Assunto: Proteger os seus sistemas – ciberataques e transações financeiras fraudulentas durante a COVID-19

Caros Colegas,

A escala e a intensidade dos ciberataques e as transações financeiras fraudulentas estão a crescer rapidamente durante a crise atual. Com o crescimento exponencial da atividade online, os criminosos encontram formas mais engenhosas de intercetar informações vitais e de desviar transações financeiras.

Mesmo o mais pequeno desvio do processo de verificação prévia padrão nos processos de pagamento/desembolso poderá conduzir não intencionalmente a uma significativa perda financeira.

Na sequência da nota de orientação sobre partilha de informações e gestão de dados (em inglês - link; tradução em português será disponibilizada em breve) do Fundo Global emitida em abril passado, foi solicitado aos BP que implementassem as necessárias atualizações aos seus processos internos e confirmassem o momento em que esta operação foi acionada.

Como lembrete de boa prática para os BP, os BS e os beneficiários de Financiamento do MCP, as seguintes boas práticas devem ser respeitadas:

- Adote a atitude **"Nunca confie, verifique sempre"** em todas as transações financeiras. Os pedidos mais perigosos são frequentemente os que parecem vir de um endereço ou número de telefone que conhecemos bem. Em alguns casos, os *hackers* utilizam contas genuínas, mas informações que desviam a atenção. Quaisquer pedidos não solicitados que envolvam uma transação financeira devem ser tratados com extrema cautela.
- Certifique-se de que o seu **antivírus** está atualizado com a versão mais recente.
- Consulte os seus bancos relativamente a atualizações para tornar o seu **software de pagamento online** mais seguro.
- Solicite **verificação prévia adicional se a conta bancária** de um fornecedor ou beneficiário diferir da localização do fornecedor ou se se verificar uma mudança no país onde a conta bancária está alojada. Pode solicitar uma carta devidamente assinada do fornecedor ou beneficiário para confirmar a autenticidade da conta bancária.
- Solicite uma confirmação adicional através de uma chamada telefónica.
- Efetue verificações adicionais no sistema de *back-end* para pagamentos efetuados a novas contas bancárias.
- Trabalhe com os seus departamentos de TI no sentido de realizar formação de reciclagem para o pessoal a fim de melhorar o conhecimento destas questões. Em particular, leve os administradores do MCP, o pessoal do Secretariado do MCP e o pessoal do BP a ter formação sobre e-mails de *phishing*.