SECRETARIATUL GENERAL AL GUVERNULUI
DEPARTAMENTUL PENTRU RELAȚIA CU PARLAMENTUL
B-dul Primăverii nr. 22, sector 1, București, Tel: 0213143400 int.5000, E-mail: drparlament@gov.ro

Nr. 5971, 5972, 5973, 5975, 5976, 5955,6035, 6036, 6037, 6038, 6060, 6061, 6062, 6063, 6046, 6047, 6033, 6034, 6059/2026

PARLAMENTUL ROMANIEI
CAMERA DEPUTAȚILOR
SECRETAR ***
Intrare/Ieșire Nr. 66-3/238
2026 Luna 05 Ziua 25

21-05-2026

Către: Doamna Deputat Oana MURARIU
Secretar al Camerei Deputaților

Ref.la:Răspunsuri la întrebări/interpelari formulate de deputați

Stimată doamnă secretar,

Vă transmitem, alăturat, răspunsurile instituțiilor vizate cu privire la unele întrebări/interpelări formulate de deputați, potrivit tabelului anexat.

Cu deosebită considerație,

NINI SAPTINARU

SECRETAR DE STAT

Nr. 5975 / DRP
DATA 19 -05- 2026

SECRETARIATUL GENERAL AL GUVERNULUI
DEPARTAMENTUL PENTRU RELAȚIA CU PARLAMENTUL
B-dul Primăverii nr. 22, sector 1, București, Tel: 0213143400 int.3000, Email: drparlament@gov.ro

Către: Domnul deputat Adrian Felician COZMA,
Parlamentul României - Camera Deputaților

Ref.la: întrebarea dvs. înregistrată la Camera Deputaților cu nr.4925A/2026

Stimate domnule deputat,

Referitor la întrebarea dumneavoastră adresată Prim-ministrului, înregistrată la Camera Deputaților cu nr.4925A/2026, având ca temă *„Solicitare de informații cu privire la agresiuni cibernetice derulate pe teritoriul României prin utilizarea rețelelor sociale și ale cartelelor preplătite fără identitate”,* vă comunicăm faptul că Departamentul pentru Relația cu Parlamentul a asigurat informarea Prim-ministrului cu privire la această întrebare și a făcut consultarea interinstituțională potrivit obiectului acesteia.

Astfel, vă transmitem informațiile comunicate de Directoratul Național de Securitate Cibernetică, prin adresa nr.T36/2026.

Folosesc acest prilej, domnule deputat, pentru a vă asigura de întreaga mea disponibilitate și determinare de a respecta obligațiile ce decurg din activitatea de control parlamentar pe calea întrebărilor și interpelărilor și de a asigura o bună relație între Guvern și Parlament.

Cu deosebită considerație,

NINI SAPUNARU

SECRETAR DE STAT

Nr. 5702 / DRP
DATA 14-05-2026

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

14-05-2026

Către Secretariatul General al Guvernului
Departamentul pentru Relația cu Parlamentul

În atenția Domnului Secretar de Stat, Nini SĂPUNARU

Referitor la Solicitarea domnului deputat Adrian-Felician COZMA

Nr. T36 din 07 mai 2026
Ex. nr. 1
NECLASIFICAT

Stimate domnule Secretar de Stat,

Ca urmare a corespondenței dumneavoastră nr. 4670 din 23.04.2026 privind întrebările formulate de către domnul deputat Adrian-Felician COZMA, adresă înregistrată la nivelul Camerei Deputaților cu nr. 4925A din 21.04.2026, vă comunicăm următoarele:

În perioadă solicitată, la nivelul Directoratului Național de Securitate Cibernetică (DNSC) au fost înregistrate un număr de 11361 sesizări privind atacuri de tip phishing (tentative de fraudă prin care atacatorii încearcă să obțină date sensibile: date cu caracter personal, parole, date bancare, coduri de autentificare, prin apeluri, mesaje sau impersonarea unor surse legitime), 8517 (aproximativ 75%) dintre acestea fiind de tip vishing/smishing/spoofing.

Atacurile de tip vishing (voice phishing) reprezintă o formă de phishing realizată prin apeluri telefonice, în care atacatorii se prezintă drept reprezentanți ai unor instituții sau companii, pentru a convinge victimele să divulge informații confidențiale.

Cele de tip smishing (SMS phishing) constau în transmiterea de mesaje SMS care conțin, de regulă, link-uri către site-uri malițioase sau solicitări de furnizare a unor date personale sau financiare, iar cele de tip spoofing reprezintă o tehnică prin care un atacator falsifică identitatea unei surse de comunicare (de exemplu un număr de telefon) pentru a părea legitimă și a induce în eroare utilizatorii, în scopul obținerii de informații sensibile sau al facilitării altor atacuri cibernetice ulterioare.

Astfel, dintre cele 8517 sesizări privind aceste atacuri de tip vishing/smishing/spoofing, 5836 au fost realizate prin intermediul unor numere de telefon mobil, însă nu poate fi determinat, la nivelul DNSC, dacă sursa amenințărilor provine de pe cartele telefonice preplătite, abonamente sau prin metode de clonare, pe fond procesul fiind unul reactiv.

De asemenea, cu privire la restul atacurilor de tip phishing, nu se poate face o diferență dacă au fost clonate sau au fost create, cu identități fictive, conturile de e-mail sau conturile de pe rețelele de socializare.

Având în vedere eventualul impact asupra persoanelor care au efectuat astfel de sesizări, putem opina că acestea au reprezentat tentative ale unor infracțiuni de înșelăciune și fraudă financiară, fără a fi cunoscută finalitatea proceselor penale, aspecte care excedează competențelor DNSC.

Totodată, facem precizarea că toate datele privind diversele atacuri cibernetice gestionate la nivelul Directoratului, care pot fi asociate cu diverse infracțiuni, sunt puse la dispoziția instituțiilor abilitate, în timp real.

Cu privire la măsurile legislative prioritare, considerăm necesar a fi stabilită o bază legală privind responsabilizarea operatorilor de telefonie pentru filtrarea SMS-urilor malițioase respectiv implementarea unor mecanisme anti-spoofing, acolo unde este posibil.

Având în vedere caracterul de urgență al stopării fenomenului de spoofing și riscurile asociate acestuia, DNSC a inițiat, împreună cu alte entități, demersuri de standardizare a măsurilor de validare a identității apelantului și de adoptare a unor măsuri tehnice rapide și eficiente, adaptate infrastructurii actuale.

Pentru orice informații suplimentare vă stăm la dispoziție.

Cu deosebită considerație,

Dan Cîmpean

ROMÂNIA DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
DIRECTORUL DNSC

Directorul Directoratului Național de Securitate Cibernetică (DNSC)

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Digitally signed by Cimpean Petre-Dan
Date: 2026.05.13 17:16:09 +02'00'