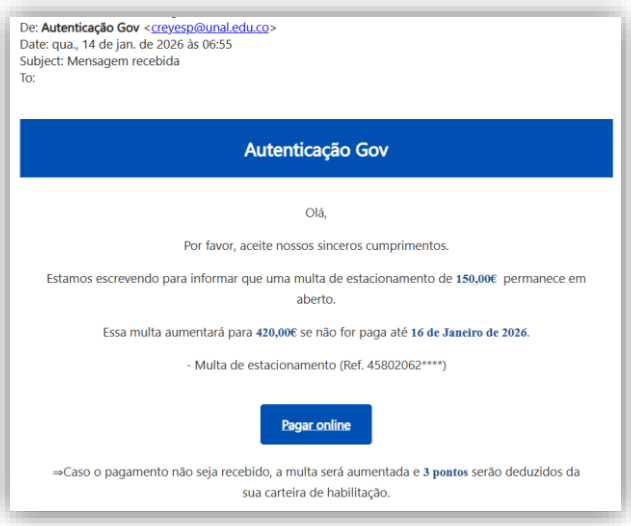
MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

20 de janeiro de 2026

'Phishing' abusando da plataforma *autenticação.gov*

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 muito mais complexa e agressiva, que provoca de imediato grandes prejuízos patrimoniais às vítimas.


De: **Autenticação Gov** <creyesp@unal.edu.co>
Date: qua., 14 de jan. de 2026 às 06:55
Subject: Mensagem recebida
To:

Autenticação Gov

Olá,

Por favor, aceite nossos sinceros cumprimentos.

Estamos escrevendo para informar que uma multa de estacionamento de **150,00€** permanece em aberto.

Essa multa aumentará para **420,00€** se não for paga até **16 de Janeiro de 2026**.

- Multa de estacionamento (Ref. 45802062****)

Pagar online

⇒Caso o pagamento não seja recebido, a multa será aumentada e **3 pontos** serão deduzidos da sua carteira de habilitação.

2. Como na generalidade dos casos de *phishing*, este método criminoso passa pela expedição, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas – neste caso, mensagens de correio eletrónico.

3. Em tais mensagens pretende fazer-se convencer o destinatário que o remetente é "*Autenticação Gov*", a plataforma de identificação, autenticação e assinatura digital do Estado Português. Aliás, das mesmas consta o logotipo da plataforma "*Autenticação Gov*". Além disso, o respetivo texto pretende convencer o destinatário de que é devedor de uma quantia (multa de estacionamento): "*Estamos escrevendo para informar que uma multa de estacionamento de 150,00€ permanece em aberto. Essa multa aumentará para 420,00€ se não for paga até* [são indicados dias imediatamente a seguir aos da mensagem]". Ainda é feita a advertência seguinte: "*Caso o pagamento não seja recebido, a multa será aumentada e 3 pontos serão deduzidos da sua carteira de habilitação*".
Nas mensagens vem incluído um botão com a menção "*Pagar* online".

4. O teor destas mensagens é enganoso e fraudulento, pretendendo fazer crer os destinatários que tais mensagens têm origem no domínio "*autenticacao.gov*". Além disso, pretendem alarmar o destinatário, apelando à urgência do pagamento da suposta quantia em dúvida, sob pena de, não o fazendo, a mesma se agravar.
Estas mensagens pretendem convencer os destinatários de que são mensagens legítimas e autênticas da Agência para a Modernização Administrativa (AMA), entidade que gere a plataforma

"*autenticacao.gov*". Porém, isso não corresponde à verdade: estas mensagens não são remetidas pela AMA nem a partir de servidores desta entidade pública.

5. Quanto ao botão com a menção "*Pagar* online", corresponde a um *link* que supostamente encaminha para a página oficial da AMA e de autenticação da Chave Móvel Digital. Porém, ao premir aquele botão, a vítima acede a uma página fraudulenta, que imita a página oficial da AMA. Nesta página, é-lhe solicitado que insira o seu número de telefone. Depois, ainda lhe é solicitado que introduza os seus dados pessoais e, de seguida, os dados do seu cartão de pagamento bancário, neles se incluindo o código de verificação de segurança (normalmente referenciado como CVS).

6. Caso a vítima insira os dados do cartão bancário naquela página fraudulenta, está a facultar aos agentes criminosos a 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 (o 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.
Caso a vítima o faça, faculta aos agentes criminosos a informação que lhes permite 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.