ALERTA CIBERCRIME

15 de junho de 2026

'Phishing' e burla por falsos agentes bancários

1. Estão em curso campanhas levadas a cabo por diferentes grupos criminosos pelas quais, por meio de técnicas combinadas de ***phishing*** e de **engenharia social**, os agentes criminosos procuram obter de forma ilícita dados de acesso a contas bancárias, para depois acederem às mesmas e, a partir delas, transferirem valores para outras contas, por eles controladas.
Não se trata de meras campanhas de *phishing* com o propósito da obtenção de dados bancários, mas antes de uma iniciativa criminosa muito mais complexa, que provoca de imediato prejuízos patrimoniais muito avultados às vítimas.
Estas campanhas têm visado clientes de diversos bancos.

2. Como sempre ocorre nos casos de *phishing*, este método criminoso começa com a expedição, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas – no caso destas campanhas criminosas, foram identificados casos de mensagens telefónicas (SMS), mas também de mensagens de correio eletrónico (email).

3. Em tais mensagens menciona-se que as mesmas são provenientes de instituições bancárias, alertando-se o destinatário para uma recente transferência ou outro pagamento bancário que terá sido efetuado a partir da sua conta. Cria-se, portanto a ideia de que poderá ter havido um acesso ilegítimo à conta. Porém, as mensagens oferecem uma solução, que passa pelo acesso a um *link* ao qual o destinatário deve aceder.

A mensagem insta ainda ao acesso "*imediatamente*", incutindo urgência e ação irrefletida da vítima.

4. O teor destas mensagens é enganoso e fraudulento. As mensagens não foram remetidas pelas instituições bancárias nem a partir de servidores daquelas entidades ou por elas geridos. Com elas, os agentes criminosos pretendem incutir nos destinatários a convicção de que as mensagens são legítimas e autênticas, tendo sido emitidas pelas instituições bancárias pelas quais pretendem fazer-se passar.

5. Se a vítima premir o *link* agregado à mensagem que recebeu, acede a uma página fraudulenta, que imita a página *oficial* da sua instituição bancária, mas não corresponde à autêntica página *web* daquela entidade.
Nela, é solicitado à vítima que introduza diversos dados pessoais e, designadamente, os dados de identificação e de acesso à sua conta bancária. Além disso, é sempre solicitado o telefone da vítima.
O número de telefone é um elemento crucial neste processo, já que vai permitir aos agentes criminosos desenrolar uma segunda parte do mesmo.

6. Com efeito, munidos dos dados de acesso, os agentes criminosos conseguem efetivamente aceder à conta bancária da vítima, verificar os respetivos movimentos e ficar a saber qual é o montante em saldo. Porém, em geral, apenas com esses dados não é possível aos agentes criminosos proceder a movimentos ou a transferências para outras contas, porque a generalidade dos bancos portugueses adotou já um procedimento a que se tem chamado *segundo fator de autenticação*.

7. Para contornar esta exigência, os agentes criminosos procedem a chamadas telefónicas às vítimas. Identificam-se como sendo funcionários da área da cibersegurança da instituição bancária. Durante a conversação, para dar credibilidade à sua abordagem demonstram conhecer detalhes sobre a vítima e a sua conta (os quais obtiveram no acesso que fizeram à conta). Depois, informam a vítima de que foi identificado um movimento suspeito, de grande valor, a partir da conta bancária em causa. Perguntam-lhe se foi a vítima quem deu a respetiva ordem.

8. Como se trata de um movimento "inventado" pelo agente criminoso, claro que a vítima nega ter sido da sua responsabilidade – naturalmente, esta abordagem provoca na vítima o receio de perder o valor em causa. O agente criminoso oferece-se então para reverter tal movimento, desde que a vítima o confirme. Esta confirmação terá que ser feita por via do *segundo fator de autenticação*. Isto é, para supostamente "anular" o movimento suspeito, a vítima tem que acionar o seu *segundo fator de autenticação* (que, consoante as instituições bancárias, pode por exemplo ser um código recebido por SMS ou uma confirmação numa aplicação telefónica).

9. Todo este procedimento dos agentes criminosos é uma encenação fraudulenta: os mesmos não têm qualquer função nas instituições bancárias e o suposto movimento "suspeito" não existe. Na verdade, o seu único propósito é convencer a vítima a facultar-lhes o *segundo fator de autenticação*, para assim conseguirem transferir valores, da conta bancária da vítima para uma outra, por eles controlada.
Para o efeito, enquanto falam com a vítima, procedem a uma ordem de transferência. Como o sistema bancário requere o *segundo fator de autenticação*, o mesmo é automatizadamente espoletado pelo

sistema – por exemplo, sendo remetido à vítima (dona da conta) um código por via de uma mensagem SMS. Nesse momento, os agentes criminosos advertem a vítima de que vão proceder à "anulação" do tal movimento "suspeito" mas que, para efeitos de confirmação da operação, a vítima vai receber um código, que deverá facultar-lhe.
Se assim proceder, facultando aos agentes criminosos o código, a vítima permite-lhes que *autentiquem* a transferência no sistema bancário e, por conseguinte, que os mesmos se apoderem da quantia em causa.

10. Mensagens como as que acima se descreveram devem ser ignoradas e apagadas, sem resposta. Chamadas telefónicas desta natureza devem também ser ignoradas. Caso a vítima acabe por facultar aos agentes criminosos dados pessoais ou da sua conta bancário, importará, como primeira diligência a empreender, contactar o banco por via dos canais institucionais habituais.