



NewTech Academy

powered by **wawiwa**

GHID PRACTIC DE SIGURANȚĂ CIBERNETICĂ PENTRU TOȚI

**Cum să-ți protejezi datele, banii și identitatea
împotriva fraudelor online?**



Contul tău a fost spart!

Nimeni nu își dorește să primească acest mesaj.

Cu toate acestea, statisticile arată că 6 din 10 români se confruntă anual cu tentative de fraudă și atacuri cibernetice.

Ce este de făcut dacă ajungi, fără să vrei, victimă a unei scurgeri de date sau chiar a unui atac cibernetic?

Acest ghid apare în contextul recentului **atac asupra ANCPi din iulie 2026**, unul dintre cele mai grave astfel de incidente din istoria administrației publice românești. Datele cu caracter personal ale cetățenilor aflați în registrul instituției au fost preluate de către hackeri, iar sisteme administrative importante (e-Terra, ePay) au fost scoase din funcțiune.

Informația înseamnă putere. Prin acest material, urmărim să oferim sprijin și claritate în primul rând persoanelor direct afectate de incidentul ANCPi. Vrem să știi exact la ce să te aștepți, acum, când datele tale s-ar putea afla în mâna unor terți cu intenții malițioase. Află cum să acționezi corect și rapid în cazul în care devii ținta unor fraude sau atacuri cibernetice.

Dincolo de acest incident, manualul se adresează tuturor celor care doresc să afle cum se pot pune la adăpost. Prevenția și intervenția corectă sunt esențiale. Parcurgând aceste pagini, vei învăța cum să recunoști pericolele înainte să producă pagube și cum să îți construiești un scut solid pentru viața ta digitală.

Cuprins

1. Scurt istoric al celor mai recente incidente majore de securitate cibernetică din România

- Atacul asupra ANCPI (14 iulie 2026)
- Alte atacuri recente
- La ce poți să te aștepți: ce urmează imediat după o breșă de securitate cibernetică?
- Cum pot arăta atacurile directe asupra ta în această etapă?
- Cum verifici dacă datele tale au fost furate?

2. Cum recunoști pericolele cibernetice?

- E-mailuri, SMS-uri sau mesaje Whatsapp/Messenger false (phishing și smishing)
- Apeluri telefonice frauduloase (vishing) — pe primul loc în topul fraudelor din 2026
- Site-uri false (spoofing)
- Care sunt semnele că un cont sau datele tale au fost compromise?
- Regula celor 3 secunde — verifică înainte de a acționa!

3. Prevenție și igienă digitală de bază

- Cum să eviți furtul de conturi și parole online
- Cum îți protejezi CNP-ul și copia cărții de identitate

4. Ghid de urgență: ce faci dacă ai fost implicat într-un atac cibernetic

- Situația A. Ai introdus datele cardului pe un site suspect
- Situația B. Ai transmis unui necunoscut parola contului tău de e-mail sau un cod de verificare
- Situația C. Ai trimis CNP-ul sau copia buletinului către un terț neverificat
- Situația D. Calculatorul sau telefonul tău se comportă suspect
- Pe cine contactezi în România în caz de urgență (atac cibernetic)
- Model de mesaj către bancă sau echipa de suport

1. Incidente majore de securitate cibernetică din România: scurt istoric recent



Atacul asupra ANCPI (14 iulie 2026)

În luna iulie 2026, Agenția Națională de Cadastru și Publicitate Imobiliară (ANCPI) a fost ținta unui incident cibernetic care a vizat accesul neautorizat la infrastructura instituției. Atacul, declanșat în perioada 14-15 iulie, a condus la indisponibilitatea unor servicii esențiale, inclusiv platforma e-Terra și sistemul intern de e-mail. Acest lucru a generat blocaje și întârzieri semnificative pentru notari, bănci, avocați și, implicit, pentru cetățenii implicați în tranzacții imobiliare.

Deși ANCPI a declarat oficial că bazele de date tehnice și juridice au rămas intacte, atacatorii au revendicat public extragerea unor volume importante de date personale și furtul codului-sursă. Indiferent de gradul real de compromitere a datelor confirmat oficial ulterior, în acest moment este necesar să devenim extrem de prudenți în fața mesajelor personalizate care ne pot fi trimise, invocând numele instituției.

Atacul asupra ANCPI nu este, din păcate, un incident singular. El se înscrie într-o serie îngrijorătoare de breșe de securitate care au vizat atât statul, cât și mediul privat din România, în istoria recentă.

Accesul neautorizat de la Banca Transilvania (2 iulie 2026)

Autoritatea Națională de Supraveghere a Prelucrării Datelor (ANSPDCP) a constatat că un angajat a accesat legal extrasele de cont ale unei persoane expunând date financiare reale, precum nume, IBAN, cod client, tranzacții și sold. Deși a fost un incident intern izolat, cazul a arătat cum datele reale scurse pot fi folosite pentru presiune sau fraude țintite.

Incidentul de la Ministerul Investițiilor și Proiectelor Europene (MIPE) (16 iulie 2026)

Aplicația destinată achizițiilor pentru beneficiarii privați din Politica de Coeziune a devenit indisponibilă în urma unui incident cibernetic. Acest blocaj a forțat ajustarea termenelor procedurale și a generat întârzieri majore pentru firmele implicate în proiecte europene.

Breșa de la Orange România (17 Iulie 2026)

Aici au avut loc două incidente distincte. O eroare de sistem a expus facturile unor clienți, iar o platformă internă de ticketing insuficient protejată a permis sustragerea unui volum uriaș de date personale: contacte, CNP-uri, acte de identitate, IBAN-uri, date despre SIM și informații privind cardurile bancare. Acest lucru a expus clienții la un risc major de preluare a conturilor sau schimbare frauduloasă a cartelei SIM.

Incidentul „Hipocrate” (2024)

Un atac cibernetic masiv de tip ransomware a paralizat zeci de spitale din România prin infectarea sistemului informatic medical Hipocrate. Acest incident a blocat accesul la fișele pacienților și a perturbat grav activitatea medicală la nivel național.

Fraudele de tip phishing pe OLX (fenomen continuu)

- **Mutarea pe WhatsApp sau Telegram:** Escrocii evită chat-ul intern OLX pentru a ocoli filtrele de securitate ale platformei.
- **Mecanismul „Curierat / Plată prin OLX”:** Vanzătorii primesc linkuri către pagini clonate unde li se cer datele cardului sub pretextul încasării banilor.
- **Vânzătorul fals (Plata în avans):** Anunțuri cu produse atractive la prețuri mici, unde se cere un avans, după care autorul dispare.
- **Astență tehnică fictivă:** Fereastră de chat integrată pe site-ul fals, unde un presupus „operator OLX” convinge victima să valideze tranzacția.
- **Dovezi de plată falsificate:** Trimiterea unor imagini cu ordine de plată contrafăcute pentru a obține livrarea produsului înainte de intrarea banilor în cont.

La ce poți să te aștepți: ce urmează imediat după o breșă de securitate cibernetică?

- **Revendicare și șantaj:** Hackerii publică mesaje triumfaliste pe forumuri de pe „dark web” sau pe aplicații criptate (precum Telegram), lăudându-se cu atacul, prezentând „mostre” de date furate și cerând răscumpărări.
- **Un val de fraude „secundare” (momentul critic pentru cetățeni):** Faptul că atacatorul îți știe numele, CNP-ul, adresa, contul bancar sau detaliile unui contract transformă niște simple mesaje text în capcane perfecte. Infractorii inițiază campanii masive în care pozează în persoane oficiale pentru a-ți câștiga încrederea, exploataând exact datele reale sustrase.



AVERTISMENT — cea mai frecventă amenințare NU este un atac de amploare

Conform statisticilor DNSC pentru primul semestru din 2026, majoritatea fraudelor raportate nu vin din marile atacuri de presă, ci din înșelătorii individuale: 42% sunt fraude prin telefon (vishing), 14% sunt phishing prin e-mail și 13% sunt fraude prin SMS (smishing). Pentru prima dată, escrocheriile telefonice au ajuns pe primul loc.

Cum pot arăta atacurile directe asupra ta în această etapă?

- **E-mailuri și SMS-uri înșelătoare (phishing & smishing):** Primești mesaje care invocă un fals scenariu de urgență, cum ar fi „cont blocat”, „amendă neplătită” sau „colet returnat”. Ți se cere să dai click pe un link scurtat sau suspect și să introduci parola, codul PIN sau codul OTP.
- **Apeluri de la falși salvatori (vishing):** Ești sunat de indivizi care pretind a fi de la bancă, Poliție sau departamente antifraudă. Îți spun că cineva încearcă să ia un credit pe numele tău și te presează să le dai coduri sau să instalezi pe telefon aplicații de acces la distanță (precum AnyDesk) pentru a „rezolva” problema.
- **Clone periculoase:** Apar site-uri false care copiază perfect vizual platforme oficiale (cum ar fi Ghișeul.ro, e-Terra etc.) și pagini de plată care îți cer datele de pe card.

Cum verifici dacă datele tale au fost furate?

Cea mai rapidă metodă de a verifica dacă adresa ta de e-mail a fost expusă este platforma gratuită Have I Been Pwned (haveibeenpwned.com).

În cazul specific al recentului atac asupra ANCPI, deși hackerii au susținut public că dețin datele cetățenilor, autoritățile române – inclusiv Directoratul Național de Securitate Cibernetică (DNSC) – au declarat oficial că, până în acest moment, nu a fost confirmată extragerea masivă de date personale sau a documentelor de carte funciară. Investigațiile sunt încă în desfășurare.

Conform legii privind protecția datelor (GDPR), dacă se va stabili cu certitudine că datele cu caracter personal au fost compromise, ANCPI are obligația legală de a transmite informațiile necesare și de a notifica cetățenii afectați – fie direct (prin e-mail sau corespondență), fie prin comunicate publice oficiale cu pașii clari de urmat. Așadar, nu lua decizii pripite, informează-te doar din surse oficiale și menține-ți un nivel de vigilență ridicat.



DE REȚINUT

Indisponibilitatea unei platforme sau afirmațiile unui atacator NU dovedesc automat că toate datele tale au fost furate. Tratează totuși aceste situații cu prudență și aplică regulile din acest ghid, mai ales dacă ai fost client al instituțiilor menționate mai sus.

2. Cum recunoști pericolele cibernetice?

Atacurile cibernetice pot avea loc oricând, nu doar imediat după un incident de breșă în securitatea unei instituții.

Atacatorii profită de context: folosesc știrile despre atacuri reale pentru a părea credibili și combină trei canale principale pentru a fura date de card și a se propaga către alte contacte din agenda victimei: prin telefon (vishing), prin SMS (smishing) sau aplicații tip Whatsapp/Facebook Messenger, prin e-mail (phishing).

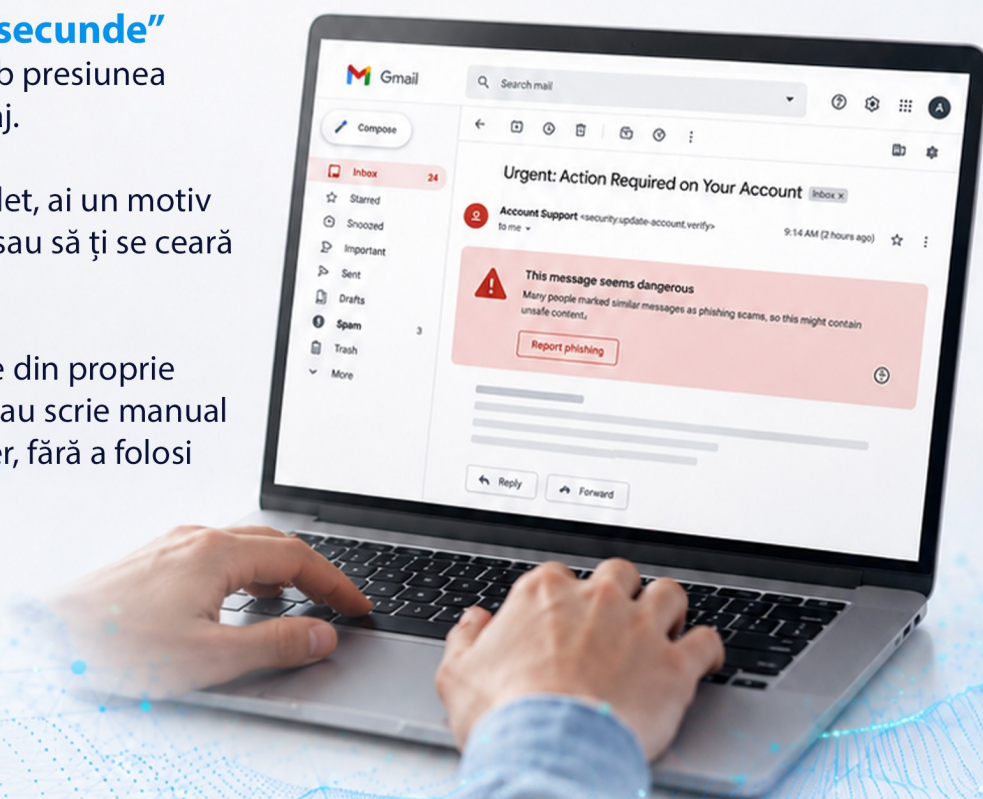
E-mailuri, SMS-uri, mesaje Whatsapp/Messenger false (phishing și smishing)

Sunt de regulă mesaje care pretind că vin de la Poșta Română, ANAF, Ghișeul.ro, firme de curierat, bănci sau firme de energie. Fii atent la următoarele caracteristici care trădează fraudă:

- **Ton de urgență:** „Contul tău va fi blocat în 24 de ore”, „Ai o amendă neplătită”, etc.
- **Greșeli de limbă:** exprimări nefirești, traduceri stângace, lipsă de diacritice, saluturi generale.
- **Solicitare directă de date sensibile:** cod PIN, CVV, parolă, cod OTP primit prin SMS.
- **Adresă de expeditor ciudată:** domenii care nu se termină corect (ex. „posta-romana-livrari.com” în loc de „posta-romana.ro”).
- **Linkuri scurtate sau ascunse:** nu poți vedea unde te duce cu adevărat linkul; sau se cere descărcarea unui fișier .zip, .apk sau .html.

Aplică „Regula celor 3 secunde”

- **Oprește-te:** Nu acționa sub presiunea urgenței generate de mesaj.
- **Întreabă-te:** Aștepti un colet, ai un motiv real să primești o amendă sau să îți se ceară reconfirmarea datelor?
- **Verifică separat:** Deschide din proprie inițiativă aplicația oficială sau scrie manual adresa instituției în browser, fără a folosi linkul din mesaj.



Apeluri telefonice frauduloase (vishing) — nr 1 în topul fraudelor din 2026

Atacatorii manipulează psihologic victimele prin crearea unui sentiment artificial de frică și urgență extremă.

- **Falsa identitate:** Persoana de la capătul firului pretinde că este ofițer de securitate bancară, reprezentant al Poliției sau al DNSC.
- **Falsa urgență:** Îți comunică fie că un credit fraudulos a fost deschis pe numele tău, fie că a fost detectată o tranzacție suspectă.
- **Falsa soluție:** Îți solicită să transferi urgent banii într-un așa-zis „cont de siguranță”.
- **Furtul codurilor:** Îți cer să le dictezi sau să confirmi „din reflex” codul OTP pe care tocmai l-ai primit prin SMS.
- **Preluarea controlului:** Te presează să instalezi aplicații de acces la distanță (precum AnyDesk sau TeamViewer) sub pretextul că te vor „ajuta” sau îți vor „proteja” contul.
- **Presiunea continuă:** Vorbesc apăsător, refuză să îți lase timp de gândire și insistă agresiv să nu închizi telefonul până nu se „rezolvă” problema.

Semnale de alarmă: Cum identifici rapid un apel telefonic suspect

- **Accente atipice și bariere lingvistice:** Pronunție nenaturală a denumirilor românești (orașe, nume de bănci, instituții) sau un ton extrem de formal combinat cu greșeli gramaticale de bază, specifice apelurilor inițiate din call-center-e din afara țării.
- **Boți și tehnologie AI (Deepfake):** Pauze nefirești de 2-3 secunde înainte de a primi un răspuns (timp de procesare a informației), reacții rigide sau repetitive la întrebări neașteptate din afara contextului și un ton vocal monoton sau robotic.
- **Tăcere la preluarea apelului:** O scurtă pauză de liniște imediat ce spui „Alo” indică un sistem automat de apelare (predictive dialer) care transferă apelul către un operator abia după ce detectează voce umană.
- **Solicitarea de aplicații de control de la distanță:** Insistența de a instala software precum AnyDesk sau TeamViewer sub pretextul „asistenței tehnice” sau al protejării contului.
- **Invocarea „contului de siguranță” sau cererea de coduri:** Îndemnul direct de a transfera fonduri către un alt cont sau cererea de a dicta coduri OTP, codul PIN ori datele cardului.

DE REȚINUT

Nicio bancă, autoritate sau echipă de suport nu îți va cere niciodată prin telefon parola completă, codul PIN sau codul OTP.

Nu te grăbi – chiar dacă atacatorul te îndeamnă să o faci. Dacă ai dubii, închide și sună tu, din proprie inițiativă, la numărul oficial de pe cardul bancar sau de pe site-ul instituției din partea căreia se pretindea a fi apelul.

Site-uri false (spoofing)

Cum distingi o adresă reală de una falsificată?

Verifică adresa (URL-ul / linkul site-ului). Instituțiile publice românești folosesc, de regulă, domenii care se termină în **.ro** sau **.gov.ro**. Orice altă terminație însoțită de numele instituției este un semnal de alarmă. Privește următorul tabel pentru a te familiariza cu modul în care adresele site-urilor false pot să arate.

Domeniu legitim	Exemple de variante FALSE folosite de escroci
anaf.ro	anaf-online.ro / anaf.ro.plata-urgenta.com
posta-romana.ro	posta-romana-livrari.com / posta-romana.co/urmarire-colet
ghiseul.ro	ghiseul.cc / ghiseul.cc / ghiseul-ro.com / ghiseul.info
numele băncii tale + .ro	numele băncii + un cuvânt suplimentar + domeniu străin (.com, .net, .info, .cc)

DE REȚINUT

Prezența cuvântului „ANAF”, „bancă” sau „gov” într-o adresă nu o face automat oficială. Nici lacătul (https) din browser nu garantează că proprietarul site-ului este instituția reală — arată doar că traficul este criptat, nu cine îl deține. Trebuie ca întreaga adresă să corespundă structural celei oficiale pentru a fi de încredere.

Care sunt semnele că un cont sau datele tale au fost compromise?

- Primești o alertă de conectare dintr-un oraș sau de pe un dispozitiv necunoscut. (Raportează-o administratorului de rețea!)
- Primești notificări de resetare a parolei pe care nu tu le-ai cerut. (Ignoră-le!)
- Apar tranzacții sau plăți pe care nu le recunoști în extrasul de cont. (Blochează contul și raportează băncii!)
- Nu te mai poți autentifica cu parola obișnuită la un cont (e-mail, rețea socială, bancă). (Apelează serviciul de suport clienți!)
- Prietenii sau familia primesc mesaje „de la tine” pe care nu le-ai trimis. (Alertează-i să nu deschidă niciun link!)
- Primești repetat cereri de aprobare 2FA pe care nu le-ai inițiat. (Raportează-le adminului!)
- Datele de recuperare ale contului (număr de telefon, e-mail secundar) au fost modificate fără știrea ta. (Activează autentificarea în 2 pași!)
- Telefonul își pierde brusc semnalul, deși alte telefoane din jur funcționează normal — poate indica o preluare frauduloasă a numărului tău (SIM swap).

[!] ÎNAINTE SĂ DAI CLICK PE UN LINK, SĂ RĂSPUNZI LA UN APEL SUSPECT SAU SĂ OFERI UN COD:

1. Oprește-te

Nu acționa sub presiune.
Urgența este cea mai folosită armă a escrocilor.
Nu este nicio grabă reală.

2. Întreabă-te

Aștept eu acest mesaj sau apel?
De ce mi-ar cere cineva parola sau codul meu? Expeditorul și adresa sunt exact cele oficiale?

3. Verifică separat

Închide mesajul sau apelul și intră singur în aplicația oficială, sau sună instituția folosind un număr găsit independent

3. Prevenție și igienă digitală de bază

Cum să eviți furtul de conturi și parole online

Scurgerea datelor online nu este întotdeauna prevenibilă (vezi cazul ANCPPI).

Există însă și câteva obiceiuri simple care stau în controlul tău și care îți pot reduce drastic riscul de a fi victimă a unei fraude, chiar și atunci când datele tale circulă deja pe internet în urma unei scurgeri.

[✓] AȘA DA	[X] AȘA NU
✓ Folosește o parolă diferită și un manager de parole (de ex. LastPass) pentru conturile importante (e-mail, bancă, cumpărături).	✗ Nu refolosi aceeași parolă la mai multe conturi importante.
✓ Activează autentificarea în doi pași (2FA/MFA) la e-mail, bancă și rețele sociale — mai ales la contul principal de e-mail, care poate reseta toate celelalte parole.	✗ Nu păstra parolele într-un mesaj trimis ție pe WhatsApp sau într-un document numit „Parole”.
✓ Verifică întotdeauna adresa completă a expeditorului și a site-ului, nu doar numele afișat sau logo-ul.	✗ Nu accesa linkuri care creează un sentiment de urgență sau frică, primite prin SMS sau e-mail.
✓ Actualizează regulat telefonul, calculatorul, browserul și aplicațiile.	✗ Evită să folosești sisteme sau browsere legacy care nu au mai primit actualizări de siguranță de mult timp.
✓ Folosește Wi-Fi-ul securizat sau datele mobile (nu Wi-Fi public necunoscut) pentru operațiuni bancare sensibile.	✗ Nu folosi rețele publice de Wi-Fi pentru tranzacții.
✓ Activează notificările pentru plăți și conectări noi în cont — și fii atent chiar și la sumele mici pe care nu le recunoști.	✗ Nu oferi niciodată codul OTP primit prin SMS unei persoane la telefon, indiferent cine pretinde că este.
✓ Păstrează copii de siguranță ale documentelor importante în format fizic și în cloud (ex. Google Drive), nu doar pe telefon.	✗ Nu te baza pe un singur dispozitiv pentru a păstra copii ale documentelor tale.
✓ Raportează mesajele și apelurile suspecte la DNSC.	✗ Nu presupune că un mesaj e autentic doar pentru că are sigla instituției — siglele pot fi copiate ușor.
✓ Păstrează-ți laptopul securizat cu parolă și nu permite niciunei persoane necunoscute accesul de la distanță.	✗ Nu instala aplicații de acces la distanță (AnyDesk, TeamViewer) la recomandarea unei persoane care te-a sunat.
✓ Instalează doar aplicații cu rating bun și provenite de pe platformele oficiale (Google Play, App Store).	✗ Nu instala aplicații din surse necunoscute.

Cum îți protejezi CNP-ul și copia cărții de identitate

[✓] AȘA DA	[X] AȘA NU
✓ Atunci când ți se solicită CI, întreabă de ce este necesară copia și cât timp va fi păstrată.	✗ Nu trimite buletinul printr-un grup de WhatsApp sau Messenger. Dacă ai apelat la servicii de printing de acte, solicită ștergerea din sistemul lor a copiei actului tău.
✓ Folosește platformele securizate indicate oficial de instituții pentru transmiterea copiei după CI, nu un link primit prin mesaj.	✗ Nu publica documentul într-un formular găsit printr-o reclamă online.
✓ Scrie pe copia fizică, vizibil: „Copie transmisă către [instituție], exclusiv pentru [scop], la data de [data]”.	✗ Nu lăsa copia fără menționarea scopului pentru care a fost transmisă.
✓ Ascunde informațiile care nu sunt necesare pentru scopul cerut, dacă procedura o permite.	✗ Nu transmite atât fața, cât și spatele documentului dacă se solicită justificat doar o singură informație.
✓ Păstrează dovada transmiterii și numele destinatarului.	✗ Nu presupune că „este doar o copie” — poate fi folosită pentru deschiderea de credite sau conturi în numele tău.

4. Ghid de urgență: ce faci dacă ai fost implicat într-un atac cibernetic



Situația A. Ai introdus datele cardului pe un site suspect

- Sună imediat banca. Blochează cardul din aplicație sau telefonic, cere verificarea tranzacțiilor și întreabă dacă e necesară emiterea unui card nou. Nu aștepta să apară prima plată frauduloasă.
- Nu mai folosi pagina suspectă și nu descărca alte fișiere de pe ea.
- Păstrează dovezile: captură cu mesajul, adresa site-ului, numărul expeditorului, data și ora.

Situația B. Ai transmis unui necunoscut parola contului tău de e-mail sau un cod de verificare

- Folosește un dispozitiv sigur (alt telefon sau calculator) pentru a schimba imediat parola contului afectat.
- Protejează mai întâi e-mailul principal — el poate fi folosit pentru resetarea parolelor la bancă, rețele sociale și magazine online.
- Închide toate sesiunile active din setările de securitate ale contului: „Deconectează toate dispozitivele” / „Sign out everywhere” / „Sesiuni active”.
- Activează autentificarea în doi pași, preferabil printr-o aplicație de autentificare, nu doar prin SMS.

Situația C. Ai trimis CNP-ul sau copia buletinului către un terț neverificat

- Anunță instituția sau firma căreia i-ai transmis documentul și cere în scris confirmarea modului în care datele sunt folosite.
- Cere restricționarea sau ștergerea datelor, atunci când există un temei legal pentru asta.
- Urmărește eventualele tentative de deschidere a unor conturi, credite sau contracte în numele tău.
- Fii atent la mesaje care folosesc date reale despre tine — pot proveni din informații deja expuse.
- Depune plângere la Poliție dacă apare o tentativă de furt de identitate sau un prejudiciu concret.

Situația D. Calculatorul sau telefonul tău se comportă suspect

- Deconectează dispozitivul de la internet.
- Nu șterge imediat toate fișierele și nu reinstala sistemul înainte de a păstra dovezile.
- Folosește un alt dispozitiv pentru schimbarea parolelor.
- Actualizează sistemul și aplicațiile, apoi rulează o scanare cu o soluție de securitate actualizată.
- Pentru un calculator de firmă, contactează imediat administratorul IT și nu conecta backupurile la un dispozitiv posibil infectat.

Pe cine contactezi în România în caz de urgență (atac cibernetic)

Instituție	Rol și date de contact
Banca unde ai deschis contul	Prima instituție de contactat dacă există risc financiar. Folosește numărul de pe spatele cardului, din aplicația oficială sau de pe site-ul oficial al băncii — niciodată numărul primit într-un mesaj suspect.
Directoratul Național de Securitate Cibernetică	Linia națională gratuită 1911 (non-stop, din orice rețea din România) pentru consiliere imediată. Raportare oficială online prin platforma PNRISC: pnrisc.dnsc.ro , sau prin e-mail la alerts@dnsc.ro . Raportarea la DNSC nu înlocuiește o plângere penală.
Poliția Română	Pentru plângere penală atunci când au fost furați bani, ți-a fost folosită identitatea, ai fost șantajat sau ai fost convins să instalezi o aplicație de acces la distanță; sesizare la orice secție de poliție sau online, pe portalul politiaromana.ro (secțiunea Cybercrime / petiții sau petitii@politiaromana.ro). Pentru pericol imediat: 112.
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal	Pentru plângeri legate de scurgeri de date sau utilizarea abuzivă a datelor tale personale de către o companie sau instituție: anspdc.ro (dataprotection.ro). Înainte de plângere, e util să contactezi în scris organizația și să păstrezi răspunsul primit.

DE REȚINUT



Raportarea la DNSC (1911 sau pnrisc.dnsc.ro) nu înlocuiește plângerea penală la Poliție — cele două demersuri sunt complementare și e bine să le faci pe amândouă dacă ai suferit un prejudiciu.

Model de mesaj către bancă sau echipa de suport

Subiect: Raportare urgentă - posibilă compromitere a contului

Bună ziua,

La data de **[DATA]**, în jurul orei **[ORA]**, este posibil să fi fost victima unei tentative de fraudă (am introdus date pe o pagină frauduloasă / am transmis un cod de verificare / am observat un acces neautorizat).

Contul sau serviciul afectat: [Contul curent / Numărul de telefon / Adresa de e-mail]

Activitatea suspectă observată: [Describe pe scurt: ex. am observat o tranzacție necunoscută de X lei / am fost sunat de cineva care a pretins că e de la bancă].

Pentru a preveni eventualele pagube, vă rog urgent să:

blocați temporar accesul sau instrumentul de plată afectat (cardul);

verificați conectările și operațiunile recente de pe contul meu;

închideți sesiunile neautorizate;

îmi comunicați pașii următori de securizare și numărul de înregistrare al acestei sesizări.

Menționez că am păstrat capturile de ecran și dovezile disponibile (SMS-uri, linkuri) pe care vi le pot pune la dispoziție.

Vă mulțumesc,

[Numele tău complet]

[Număr de telefon]

[Număr client - dacă este necesar/cunoscut]



[!] ATENȚIE

Nu include niciodată parola, PIN-ul cardului sau codurile de autorizare (OTP) în acest mesaj. Nici măcar banca nu are nevoie de ele pentru a bloca un cont sau a identifica o fraudă.

Regula de aur: oprește-te trei secunde, verifică separat. Nicio urgență reală nu justifică transmiterea parolei sau a codului tău. Nu ești singurul vizat — aceste incidente au fost recunoscute public de autorități. Cel mai bun răspuns este calmul, verificarea și raportarea rapidă — nu intra în panică.

DE REȚINUT: STOP - VERIFICĂ - PROTEJEAZĂ

- 1. NU TE GRĂBI.** Mesajele despre blocarea contului, amenzi sau penalizări pot fi false.
- 2. NU ACCESA LINKUL.** Intră direct în aplicația oficială sau tastează manual adresa instituției.
- 3. NU TRANSMITE CODURI.** Parola, PIN-ul și codul OTP sunt doar pentru tine.
- 4. BLOCHEAZĂ ȘI SCHIMBĂ.** Dacă ai introdus datele, blochează cardul și schimbă parolele.
- 5. RAPORTEAZĂ.** Contactează banca, DNSC, Poliția Română sau ANSPDCP.