



## ALERTA CIBERCRIME

6 de abril de 2026

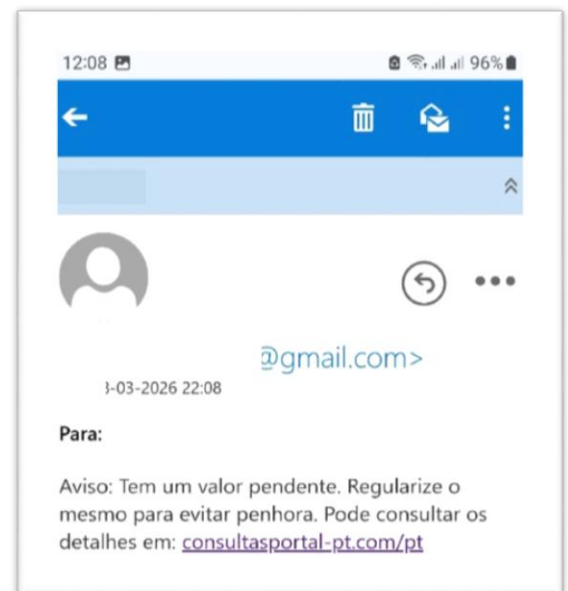
***Burla – Falsas Dívidas à Autoridade Tributária***

1. Está em curso mais uma campanha de **burlas por via das redes de comunicações**, que passa pela expedição massiva de mensagens por via de *WhatsApp*, ou correio eletrónico, para destinatários indiscriminados. Em tais mensagens é referido que o destinatário tem uma **dívida fiscal à AT (Autoridade Tributária)**, razão pela qual esta vem reclamar o respetivo pagamento. Os primeiros sinais desta campanha criminosa surgiram nas últimas semanas de março de 2026.

2. Trata-se de uma campanha criminosa por via da qual, arditosamente, os agentes criminosos pretendem convencer as vítimas de que têm uma dívida à Autoridade Tributária, a qual está pendente de pagamento. No passado, foram identificadas campanhas da mesma natureza, reclamando o pagamento de falsas dívidas à EDP, à Segurança Social, ao SNS e à própria Autoridade Tributária também.

3. O método criminoso consiste na remessa de mensagens escritas, por telefone ou por via de correio eletrónico, para as potenciais vítimas. Tais mensagens são remetidas de forma indiscriminada e massiva, para inúmeros destinatários. Para o efeito são usados cartões telefónicos de redes nacionais, frequentemente com o número chamador oculto, ou cartões telefónicos pré-pagos.

4. De tais mensagens consta uma suposta notificação, efetuada pela Autoridade Tributária, vagamente advertindo da existência de uma dívida, a qual deverá ser paga. Encaminham ainda a vítima para um *link*, onde a mesma "*pode consultar os detalhes*". O texto sublinha ainda que tal pagamento é necessário "*para evitar penhora*". Com esta formulação, pretendem os agentes criminosos levar à reação urgente a esta mensagem, precipitando o pagamento impulsivo e pouco refletido de um valor.





5. Estas mensagens não são remetidas pela Autoridade Tributária, nem por qualquer outra entidade por ela autorizada a fazê-lo, embora induzam ter origem naquela entidade pública. Esta alegada proveniência é falsa e tem como único propósito convencer vítimas a efetuarem pagamentos indevidos a terceiros – de cujos montantes estes últimos se apoderarão indevidamente.

6. Em campanhas criminosas anteriormente identificadas, os agentes criminosos incluíram, desde logo na própria mensagem, dados para permitiam proceder ao pagamento, por via do sistema bancário, em caixas ATM (Multibanco) ou por via de *homebanking*. Porém, a presente campanha é mais sofisticada e agressiva: a mensagem incluiu um *link*, o qual, uma vez acedido, abre uma página na Internet que simula ser a do Portal das Finanças. Esta página *web* utiliza uma imagem gráfica semelhante à do Portal das Finanças e inclui logotipos da Autoridade Tributária.

Uma vez acedida esta página fraudulenta, num primeiro momento, é solicitado à vítima que ali introduza o seu Número de Contribuinte e o seu código pessoal de acesso. Inseridos estes, é exibida uma



outra página, da qual consta existir uma dívida, sendo indicado o respetivo valor e a forma de pagamento (dados para pagamento em caixas ATM ou por via de *homebanking*). Além disso, é referido, de forma destacada, que o pagamento "*Expira hoje*", sendo providenciado um botão com a menção "*PAGAR AGORA*" e também graficamente salientado "*EVITE APREENSÃO*" e que "*o montante deverá ser pago, podendo resultar em processo de execução fiscal e penhora de bens*".

7. Estas páginas (onde as vítimas introduzem as suas informações de acesso ao Portal das Finanças e onde se visualizam os dados para pagamento) não são geridas pela Autoridade Tributária nem por qualquer entidade por ela autorizada a fazê-lo. São páginas *falsas*, que pretende imitar o autêntico Portal das Finanças e convencer as vítimas de que assim é.

Foi em concreto identificada uma destas páginas falsas registada num endereço pertencente ao Registrar *Porkbun LLC* (<https://porkbun.com/>), um servidor que providencia alojamento de conteúdos *em nuvem*, com sede em Sherwood, Oregon, Estados Unidos da América, mas gerido pelo Registrant *Private by Design, LLC* (<https://private.design/>), com sede em Sanford, Carolina do Norte,





**MINISTÉRIO PÚBLICO**  
**PORTUGAL**

PROCURADORIA-GERAL DA REPÚBLICA  
GABINETE CIBERCRIME

Estados Unidos da América. Este último é um fornecedor de serviço especializado em garantir privacidade aos seus clientes: faculta aos mesmos a navegação na Internet mantendo ocultos e confidenciais os respetivos nomes, número de telefone e endereço, entre outros dados pessoais.

**8.** Os dados bancários para pagamento da suposta dívida são solicitados pelos agentes criminosos a entidades financeiras que prestam tais serviços na União Europeia.

**9.** O propósito dos autores destes factos criminosos é enganar vítimas menos atentas, convencendo-as a efetuar pagamentos que não são devidos. É recomendável que se avaliem cautelosamente as mensagens eletrónicas desta natureza que sejam recebidas. Não deve responder-se às mesmas ou aceder aos *links* nelas incluídos, devendo antes tais mensagens ser comunicadas ao Ministério Público ou aos órgãos de polícia criminal. Para lá disso, mensagens deste tipo devem ser ignoradas, sem se lhe dar qualquer sequência.