

# E-MAILS DE PHISHING

O phishing usa e-mails fraudulentos para enganar o destinatário de modo a que este partilhe dados pessoais, financeiros ou códigos de segurança.

## COMO FUNCIONA?

Estes e-mails:

podem **parecer** idênticos ao tipo de correspondência enviada pelos bancos.

**copiam** logótipos, estilo visual e mensagens de e-mails reais.



**pedem** para descarregar um anexo ao e-mail ou clicar num link.

**usam** linguagem para transmitir urgência.

## O QUE PODE FAZER?

- > **Mantenha o seu software atualizado**, incluindo browser, antivírus e sistema operativo.
- > Esteja **especialmente atento** se um suposto e-mail do banco lhe pedir dados sensíveis (ex: os códigos de acesso ao homebanking).
- > **Examine o e-mail com cuidado**: compare o endereço com o de mensagens anteriores do banco. Veja se encontra erros de escrita.
- > **Não responda a e-mails suspeitos**. Encaminhe-os para o seu banco escrevendo o endereço manualmente.
- > **Não clique nos links nem descarregue ou abra os anexos**. Escreva manualmente o endereço do seu banco no browser.
- > Em caso de dúvida, **verifique a autenticidade** no site do banco ou por telefone.



Os atacantes confiam que as pessoas não estão atentas; numa vista rápida, estes e-mails falsos parecem verdadeiros.



Atenção quando usa o seu telemóvel. Pode ser mais difícil detetar uma tentativa de ataque no telemóvel ou no tablet.

#CyberScams

