## Lista de verificação de consciencialização de phishing

#### Mantenha-se alerta e utilize esta lista de verificação para determinar rapidamente se uma mensagem estranha pode constituir um ataque de phishing.

#### 4 formas de identificar um phish

1. **Avalie o cabeçalho**

* Já alguma vez dei o meu endereço eletrónico a esta empresa?
* Tenho uma conta nesta empresa?
* A identidade do remetente corresponde à finalidade da mensagem eletrónica?
* O meu endereço eletrónico está indicado no endereço De: ?
* O endereço Para: dirige-se a destinatários não revelados ou a um grande conjunto de destinatários que não conhece?

1. **Avalie o conteúdo**

* As hiperligações incluídas no corpo da mensagem eletrónica parecem ser válidas?
* A mensagem tem erros ortográficos e gralhas? O texto é correto ao nível da gramática e tem um tom adequado?
* Estão a prometer-me muito dinheiro em troca de pouco ou nenhum esforço?
* Estão a pedir-me que dê dinheiro adiantado como pagamento de atividades questionáveis, uma taxa de processamento ou pagar o custo de acelerar o processo?
* Estão a pedir-me o meu NIB, outras informações financeiras ou palavras-passe? ("Verifique a sua conta." ou "Clique na hiperligação abaixo para obter acesso à sua conta." são frases comuns)

1. **Reflita sobre a finalidade da mensagem eletrónica**

* O assunto é tão urgente como o remetente o descreve?
  + "Se não responder dentro de 48 horas, a sua conta será encerrada."
  + "O não cumprimento desta ação irá desativar automaticamente a sua conta."
* Por que razão o remetente pede confidencialidade? Como posso avaliar se a atividade proposta é legítima e autêntica?

1. **Tenha cautela com os anexos**

* Não abra anexos inesperados.
* Não abra anexos enviados por desconhecidos. Assegure sempre que conhece o remetente.
* Não abra anexos invulgares.
* Não abra anexos que são enviados com mensagens de cariz estranho.