

## Te ajutam să te ții departe de fraude!

În ziua de astăzi, există tot felul de metode de fraudare în care poate fi folosit numele „Telekom Romania Communications”. În primul rând, ne cerem scuze pentru ele, dar vrem să te asigurăm că nu suntem răspunzători. De aceea, vrem să te ajutăm să nu cazi în plasa lor, oferindu-ți câteva informații și sfaturi.

### Frauda prin telefon/SMS

Este posibil să fii apelat sau să primești un SMS, pe numărul tău, de la persoane care pretind că sunt reprezentanți ai companiei Telekom Romania Communications și care:

- Îți solicită informații confidențiale pentru un premiu sau verificări de bază de date;
- Te roagă să apelezi un număr care începe cu 090 pentru a intra în posesia premiului;
- Te roagă să efectuezi o plată bancară.



### În acest caz, îți recomandăm:

- Să te asiguri că într-adevăr ai participat la un concurs cu premii oferite de Telekom Romania Communications;
- Să ceri mai multe detalii cu privire la concursul/evenimentul în urma căruia ai fi putut câștiga premiul;
- Să nu comunicii informații personale confidențiale (precum CNP, serie și număr de buletin, conturi bancare, parole personale de acces la contul de abonat);
- Să nu apelezi numerele indicate, înainte de a verifica dintr-o sursă sigură dacă sunt alocate ca parte a unui concurs Telekom Romania Communications;
- Să nu formezi combinații de cifre de forma 91407% (pe linie telefonică fixă), deoarece aceste acțiuni vor redirecționa apelurile către numere de mobil. Un deranjament telefonic nu se rezolvă prin formarea de coduri speciale, iar un aparat telefonic fix obișnuit nu se poate virusa;
- Să nu faci plăți bancare către beneficiari pe care îi cunoști doar prin telefon;
- Să nu dai curs solicitărilor exprese de a tasta pe aparatul telefonic diverse coduri. Poți găsi detalii cu privire la campaniile și promoțiile lansate de Telekom Romania Communications pe <https://www.fix.telekom.ro>, în magazinele Telekom Romania Communications sau ale partenerilor nostri, precum și sunând gratuit de pe telefonul mobil la numărul 1930 (apelabil din rețeaua Telekom Romania Communications) – apeluri cu tarif normal.

### Atenție la atacurile prin SMS!

În această perioadă, se desfășoară o campanie de Smishing (Phishing prin SMS), prin care utilizatorii de telefoane și internet sunt informați prin intermediul unui SMS că urmează să primească un colet. Aceste mesaje, ce par a fi trimise de o firmă de curierat, conțin viruși care afectează dispozitivele și accesează datele personale ale utilizatorilor (inclusiv parole și date ale cardurilor bancare), pe care hackerii le utilizează în scopuri ilicite.

Vă recomandăm să parcurgeți cu atenție mesajele pe care le primiți de la destinatari necunoscuți și să nu deschideți linkurile incluse în text.

Dacă ați primit un astfel de mesaj, vă recomandăm să-l ștergeți imediat.

În cazul în care ați accesat linkul și telefonul este compromis, vă recomandăm să resetați dispozitivul, să-l aduceți la setările din fabrică. **Această operațiune presupune pierderea tuturor informațiilor din telefon!**

Protejați-vă datele și dispozitivele, nu furnizați informații confidențiale persoanelor necunoscute,

indiferent de forma prin care vă sunt solicitate – telefonic sau în prin mesaje scrise.  
Nu contactați numere necunoscute, cu atenție sporită asupra numerelor internaționale.  
Nu accesați linkuri sau pagini web care imită identitatea vizuală a unor organizații cunoscute.

### **Frauda de tip Wangiri**

Persoane necunoscute care au intenția de a te înșela dau bip-uri sau te apelează de pe numere internaționale, atragându-te să sune înapoi pentru a participa la anumite tombole / concursuri cu premii mari în bani (de exemplu 5000 \$). Numerele internaționale sunt din afara Europei, iar apelurile către acestea au tarife pe minut ridicate.

Tombolenle/castigurile care sunt menționate sunt fictive și au scopul de a te înșela, de a te atrage să apelezi numerele suspecte cu tarife mari și să rămâi cât mai mult timp conectat în convorbire.

### **În acest caz, îți recomandăm:**

Să nu sune înapoi pe numere pe care nu le cunoaști, cu atât mai mult dacă acestea sunt numere internaționale. Numerele de România le poți identifica ușor, acestea încep cu +40 sau 0040 sau 07, 02, 03;

Să nu furnizezi date cu caracter personal dacă acestea îți sunt solicitate prin aceste apeluri.

Apelarea acestor numere este decizia ta, dar te informăm că tariful pentru aceste destinații este ridicat și valoarea apelurilor efectuate va face să crească costul facturii tale telefonice!

### **Frauda cu facturi**

Este posibil să primești o factură asemănătoare cu cea de la Telekom Romania Communications în care să îți se solicite să plătești servicii care, până în acel moment, nu erau tarificate și nici solicitate de tine.



### **În acest caz, îți recomandăm:**

Să verifici existența însemnelor vizuale Telekom Romania Communications și a datelor de identificare

Să verifici prezența codului de facturare și a codului de abonat (comparându-le cu o factură anterioară);

Să soliciți lămuriri, apelând numărul 1930, serviciul nostru de Vânzări și Relații cu

Clienții (apel gratuit în rețea);

Să nu achizițezi factura în cauză, decât dacă ești sigur pentru ce anume plătești.



## **Frauda pe internet**

Este posibil să fii victima unor abuzuri online, ca de exemplu:

### *Abuzuri pe e-mail, spam:*

- Dacă primești mesaje e-mail cu caracter comercial, fără a le fi solicitat.
- Dacă echipamentele tale conectate la serviciile de internet Telekom Romania Communications, ca urmare a contaminării acestora cu malware, sunt folosite fără acordul tău, de către terțe persoane (hackeri) pentru desfășurarea unor activități ilegale, de genul trimiterii de spam-uri sau lansare de atacuri către alți clienți sau alte rețele/serve.

### *Oferte înșelătoare, aplicații de phishing*

Acestea constau în primirea de e-mailuri cu linkuri către site-uri care imită pagini web ce urmăresc să-ți creeze impresia să interacționezi cu un furnizor de servicii: banca, site-ul de socializare, magazin online sau urmăresc sau să-ți atragă atenția în diverse concursuri false, „scheme financiare”, toate acestea având ca scop: obținerea de bani, furtul de date personale sau furtul/folosirea datelor bancare.

### *Alerte firewall, atacuri DoS, acces neautorizat:*

Prin intrarea, prin porturi, a unui hacker sau virus în calculator;

Cu ajutorul unor programe, ei pot scana porturi deschise, infiltrându-se astfel în calculator și provocând diferite neplăceri. Atacul de tip DoS este o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator.

### **În aceste cazuri de fraudă pe internet, îți recomandăm:**

Pentru a vă proteja de spam: instalați filtre spam, evitați publicarea adresei dvs. de mail pe diverse site-uri, nu vă înregistrați cu mailul pe site-uri despre care nu aveți suficiente informații, nu răspundeți la mesaje trimise de pe adrese suspecte, nu deschideți atasamentele de la destinatari necunoscuți, folosiți un antivirus la zi, eventual folosiți o metodă de criptare și vizualizați mailul în plain text.

Puteti raporta spam-ul inițiat de pe IP-uri aparținând Telekom Romania Communications, salvând sursa mesajului, headerele și trimițându-le către [abuse@telekom.ro](mailto:abuse@telekom.ro).

Nu accesați linkuri primite prin e-mail de la persoane necunoscute. Telekom Romania Communications nu solicită nicodată date personale sau elemente de securitate aparținând clienților (număr card, data de expirare, PIN-ul sau parola) prin accesarea unui link transmis prin email;

De asemenea, este recomandat să utilizați securizarea browserului, a e-mailului precum și softuri folosite pentru prevenirea furtului de identitate, prin configurarea corespunzătoare a acestora.

**Dacă identificați o tentativă de fraudă, te rugăm să ne informați la numerele de telefon menționate mai sus și să te adresezi organelor de Poliție, urmând ca toate informațiile și documentele solicitate și disponibile în evidențele Telekom Romania Communications să fie puse la dispoziția acestora, la cerere, în funcție de legislația aplicabilă.**