Cerejeira Namora, Marinho Falcão

Phishings, Smishings, Pharmings e Spoofing

Estrangeirismos para o Crime Moderno

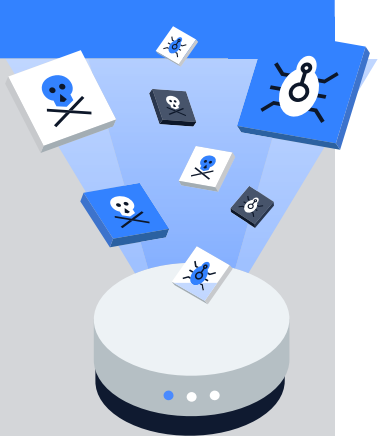
Nos últimos meses temos assistido a uma crescente divulgação de notícias sobre o aumento de fraudes bancárias e das técnicas que lhe estão associadas. É, por exemplo, o caso do hacker que, em Espanha, vendia kits de *phishing* prontos a utilizar por quem pretendesse começar a sua actividade criminosa e que gerou prejuízos ainda por calcular, mas sempre na ordem dos muitos milhões de euros ou a descoberta da Microsoft que impediu uma campanha de *phishing* cujo código terá sido criado com recurso à IA. Por cá, fomos avisados no mês passado da utilização ilícita da imagem e nome do Cartão Continente como veículo para mais uma campanha de *phishing*.

A página da internet do Gabinete do Cibercrime do Ministério Público, da Polícia Judiciária e o sítio do Banco de Portugal estão lotados de alertas, avisos e documentos com a descrição dos esquemas. Mas, por mais avisos que se façam, os clientes continuam a ser enganados pois os golpes são cada vez mais sofisticados e perfeitos: **é difícil distinguir o que é real do que é criminoso.**

Segundo dados divulgados recentemente pela imprensa, só nos últimos dois anos a PJ abriu

+ de 2000 inquéritos

por situações de *phishing* e esquemas semelhantes.

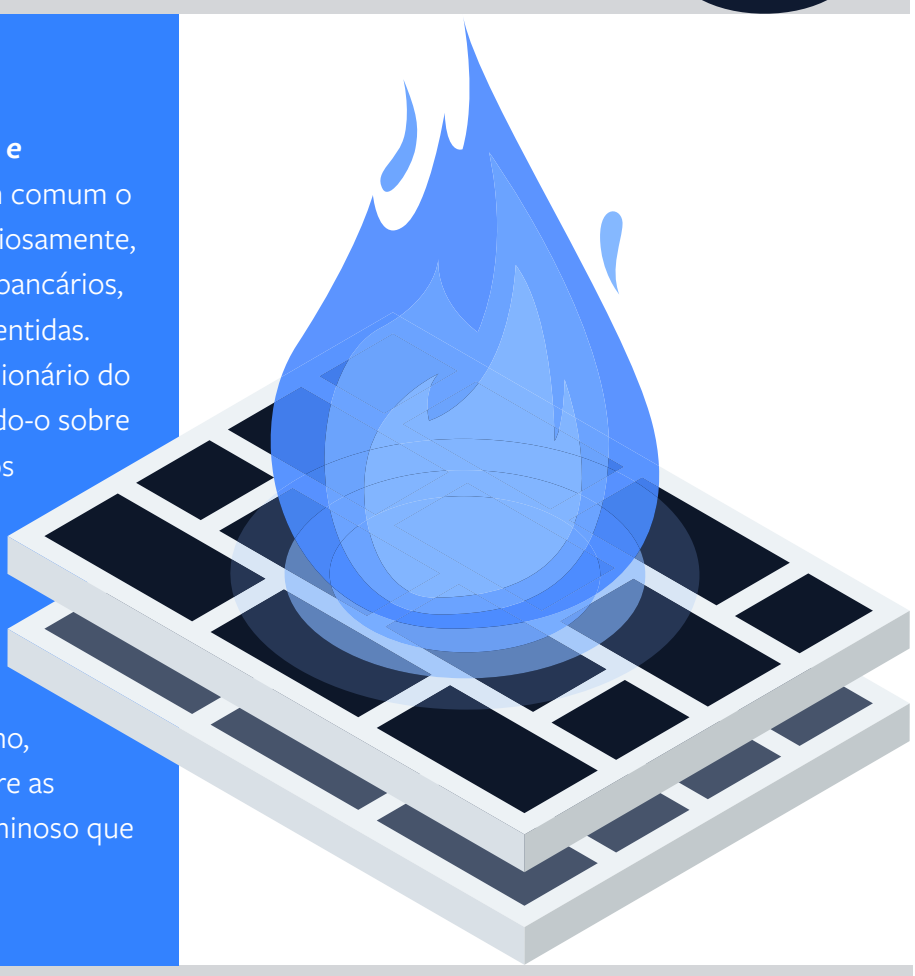


O que é o Phishing, o Smishing, o Pharming e o Spoofing?

O ***phishing*** tem por base um email ou link falso, o ***smishing*** resulta de um sms falso, o ***pharming*** redirecciona o utilizador para um site falso que não pertence ao Banco e, finalmente, no ***spoofing*** o cibercriminoso disfarça-se de uma entidade fidedigna para se apropriar dos dados confidenciais do utilizador.

Como atuam?

Entre ***phishings, smishings, pharmings e spoofings,*** todos estes métodos têm em comum o contacto de um interolocutor que, maliciosamente, tenta apropriar-se dos dados pessoais e bancários, com vista a realizar transações não consentidas.
É o exemplo paradigmático do falso funcionário do Banco que contacta o cliente e, alarmando-o sobre presença de movimentos não autorizados na sua conta, pede-lhe que forneça os códigos que irá receber para poder "cancelar" as operações.
Ou as hipóteses mais sofisticadas em que o utilizador procura aceder à sua conta *homebanking*, mas, sem saber como, acaba num site fraudulento, no qual insere as suas credenciais e dá acesso ao cibercriminoso que aguarda escondido por detrás do site.



O que nos diz a lei?

O nosso regime dos serviços de iniciação de pagamento (Decreto-Lei n.º 91/2018) não ignora o nível de sofisticação tecnológica que as formas de fraude bancária podem assumir, as quais muitas vezes ultrapassam as precauções do utilizador mais cauteloso.

Comunicado pontualmente o extravio, **a Lei estabelece do lado do Banco o dever de reembolso imediato do montante.** Portanto, antes de se entrar na discussão sobre quem é o responsável pelo extravio, deve o utilizador ser provisoriamente ressarcido, evitando-se a agravação da sua situação patrimonial.

A inobservância deste dever (ainda que seja frequente na prática bancária) **é punida como contraordenação muito grave.**

Com a comunicação, o Banco não só solicitará a participação criminal do extravio, como irá avançar com o seu processo averiguação interno.

Ora, frequentemente, os Bancos concluem pela inexistência de qualquer falha técnica no seu sistema, imputando a responsabilidade pela fraude ao utilizador. A realidade tem demonstrado que as fraudes bancárias costumam quase sempre ter origem na esfera de atuação do utilizador, e não no sistema de serviços de pagamento do Banco. Mas não é por isso que a legislação e a prática judiciária têm isentado os Bancos de qualquer responsabilidade.

Com efeito, não basta demonstrar a ausência de avaria técnica, mas também que o utilizador agiu com negligência grosseira.

Não sendo suficiente o mero desleixo, desconhecimento ou até ingenuidade, o recentíssimo Acórdão do Supremo Tribunal de Justiça de 17 de Junho de 2025 espelhou aquilo que tem vindo a ser prática judiciária dos últimos anos, ao estabelecer **que a apropriação por terceiro dos dados bancários não significa, por si só, que o utilizador agiu com negligência grosseira.**

No caso concreto, os Conselheiros concluíram que, atendendo aos elevados níveis de competência técnica que as instituições bancárias devem assegurar, **a monitorização dos movimentos permitia ao Banco detetar a presença de uma operação não consentida, porquanto aqueles destoavam do padrão normal do cliente.** Estando em causa uma atuação devida pelo Banco ao abrigo do princípio da boa-fé, esta decisão reforça a necessidade de as instituições bancárias adotarem mecanismos que permitam evitar a operação não consentida, logo que tomem conhecimento da mesma.