

# CHECKLIST DE ENGENHARIA SOCIAL

Antes de clicar, partilhar um código ou enviar dinheiro, confirme cada ponto.

**Se não conseguir verificar um pedido inesperado, pare e confirme por outro canal.**

## 1 CONFIRME QUEM ESTÁ A PEDIR

- ☐ Reconheço a pessoa ou instituição e confirmei a identidade por um contacto que já conhecia.
- ☐ Se pediram dinheiro por WhatsApp, liguei para o número habitual da pessoa antes de transferir.
- ☐ Não partilhei PIN, palavra-passe ou código recebido por SMS/aplicação, mesmo perante um pedido urgente.
- ☐ Questionei pedidos com pressão, segredo, ameaça de bloqueio ou promessa demasiado boa.

## 2 VERIFIQUE LINKS E PAGAMENTOS

- ☐ Entrei na aplicação ou no site oficial directamente, sem usar o link de uma mensagem inesperada.
- ☐ Confirmei o destinatário, o número e o valor antes de autorizar qualquer pagamento.
- ☐ Se um fornecedor mudou a conta bancária, confirmei a alteração por um contacto anterior e obtive segunda aprovação.

## 3 PROTEJA AS SUAS CONTAS

- ☐ Activei a autenticação multifactor e só aprovo acessos ou códigos que eu próprio iniciei.
- ☐ Mantenho aplicações actualizadas e acompanho os alertas e movimentos das contas.
- ☐ Se o pedido envolve a empresa, conheço a pessoa ou equipa a quem devo comunicar a suspeita.

### SE JÁ RESPONDEU OU ENVIOU DINHEIRO

- 1 Contacte imediatamente o banco ou a operadora pelos canais oficiais.
- 2 Altere as palavras-passe afectadas e termine sessões abertas.
- 3 Guarde mensagens, números, horários e comprovativos; avise contactos afectados.
- 4 Denuncie a tentativa ou a fraude às entidades competentes.