

Question for written answer E-000626/2026
to the Commission
Rule 144
Yannis Maniatis (S&D)

Subject: Malicious SMS messages sent to the mobile phones of European citizens

Attempts to obtain personal and sensitive financial data of European citizens via mobile phone messages (SMS) originating from outside the EU (phishing, smishing techniques) have recently intensified. In Greece, citizens are receiving a surge of fake messages from abroad, some even going so far as to impersonate the Authority for Public Revenue¹. The resulting risk is disproportionately high for citizens with limited digital literacy and older people, and clearly cannot be addressed through announcements and appeals to citizens in favour of cybersecurity, as was recently the case in Greece.

Can the Commission answer the following:

1. How has it guaranteed the implementation of the obligations of the Member States, and in particular Greece, in the framework of their national cybersecurity strategies, to adopt policies to promote active cyber protection (Directive (EU) 2022/2555) and to ensure that telecommunication providers take measures to ensure the security of telecommunication services (Directive (EU) 2018/1972)?
2. Is the Commission considering adopting measures aimed at tackling the root of the problem, such as, for example, the imposition of a fee on SMS messages sent from abroad by unregistered users or the mandatory European certification of sender ID and anti-spoofing measures for SMS messages sent into the EU (i.e. an obligation for providers not to deliver SMS messages indicating a European brand but originating from outside the EU or following an unauthorised digital path)?

Submitted: 12.2.2026

¹ Official communication: <https://www.aade.gr/deltia-typoy-anakoinoseis/deltio-typoy-02022026>