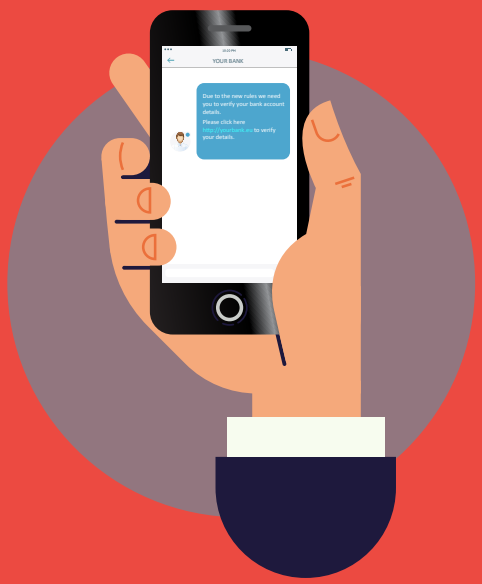
SMSs DE PHISHING

O “smishing” (combinação das palavras SMS e Phishing) é a tentativa por atacantes de obter dados pessoais, financeiros ou de segurança por mensagem de texto.



COMO FUNCIONA?

A mensagem de texto tipicamente pedirá para clicar num link ou ligar para um número de modo a "verificar", “atualizar", ou "reativar" a sua conta. Mas... o link leva a uma página falsa e o número de telefone liga ao atacante, que finge ser a empresa verdadeira.

O QUE PODE FAZER?

- **Não carregue em links, anexos ou imagens** que receba em mensagens de texto não solicitadas, sem verificar quem as mandou.
- **Não deixe que o apressem**. Verifique calmamente tudo o que precisa antes de responder.
- **Nunca responda a mensagens de texto** que lhe peçam o PIN, passwords de acesso ao banco ou outros códigos de segurança.
- Se acha que respondeu a uma mensagem de smishing, indicando dados bancários, **contacte o seu banco imediatamente**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams