PSP alerta para nova burla informática chamada “spoofing”

written by O Cidadão | 15 de Agosto, 2024

Em comunicado, a Direção Nacional da PSP avança com diversos conselhos de segurança e pede que se denunciem todas as burlas, incluindo meras tentativas.

“Proteja-se dos criminosos que se protegem atrás de um ecrã”, sublinha a PSP.

O ‘spoofing’ consiste na falsificação de uma entidade como ‘email’, número de telefone, ‘site’, endereço IP, entre outros, para dar uma aparência de legitimidade e de confiança naquele contacto, tendo em vista iludir a vítima.

Segundo a PSP, os casos registados “mais recorrentes” reportam-se a ‘spoofing’ de ‘email’ e de chamadas e SMS

(mensagens).

"O cibercriminoso, com recurso a sistemas informáticos, reproduz endereços de 'email' e números telefónicos, fazendo-se passar por entidades bancárias, empresas amplamente conhecidas ou instituições públicas, com o objetivo de obter os dados pessoais da vítima ou credenciais para fins criminosos", descreve a Direção Nacional na nota divulgada hoje.

A PSP alerta que "***estas situações podem acontecer a qualquer pessoa"***, razão pela qual frisa: ***"A prevenção é o melhor método de segurança".***

A polícia aconselha a duvidar de qualquer chamada telefónica ou SMS que contenha uma saudação genérica em vez do nome real do recetor ou de uma mensagem personalizada dirigida ao recetor.

No caso das mensagens ou telefonemas por parte de alegadas entidades bancárias, onde sejam solicitados códigos, credenciais ou palavras passe, deve ser verificada a veracidade do pedido junto da entidade bancária em questão.

Já perante 'emails' ou SMS que contenham 'links' duvidosos, devem os mesmos ser ignorados e as mensagens de imediato eliminadas.

É ainda recomendado que não se coloque o contacto telefónico nas redes sociais e que se bloqueie manualmente números provenientes de chamadas indesejadas e duvidosas.

É considerado importante ***"respeitar o alerta sobre chamadas ou SMS marcadas como 'spam' [lixo] nos aparelhos telefónicos mais recentes".***

E, ao receber um 'email' ou outra qualquer comunicação que evidencie a prática de 'spoofing', deve ser informado o suposto remetente sobre o sucedido, no sentido de ajudar a

impedir novos ciberataques deste tipo.

“***Podem fazê-lo nos sites das empresas visadas que, normalmente, possuem páginas onde é possível relatar ‘spoofing’ e outros problemas de segurança***”, conclui a PSP.