Ziarul Ancheta Online

Sursa ta în timp real

Mesajul care te poate lăsa fără bani în cont. Avertismentul DNSC

By Daniela Neacșa - 27/07/2026

Directoratul Național de Securitate Cibernetică (DNSC) avertizează asupra unei noi campanii de fraudă prin SMS, în care infractorii invocă taxe de parcare neachitate pentru a păcăli utilizatorii și a le fura datele personale și bancare.

Potrivit specialiștilor DNSC, potențialele victime primesc un mesaj despre o presupusă taxă de parcare neachitată: „contul de parcare prezintă plăți restante”. Acesta este doar pretextul folosit de atacatori pentru a determina destinatarul să acceseze un link malițios.

Mesajul este construit astfel încât să creeze încă din primele rânduri o stare de îngrijorare. După ce informează utilizatorul despre existența unei presupuse datorii, acesta primește și o

aparentă veste bună: „ținând cont de istoricul dumneavoastră de plată, vă oferim o ultimă oportunitate de a achita suma datorată fără penalități de întârziere”. Specialiștii DNSC explică faptul că această tehnică este folosită pentru a câștiga încrederea victimei și pentru a o determina să acționeze fără să verifice autenticitatea mesajului.

Pasul următor este accesarea link-ului inclus în SMS. În realitate, acesta nu conduce către pagina unei instituții oficiale, ci către un site fraudulos controlat de atacatori. Acolo sunt solicitate informații personale și financiare, inclusiv datele cardului bancar. Introducerea acestora poate duce la compromiterea conturilor și la pierderi financiare.

Pentru a accentua presiunea, mesajul stabilește și un termen-limită de plată, avertizând că, după data de 28 iulie 2026, vor fi aplicate taxe suplimentare de cel puțin 200 de lei, costuri de recuperare, dobânzi și chiar consecințe asupra istoricului de credit. Potrivit DNSC, acesta este un mecanism psihologic întâlnit frecvent în atacurile de tip phishing, prin care victimele sunt împinse să reacționeze impulsiv.

Cum îți dai seama că mesajul este o tentativă de fraudă

Specialiștii în securitate cibernetică spun că există mai multe indicii care arată că mesajul nu este autentic:

- sursa mesajului este o adresă de e-mail
- domenii suspecte sau fără legătură cu instituția oficială
- formulări alarmante și presiune privind termenul-limită: „termenul limită de plată”, „taxe suplimentare de cel puțin 200 lei”, „vă oferim o ultimă oportunitate de a achita suma datorată”
- solicitarea accesării urgente a unui link
- prezența celor 3 elemente comune tentativelor de fraudă – emoția, urgența, urmată de socilitarea furnizării de date

Recomandările DNSC

Pentru a nu cădea în capcana atacatorilor cibernetici, DNSC recomandă românilor să nu acceseze link-urile primite prin astfel de mesaje, să verifice întotdeauna autenticitatea domeniului și să confirme orice informație privind eventuale obligații de plată exclusiv pe site-urile oficiale ale instituțiilor.

Totodată, oamenii sunt sfătuiți să nu introducă date personale sau bancare pe pagini care ridică suspiciuni.

Tentativele de fraudă pot fi raportate la numărul 1911 sau prin Platforma Națională de Raportare a Incidentelor de Securitate Cibernetică. Pentru un nivel suplimentar de protecție, DNSC recomandă instalarea extensiei DNSC Blacklist Protection, care avertizează utilizatorii atunci când încearcă să acceseze domenii periculoase sau frauduloase.

Specialiștii reamintesc că cele mai multe atacuri cibernetice exploatează emoția, urgența și lipsa de verificare. Câteva secunde acordate verificării sursei mesajului pot face diferența dintre evitarea unei fraude și pierderea datelor personale sau a banilor din conturi.

Foto (descriptiv): FreePik

Original article:

https://anchetaonline.ro/mesajul-care-poate-lasa-fara-bani-cont-avertismentul-dnsc-334029/