

GHID

Combaterea impersonării conturilor de social media

 **NOIEMBRIE 2025**

Prezentul ghid este destinat **instituțiilor publice din România** și vizează sprijinirea specialiștilor din compartimentele de comunicare instituțională, care gestionează prezența instituției în *social media*, oferind recomandări pentru **prevenirea preluării neautorizate a elementelor de identitate vizuală a conturilor instituției**. Ghidul poate fi util și **persoanelor care ocupă funcții de demnitate publică**.

Măsurile cuprinse în prezentul ghid au ca scop combaterea fenomenului cunoscut drept *impersonare a conturilor* care utilizează identitatea vizuală a anumitor instituții publice sau a unor persoane cu funcții de demnitate publică pentru transmiterea de conținut *fake news*, dezinformare, tentative de fraudă etc.

CUPRINS

1. Introducere	1
1.1 Cadrul legislativ european	1
1.2 Cadrul legislativ național.....	2
2. Platforme online.....	3
2.1 Platformele online foarte mari (VLOPs) și motoarele de căutare online foarte mari (VLOSEs)	3
2.2 Alte platforme relevante non-VLOPs	3
3. Identificarea conturilor false	4
3.1 Indicatori	4
3.2 Instrumente de verificare a conturilor	5
4. Documentarea.....	6
4.1 Evaluarea riscului.....	6
4.2 Documentare internă	6
5. Raportarea	7
5.1 Procesul de raportare.....	7
5.2 Exemple de mecanisme de raportare.....	7
5.3 Plângere către ANCOM	11
6. Măsuri de prevenire	12
6.1 Proactivitate și monitorizare continuă	12
6.2 Verificarea conturilor	12
6.3 Recomandare cu privire la stabilirea politicilor și procedurilor interne de gestionare a identității în mediul online.....	12
6.4 Instruirea internă a personalului.....	12
6.5 Comunicarea publică	12
7. Cooperare interinstituțională	13

1. Introducere

În contextul actual, caracterizat de creșterea exponențială a utilizării tehnologiilor digitale, prezența online a instituțiilor publice constituie un element esențial pentru comunicarea transparentă și eficientă cu cetățenii. Odată cu creșterea utilizării rețelelor sociale și a serviciilor digitale, a crescut și riscul apariției conturilor false care impersonează conturile oficiale ale instituțiilor publice și ale persoanelor care ocupă funcții de demnitate publică.

Impersonarea conturilor oficiale ale unor instituții publice, realizată prin preluarea neautorizată a identității vizuale a acestora, poate avea ca scop acțiuni precum:

- ✓ dezinformare: paginile răspândesc știri false și informații care prezintă realitatea în mod eronat/distorsionat, folosindu-se de numele instituțiilor oficiale;
- ✓ escrocherii și fraudă financiară: prin intermediul conturilor false care aparent provin de la instituții publice sunt derulate campanii de colectare a datelor personale și de obținere a unor beneficii financiare;
- ✓ furt de identitate: datele personale colectate pot fi folosite în activități cu caracter infracțional;
- ✓ afectarea încrederii cetățenilor în comunicarea publică oficială.

Prezentul ghid oferă un cadru metodologic și practic pentru identificarea și raportarea conturilor false îndeosebi în conformitate cu termenii și condițiile platformelor online.

Astfel, în cele ce urmează vor fi descrise metode concrete pentru identificarea conturilor false, va fi detaliat pas cu pas procesul de raportare a conturilor false către platformele online, vor fi indicate măsuri de urgență și proceduri de escaladare aplicabile în situații de natură critică ce pot afecta încrederea publică, ordinea publică sau chiar securitatea națională și vor fi prezentate măsuri pentru securizarea conturilor oficiale, formarea și educarea personalului, precum și monitorizarea continuă.

Combaterea fenomenului impersonării conturilor oficiale trebuie să fie preocuparea tuturor autorităților sau instituțiilor publice pentru a-și proteja identitatea în mediul digital și a putea acționa prompt împotriva conținutului difuzat prin intermediul acestor conturi neoficiale.

Instrumente utile pentru protejarea identității digitale și recuperarea conturilor de *social media* pot fi consultate și în „[Ghidul de protejare și recuperare conturi de social media](#)”, elaborat de Directoratul Național de Securitate Cibernetică (DNSC), precum și în materialul „[Deepfake – Ghid pentru organizații](#)”, care abordează un alt fenomen îngrijorător ce pune în pericol securitatea și reputația organizațiilor.

1.1 Cadrul legislativ european

Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul DSA) impune³ ca toți furnizorii de servicii intermediare să includă, în condițiile lor generale de utilizare, informații⁴ cu privire la orice restricții pe care le impun în legătură cu utilizarea serviciului lor în ceea ce privește informațiile furnizate de destinatarii serviciului. Informațiile respective sunt prezentate într-un limbaj clar, simplu, inteligibil, accesibil și lipsit de ambiguitate și se pun la dispoziția publicului într-un format ușor accesibil și care poate fi citit automat.

În aplicarea și asigurarea respectării restricțiilor menționate, furnizorii de servicii intermediare trebuie să acționeze în mod diligent, obiectiv și proporțional, ținând seama în mod corespunzător de

¹ <https://www.dnsc.ro/vezi/document/dnsc-ghid-retele-sociale-ro>

² <https://www.dnsc.ro/deepfake/>

³ Art. 14 din Regulamentul DSA.

⁴ Informațiile respective includ informații cu privire la politicile, procedurile, măsurile și instrumentele utilizate în scopul moderării conținutului, inclusiv procesul decizional algoritmic și verificarea de către o persoană, precum și cu privire la regulamentul de procedură al sistemului lor intern de soluționare a plângerilor.

drepturile și interesele legitime ale tuturor părților implicate, inclusiv de drepturile fundamentale ale destinatarilor serviciului, cum ar fi libertatea de exprimare, libertatea și pluralismul mijloacelor de informare în masă și alte drepturi fundamentale.

În plus, Regulamentul DSA impune⁵ furnizorilor de servicii de găzduire, inclusiv platformelor online, obligația de a institui mecanisme care să-i permită oricărei persoane fizice sau entități (destinatarii serviciilor) să notifice acestor furnizori prezența în cadrul serviciului lor a anumitor informații pe care persoana sau entitatea respectivă le consideră a constitui *conținut ilegal*⁶.

Suplimentar, Regulamentul DSA mai impune⁷ doar platformelor online obligația de a oferi destinatarilor serviciului, inclusiv persoanelor fizice sau entităților care au transmis o notificare, pe o perioadă de cel puțin șase luni de la data deciziei menționate la prezentul alineat, acces la un sistem intern eficace de soluționare a plângerilor, care să le permită acestora să depună plângeri pe cale electronică și în mod gratuit, în legătură cu deciziile luate de furnizorul platformei online la primirea unei notificări sau în legătură cu următoarele decizii luate de furnizorul platformei online pe motiv că informațiile furnizate de destinatari constituie conținut ilegal sau sunt incompatibile cu condițiile lor generale de utilizare:

- a) deciziile de a elimina sau nu informațiile, de a bloca sau nu accesul la acestea ori de a restrânge sau nu vizibilitatea lor;
- b) deciziile de a suspenda sau nu ori de a sista sau nu furnizarea serviciului către destinatari, integral sau parțial;
- c) deciziile de a suspenda sau nu ori de a închide sau nu contul destinatarilor;
- d) deciziile de a suspenda sau nu, de a sista sau nu ori de a restricționa sau nu în alt mod capacitatea de a monetiza informațiile furnizate de destinatari.

1.2 Cadrul legislativ național

În România, pentru aplicarea Regulamentului DSA a fost adoptată [Legea nr. 50/2024](#), iar în baza acesteia Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) a fost desemnată coordonator al serviciilor digitale (DSC) la nivel național, având atribuțiile stabilite de art.51 din Regulamentul DSA.

Atribuțiile ANCOM se exercită în raport de *furnizorii de servicii intermediare din România*⁸, iar sesizările care privesc respectarea Regulamentului DSA de către furnizori care nu au sediul în România sau care nu și-au desemnat reprezentantul legal în România sunt de competența *coordonatorului serviciilor digitale din țara de stabilire*⁹ sau de competența Comisiei Europene, după caz.

⁵ Art. 16 din Regulamentul DSA.

⁶ Art. 3 lit. h) din Regulamentul DSA.

⁷ Art. 20 din Regulamentul DSA.

⁸ Art. 4 alin. (1) lit. d) din Legea nr. 50/2024.

⁹ Art. 3 lit. n) din Regulamentul DSA.

2. Platforme online

2.1 Platformele online foarte mari (VLOPs) și motoarele de căutare online foarte mari (VLOSEs)

Conform Regulamentului DSA, VLOPs și VLOSEs sunt acele platforme online ori motoare de căutare online care au peste 45 de milioane de utilizatori activi lunar în Uniunea Europeană (UE). Acestea trebuie să respecte cele mai stricte norme ale Regulamentului DSA.

Nr. crt.	VLOP	Nr. crt.	VLOP
1	AliExpress	13	Shein
2	Amazon Store	14	Snapchat
3	Apple AppStore	15	Stripchat
4	Booking.com	16	Temu
5	Facebook	17	TikTok
6	Google Maps	18	Wikipedia
7	Google Play	19	X (fost Twitter)
8	Google Shopping	20	XNXX
9	Instagram	21	Xvideos
10	LinkedIn	22	YouTube
11	Pinterest	23	Zalando
12	PornHub		

Cu privire la VLOSEs, Comisia Europeană a identificat două platforme care se încadrează în această categorie: Google Search și Bing.

Informații actualizate cu privire la VLOPs și VLOSEs pot fi consultate pe site-ul¹⁰ Comisiei europene, în [secțiunea dedicată](#).

2.2 Alte platforme relevante non-VLOPs

Nr. crt.	Platformă online	Descriere
1	Reddit	Forum de discuții cu comunități multiple
2	Dailymotion	Platformă video alternativă
3	Vimeo	Platformă pentru conținut video profesional
4	Twitch	Streaming live pentru gaming și conținut divers
5	Discord	Platformă de comunicare pentru comunități
6	Telegram	Aplicație de mesagerie cu canale publice

¹⁰ <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

3. Identificarea conturilor false

Un cont fals care impersonează contul oficial al unei instituții publice poate fi identificat analizând atât indicatorii vizuali (steme, embleme, denumire, acronim etc.), cât și caracteristicile comportamentale (frecvența și tipul postărilor, interacțiunea cu comunitatea).

3.1 Indicatori

Elemente de identitate

- ✓ **Denumire/acronim identice;**
- ✓ **Denumire/acronim similare** dar cu modificări subtile (ex: în cazul Ministerului X, denumirea este „*Ministerul.X*” ori au fost operate schimbări minore: *Ministeru1 X*);
- ✓ **Domenii suspecte în cazul în care acestea apar asociate cu contul rețelei sociale**, precum *.tk*, *.ml*, *.ga* în loc de ***.gov.ro*** sau utilizarea „*ministerul.X.ro*”, în loc de ***ministerulx.gov.ro***;
- ✓ **Utilizarea neautorizată** a elementelor de identitate vizuală oficiale (stemă, emblema, logo etc.¹¹);
- ✓ **Conturi false în numele persoanelor care ocupă funcții de demnitate publică.**

Caracteristici comportamentale

- ✓ **Activitate online** în intervale orare care nu corespund cu programul oficial al instituției sau fusul orar al României;
- ✓ **Postări repetitive** cu același conținut/conținut similar la intervale scurte;
- ✓ **Număr neverosimil de urmăritori** raportat la istoricul activității;
- ✓ **Lipsa interacțiunii autentice** cu comunitatea.

Tipologii frecvente de *typo-uri*

- ✓ **Înlocuirea literelor** (ex: „0” în loc de „o”, „1” în loc de „l” etc.);
- ✓ **Adăugarea** de caractere suplimentare („*mMinisterul*” în loc de „*ministerul*”, „*adminisRtația*” în loc de „*administrația*” etc.);
- ✓ **dublarea unor caractere** (ex. „*goovernul*” în loc de „*guvernul*”);
- ✓ **inversarea unor caractere** (ex: „*poliita*” în loc de „*politia*” etc.);
- ✓ **eliminarea unor caractere** (ex. „*misterul*”, „*ministeru*”, „*pefectura*”);
- ✓ **introducerea** unor separatori, precum puncte, liniuțe etc. („*primaria-municipiului-x*” în loc de „*primariamunicipiuluix*”, „*minister_oficial*”, „*prefectu_ra*” etc.);
- ✓ **folosirea** extensiilor de cuvinte („*officialro*”, „*Ministerul X Real*” etc.);
- ✓ **prefixe/sufixe:**
 - **prefixe:** „*oficial-primaria*”, „*real-ministerul*”;
 - **sufixe:** „*primaria-romania*”, „*ministerul-gov*”;
 - **cifre:** „*primaria2*”, „*politia1*”.

¹¹ Aceste elemente – *stemă, emblema, logo* – pot fi protejate ca marcă înregistrată, iar în unele cazuri – simboluri naționale – sunt protejate prin lege.

3.2 Instrumente de verificare a conturilor

Pentru verificarea unor imagini considerate a nu fi autentice sau domenii suspecte asociate conturilor de *social media*, pot fi utilizate instrumente, cum ar fi:

- ✓ **Reverse Image Search** – Exemple: Google Images, TinEye pentru verificarea fotografiilor de profil;
- ✓ **Analiza metadatelor** pentru identificarea sursei imaginilor;
- ✓ **Verificarea domeniilor de internet asociate contului** prin servicii WHOIS;
- ✓ **Monitorizarea mediatică** a instituției pe diverse platforme.

4. Documentarea

Protejarea identității digitale nu este numai responsabilitatea platformelor de *social media*, ci necesită implicarea activă a deținătorului real al contului, atât pentru apărarea reputației, cât și pentru combaterea dezinformării, fraudelor sau răspândirii de fake news și, nu în ultimul rând, pentru păstrarea încrederii cetățenilor.

4.1 Evaluarea riscului

În situația în care se constată impersonarea contului instituției publice recomandăm o analiză de urgență a efectelor și a gravității situației. Această analiză trebuie să fie realizată împreună cu personalul nominalizat să gestioneze prezența în mediul online a instituției.

Riscuri posibile

- ✓ diseminarea de informații false în numele instituției;
- ✓ solicitarea de date personale de la cetățeni;
- ✓ utilizarea neautorizată a elementelor de identitate;
- ✓ imitarea fără impact asupra activității instituționale.

În situația în care se constată o situație ce necesită o reacție imediată, ținând cont de rapiditatea cu care se propagă informația în mediul online, cum ar fi un răspuns oficial privind un fake news sau o alertă pentru cetățeni privind un risc ce îi afectează, se vor lua măsurile necesare fără întârziere.

4.2 Documentare internă

- ✓ **Capturi de ecran** ale contului fals;
- ✓ **URL-uri și identificatori** unici ai contului;
- ✓ **Descrierea detaliată** a modului de preluare a elementelor de identitate vizuală;
 - lipsa verificării (ex: *blue checkmark*);
 - cont creat recent/cont care și-a schimbat denumirea;
 - număr redus de urmăritori;
 - conținut replicat de pe pagina oficială;
 - promovarea unor practici frauduloase (ex: donații, solicitarea unor sume de bani, investiții, concursuri etc.);
 - greșeli gramaticale;
 - modificarea elementelor de identitate vizuală;
 - campanii de colectare a datelor personale;
 - distribuirea unor URL-uri suspecte;
- ✓ **Evaluarea impactului** asupra instituției și cetățenilor pe baza următorilor indicatori:
 - menționări/trimiteri în social media/mass-media;
 - promovarea unor teme controversate, nespecifice instituției;
 - promovarea unor conflicte ori controverse;
 - asocieri cu evenimente naționale/internaționale;
 - alerte/sesizări primite de la utilizatori ai platformelor online.
- ✓ **Dovezi comparative** cu contul oficial;
 - indicarea conturilor oficiale;
 - adresa de e-mail;
 - numere de telefon.

5. Raportarea

5.1 Procesul de raportare

Este indicat ca raportarea contului fals să se realizeze rapid, de pe contul oficial al instituției, direct către platforma online pentru a întreprinde măsurile necesare. La aceste demers se vor atașa inclusiv informațiile documentate, pentru a aduce la cunoștință platformei online situațiile identificate.

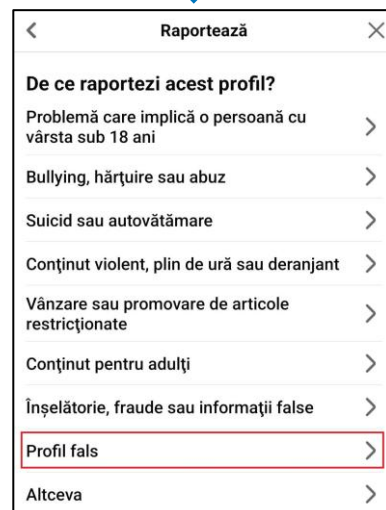
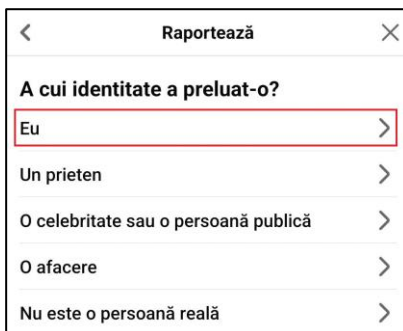
1. Folosiți mecanismul de raportare al platformei detaliat în exemplele de la 5.2;
2. Furnizați documentația completă (link oficial, dovezi care atestă calitatea persoanei care face raportarea);
3. Așteptați răspunsul platformei;
4. Faceți apel dacă platforma refuză și salvați capturile de ecran;
5. Puteți depune o plângere la ANCOM în cazul în care:
 - platforma nu răspunde;
 - răspunsul platformei este inadecvat sau incomplet;
 - platforma nu oferă acces la un sistem intern de soluționare a plângerilor;

Observație: plângerile la ANCOM se depun însoțite de prezentarea în detaliu a etapelor parcurse în raport de platformă, precum și a oricăror elemente probatorii pe care se poate sprijini înaintarea sesizării către *coordonatorul serviciilor digitale din țara de stabilire*.

5.2 Exemple de mecanisme de raportare

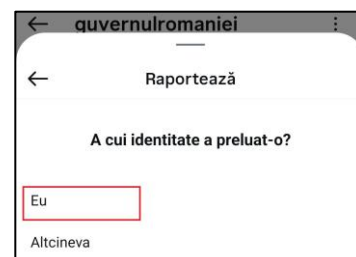
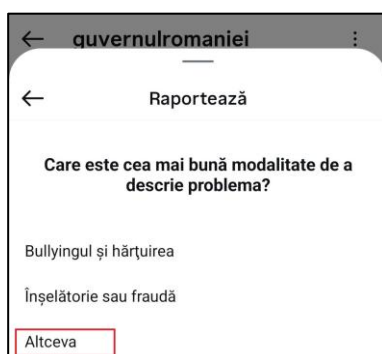
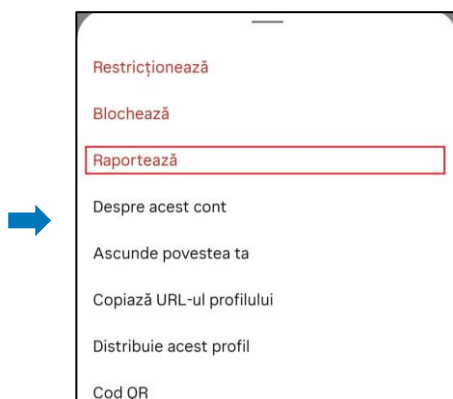
Facebook (Meta)

2. accesarea contului suspect/fals;
3. click pe „...” (trei puncte) → „**Raportează pagina/profilul**” → “Ceva despre acest profil”
4. selectarea „**Profil fals**”
5. selectare „**Eu**” la întrebarea “a cui identitate a fost preluată”
6. furnizarea documentației necesare:
 - informații despre instituție;
 - dovada reprezentării legale;
 - capturi de ecran comparative.



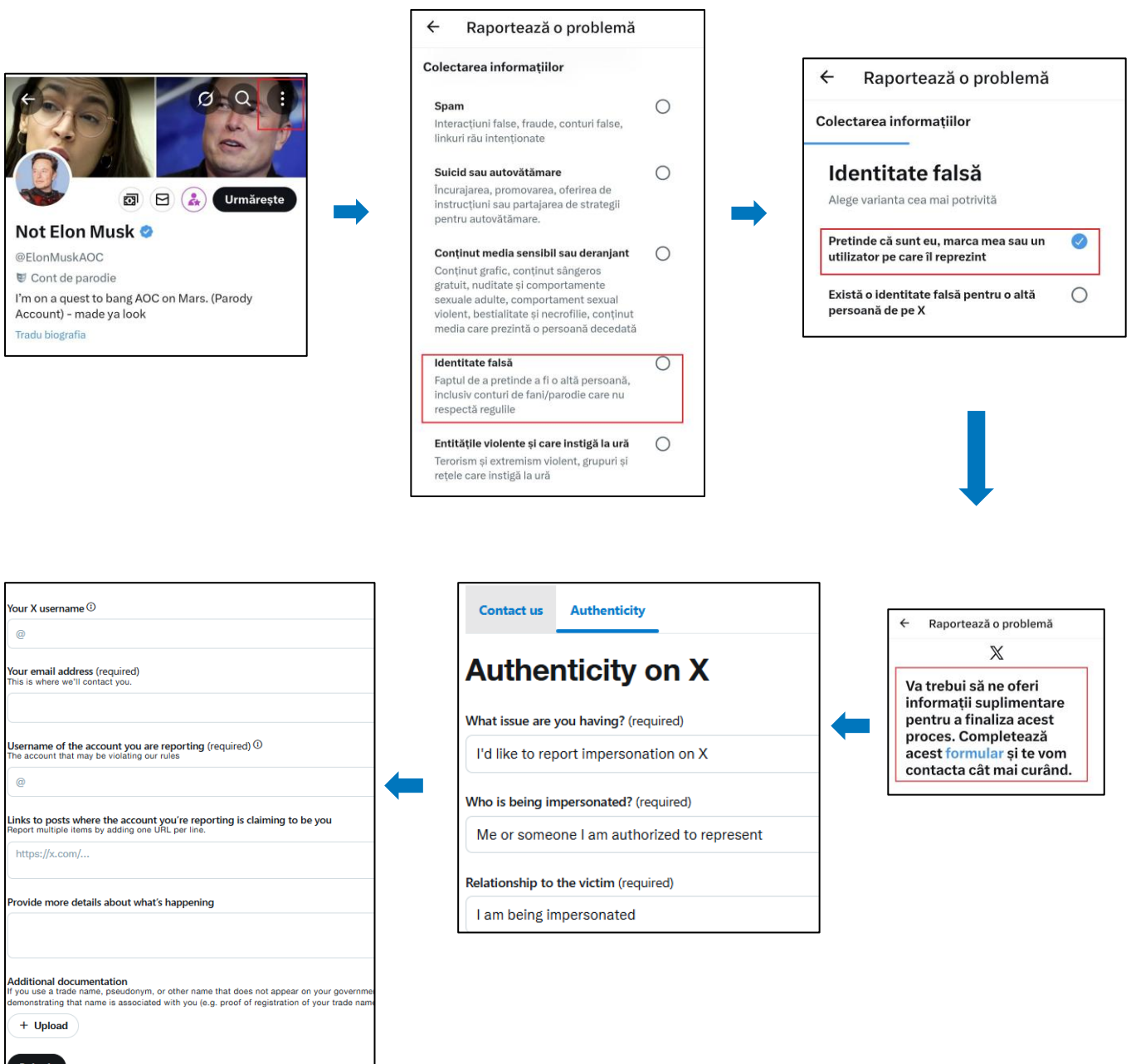
Instagram (Meta)

1. accesarea profilului fals;
2. click pe "..." → „**Raportează**”;
3. selectare „**Ceva despre acest cont**” → „**Pretinde că este altcineva**” → selectare „**Eu**” la întrebarea “a cui identitate a fost preluată” → introducerea entității impersonate;
4. furnizarea datelor solicitate;



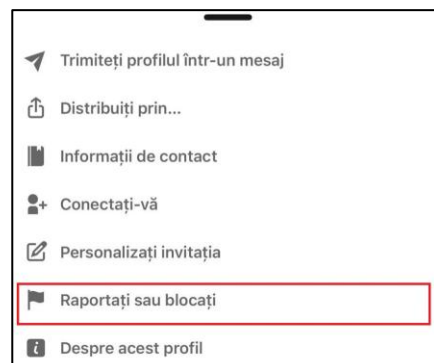
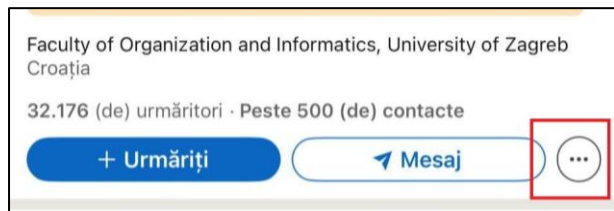
X (fost Twitter)

1. accesarea contului suspect/fals;
2. clic pe „...” → „**Raportează**”;
3. selectarea „**Identitate falsă**”, iar ulterior „**pretinde că sunt eu, marca mea sau un utilizator pe care îl reprezint**”;
4. Completarea formularului detaliat cu:
 - informații despre instituție;
 - dovezile de impersonare;
 - linkuri către conturile oficiale.



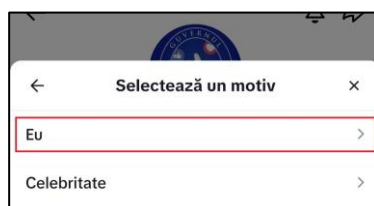
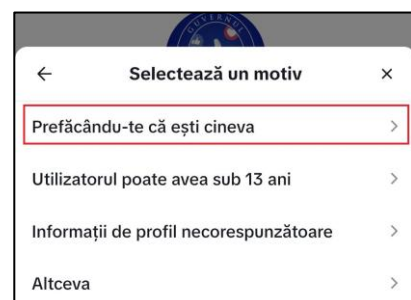
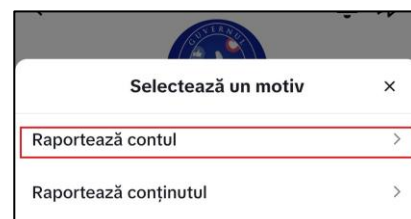
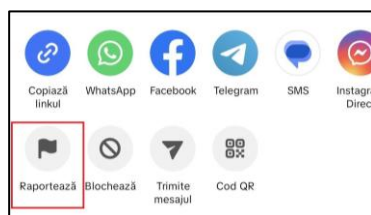
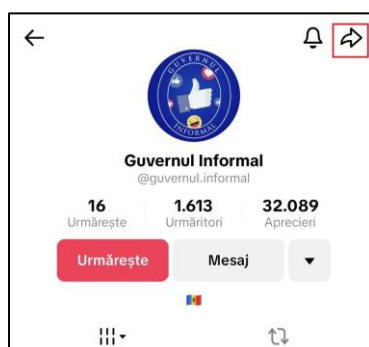
LinkedIn

1. accesarea paginii false
2. click pe „...” → „**Raportați sau blocați**” → **“Raportați pe sau întregul cont”** → **“Această persoană a preluat o altă identitate”**;
3. trimiteți raportarea.



TikTok

1. accesarea contului suspect/fals;
2. clic pe „share” (colțul dreapta sus) → „**Raportează**”;
3. selectarea „**Prefăcându-te că ești cineva**” → selectare **“Eu”**;
4. urmați instrucțiunile.



5.3 Plângere către ANCOM

În situația în care se constată că platforma online nu și-a respectat obligațiile stabilite prin Regulamentul DSA privind primirea și soluționarea plângerilor, se poate formula o plângere la ANCOM, coordonatul serviciilor digitale din România. Plângerea trebuie însoțită de următoarele:

- ✓ **capturi de ecran** ale contului fals;
- ✓ **dovada raportării** către platformă;
- ✓ **răspunsul platformei**, dacă există;
- ✓ **impactul estimat** asupra entității;
- ✓ **alte dovezi relevante** (comentarii, distribuiri etc.);
- ✓ **sunt aplicabile și unele precizări din secțiunea 5.1.**

6. Măsuri de prevenire

6.1 Proactivitate și monitorizare continuă

Măsuri ce pot fi luate pentru a preîntâmpina impersonarea contului:

- ✓ configurarea alertelor *Google* pentru numele instituției;
- ✓ monitorizarea menționărilor pe platformele sociale, inclusiv prin implementarea unor automatizate;
- ✓ verificarea periodică a conturilor care fac trimitere la denumirea/acronimul actual sau istoricul instituției;
- ✓ realizarea unor rapoarte periodice de monitorizare;
- ✓ adaptarea la modificările termenilor și condițiilor platformelor online;
- ✓ deprinderea de bune practici.

6.2 Verificarea conturilor

- **Solicitarea verificării oficiale** de către platforme (obținerea bifă/badge de verificare etc.);
- **Actualizarea constantă** a informațiilor de contact și documentației, precum și publicarea pe pagina oficială de internet a instituției a unor linkuri către conturile oficiale.

6.3 Recomandare cu privire la stabilirea politicilor și procedurilor interne de gestionare a identității în mediul online

1. **Desemnarea responsabililor** pentru gestionarea și inventarierea tuturor conturilor oficiale de social media ale instituției;
2. **Definirea procedurilor** de publicare și moderare;
3. **Implementarea unui calendar** de postare și monitorizare;
4. **Stabilirea protocolului** de răspuns în situații de criză.

6.4 Instruirea internă a personalului

- Modalitatea de răspuns adecvat în cazurile de preluare a identității vizuale;
- Instruire și conștientizare cu privire la identificarea conturilor false;
- Proceduri de gestionare a incidentului identificat;
- Utilizarea instrumentelor de monitorizare.

6.5 Comunicarea publică

- ✓ **anunțuri oficiale** pe canalele verificate;
- ✓ **alertarea cetățenilor** despre existența contului fals;
- ✓ **îndrumarea către surse autentice** de informare;
- ✓ **actualizări constante** asupra progresului investigației.

7. Cooperare interinstituțională

Cooperarea interinstituțională nu este doar un mecanism de lucru, ci o condiție esențială pentru consolidarea încrederii cetățenilor în autoritățile sau instituțiile publice.

Prevenirea și combaterea eficientă a fenomenul impersonării conturilor oficiale, dar și protejarea integrității comunicării publice poate fi realizată prin acțiuni de cooperare și coordonare, cum ar fi:

- schimb de informații între instituții;
- susținerea reciprocă a campaniilor de informare prin distribuirea mesajelor;
- alertarea reciprocă cu privire la conținut ilegal și/sau impersonarea conturilor;
- coordonarea informării publice în situația identificării unor situații cu impact interinstituțional.



Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Strada Delea Nouă nr.2, sector 3, 030925 București

Tel: 0372 845 400 / 0372 845 454; Fax: 0372 845 402

ancom@ancom.ro www.ancom.ro

