MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

20 de abril de 2026

'*Phishing*' – falsos reembolsos da TAP

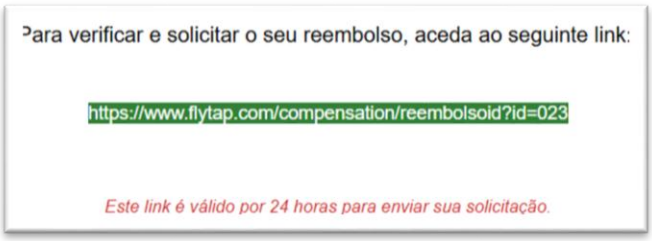
1. Está em curso uma campanha criminosa pela qual, por meio de técnicas combinadas de ***phishing*** e de **engenharia social**, os agentes criminosos procuram obter de forma ilícita dados de cartões bancários de pagamento, para depois com eles efetuarem pagamentos de compras *online*.
Não se trata de uma mera campanha de *phishing* com o propósito da obtenção de dados de cartões bancários, mas antes de uma iniciativa criminosa mais complexa, que provoca de imediato prejuízos patrimoniais às vítimas.

2. Como na generalidade dos casos de *phishing*, este método criminoso começa com a expedição, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas – no caso desta campanha criminosa, mensagens de correio eletrónico.

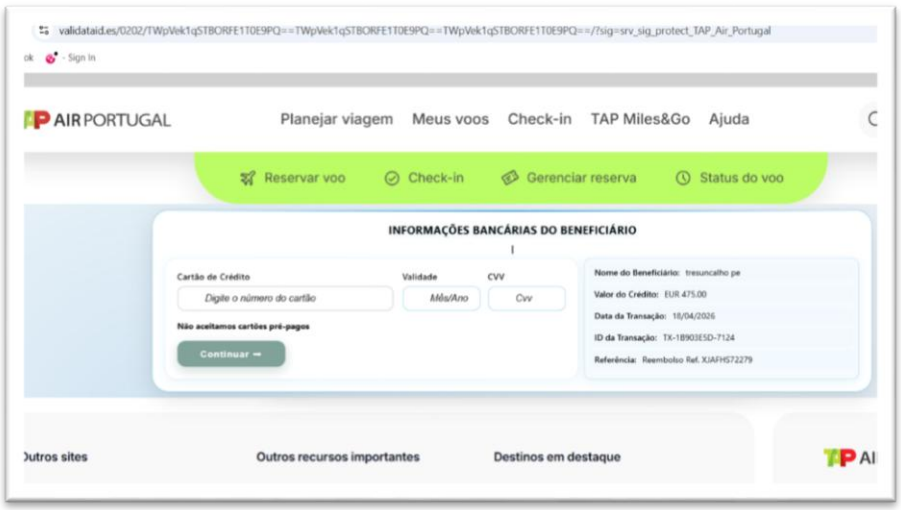
3. Em tais mensagens menciona-se que o remetente é a "*TAP Air Portugal*". Além disso, o respetivo texto pretende convencer o destinatário de que aquela companhia pretende transferir-lhe um valor: referem que "*detetámos que o seu último voo, a partir do Aeroporto de Lisboa, sofreu um atraso significativo*". Adiantam ainda que, por esse motivo, o destinatário da mensagem (a vítima) "*tem direito a compensação financeira*". A mensagem ainda inclui um *link* para uma página *web*, que a vítima deve aceder "*para verificar e solicitar o reembolso*".

4. O teor destas mensagens é enganoso e fraudulento, pretendendo fazer crer os respetivos destinatários de que tais mensagens têm origem na "*TAP Air Portugal*". Além disso, pretendem gerar nas vítimas a expetativa de que vão receber uma quantia monetária. Por último, ainda apelam à urgência na reação, por incluírem a advertência, em realce, de que o "*link é válido por 24 horas*".
Ou seja, os agentes criminosos pretendem incutir nos destinatários a convicção de que as mensagens são legítimas e autênticas, tendo sido emitidas pela "*TAP Air Portugal*". Porém, isso não corresponde à verdade: estas mensagens não foram remetidas pela "*TAP Air Portugal*" nem a partir de servidores daquela entidade ou por ela geridos.

5. Quanto ao *link* indicado nas mensagens, inclui segmentos e palavras que aparentemente apontam para a legítima página *web* da "*TAP Air Portugal*". Porém, ao premir aquele *link*, a vítima acede a uma página fraudulenta, que imita a página *oficial* da "*TAP Air Portugal*", mas não corresponde à autêntica página *web* daquela entidade.



6. Nesta página, é solicitado à vítima que insira os seus dados pessoais de identificação (nome, número de telefone e endereço). Depois, é-lhe solicitado que introduza os dados do seu cartão de pagamento bancário, neles se incluindo o código de verificação de segurança (comummente referenciado como CVV).



Caso a vítima insira os dados do cartão bancário naquela página fraudulenta, está a facultar aos agentes criminosos informação que permite aos mesmos a realização de compras *online*.

7. Aliás, na posse dos dados dos cartões das vítimas, de imediato os agentes criminosos efetuam compras. Para autenticar as mesmas, normalmente, o sistema de segurança do cartão bancário emite uma mensagem SMS para o telefone da vítima (ou espoleta um outro mecanismo do chamado *segundo fator de autenticação*).

Para ir ao encontro desta exigência de segurança do sistema, a página fraudulenta gerida pelos agentes criminosos solicita então à vítima que seja introduzido o código remetido por via dessa mensagem SMS (ou que proceda conforme o sistema bancário solicitar, acionando o *segundo fator de autenticação*). Caso a vítima o faça, permite aos agentes criminosos *autenticar* a transação, tornando efetivo o pagamento *online*.

8. O propósito dos agentes criminosos é o de, utilizando os dados dos cartões bancários das vítimas, proceder ao pagamento de compras *online* por si efetuadas, assim beneficiando economicamente.

Mensagens de correio eletrónico como as que descreveram devem ser ignoradas e apagadas, sem resposta.

Caso a vítima acabe por facultar aos agentes criminosos os seus dados pessoais e os do seu cartão bancário, importará, como primeira diligência a empreender, contactar o banco ou outra entidade emissora do cartão.