logotipo do formulário de pedido com aquele no site oficial da empresa, às vezes ele pode ser diferente.
- Compare o formato do endereço de e-mail (nome da pessoa e da empresa) de sua correspondência com os que você pode encontrar no site (muitas vezes no link de navegação "Contato"). Normalmente há apenas um formato para toda a empresa. Quaisquer diferenças devem ser consideradas suspeitas (por exemplo, ana_smith@company.fr vira a.smith@company-service.com ou smith.a@company-group.eu).
- Os fraudadores frequentemente usam nomes de pessoas que realmente trabalham na empresa, mas com domínios ligeiramente diferentes.
- Tome cuidado com os endereços de e-mail genéricos, por exemplo, contabilidad empresa.com.
- Compare o número de telefone fornecido com aqueles disponíveis no site oficial, ou em fontes oficiais.
- Verificar se a empresa tem uma subsidiária ou um projeto no país onde eles solicitam a entrega do pedido.
- Erros de sintaxe ou erros ortográficos podem ser encontrados no formulário de pedido e especialmente nas condições específicas. Portanto, você deve prestar atenção ao documento e estabelecer medidas internas para verificar a validade do documento.
- Pergunte-se se a atividade do comprador é compatível com a sua.
- Confia, mas verifique: em caso de mudanças nos pedidos, endereço de entrega, mudança de dados bancários, etc., sempre ligue para seu comprador para confirmar e certificar-se de que as mudanças são reais.
- Lembrete: os casos de phishing e os pagamentos feitos em contas bancárias falsas ainda são comuns. Portanto, é sempre importante confirmar todos a razão da mudança (endereço, conta bancária) com seu fornecedor.

FAX E E-MAILS NÃO SÃO SEGUROS!

coface
FOR TRADE