



SMART ONLINE = SAFE OFFLINE

Siguranța ta online

Ghidul adolescentului: cum recunoști capcanele, cum îți protejezi conturile și cui ceri ajutor atunci când ceva nu e în regulă.

Nicholas Cârstoiu

Ghid gratuit pentru elevii claselor VII-XII · Ediția în limba română · Actualizat la octombrie 2026

Despre acest ghid

Ai în mână un ghid scris pentru tine, nu pentru specialiști. Nu trebuie să știi programare și nici să fii pasionat de calculatoare ca să îl înțelegi. Aproape tot ce urmează e despre oameni: despre cei care încearcă să te păcălească, despre trucurile pe care le folosesc și despre deciziile mici, de câteva secunde, care fac diferența dintre un cont furat și unul în siguranță. Poți să îl citești de la cap la coadă sau poți sări direct la capitolul de care ai nevoie; fiecare se încheie cu o secțiune **Pe scurt**.

Ghidul pornește de la cursul SMART ONLINE = SAFE OFFLINE, pe care îl prezint gratuit în școlile din București. Aici am păstrat ce contează cel mai mult, am verificat din nou fiecare cifră și am adăugat subiectele care au devenit importante pentru adolescenți: sextorsiunea, imaginile false create cu AI, chatboturile, grupurile care cer „probe” și furtul conturilor prin coduri.

Despre programul SMART ONLINE = SAFE OFFLINE

Acest ghid face parte din programul gratuit SMART ONLINE = SAFE OFFLINE, pe care Nicholas Cârstoiu îl oferă școlilor gimnaziale și liceelor din București, pentru elevii claselor VII-XII. Programul este gratuit pentru școli, elevi, profesori și părinți. Detalii: www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html

Materialul de bază al cursului a fost dezvoltat inițial de Alexandru Cârstoiu, specialist în securitatea informației, și adaptat de Nicholas pentru adolescenți.

Ghidul și platforma TRUST // NO TRUST se completează. Aici găsești explicațiile și pașii pe care îi poți păstra la îndemână. Pe platformă exersezi deciziile în situații fictive, înainte să ai nevoie de ele în realitate. Ambele sunt gratuite, pentru ca accesul la informații de siguranță să nu depindă de posibilitatea de a plăti.

Fiecare cifră are sursa notată sub ea, iar lista completă e la final. Dacă găsești o cifră care între timp s-a schimbat, scrie-mi. Ediție revizuită pe baza surselor disponibile la 23 octombrie 2026.

Ai nevoie de ajutor chiar acum?

112 dacă tu sau altcineva sunteți în pericol imediat. **119** pentru abuz, exploatare sau neglijare a unui copil, gratuit și non-stop. **116 111** dacă vrei să vorbești cu un consilier. Toate serviciile și pașii sunt în [capitolul 10](#).

Cuprins

	Despre acest ghid	2
	Despre autor	4
1	De ce contează	5
2	Cum lucrează atacatorii	7
3	Capcanele clasice	11
4	Oameni care vor să te manipuleze	19
5	Conturile și telefonul tău	27
6	Gaming sigur	31
7	Social media și creierul tău	35
8	Deepfake și inteligența artificială	38
9	Escrocheriile virale	42
10	Dacă ți s-a întâmplat	45
11	Tridentul: de ce cursul în școli	49
	Surse	50
	Contact, drepturi de autor și siguranță	53

Despre autor



Salut, sunt **Nicholas Cârstoiu**. Am 17 ani, sunt elev în clasa a XI-a la Liceul Româno-Finlandez din București și joc baschet de performanță la CSU ASE București. La liceu sunt antrenor secund la echipele de juniori.

Din 2023 sunt membru al Boardului Copiilor UNICEF România, din 2024 fac parte din Consiliul Consultativ al Copiilor din Primăria Municipiului București, iar în 2026 am devenit Ambasador pentru România al United Citizens of Europe. Tot în 2026 am primit Premiul I „Tânăr lider în voluntariat” la Gala Voluntarului Social România.

Siguranța online nu e un subiect nou pentru mine. Am creat programul SMART ONLINE = SAFE OFFLINE, cu care merg de trei ani prin școlile din București, și The Fake News Factory, un proiect de educație media care a câștigat două premii în 2026. Acum construiesc TRUST // NO TRUST, o platformă gratuită în care adolescenții exersează deciziile care îi țin în siguranță, cu care particip la concursul Lider European 2026.

„Generația mea nu trebuie să fie cea mai ușor de păcălit online. Putem fi cei mai greu de păcălit.”

Hai să mă cunoști mai bine!

www.looksmart.ro/nicholas

CAPITOLUL 1

De ce contează

Viața ta se mută tot mai mult pe ecran: prietenii, școala, jocurile, banii, chiar și primele iubiri. Exact acolo te caută și cei care vor să profite de tine.

Când auzi „securitate cibernetică”, probabil te gândești la un hacker în glugă care sparge parole cu viteza luminii. Realitatea e mult mai banală și tocmai de aceea mai periculoasă. Multe atacuri nu încep cu un calculator, ci cu un om: un mesaj care te grăbește, un premiu prea frumos, o voce cunoscută la telefon, un „prieten” nou care te înțelege mai bine decât toți ceilalți.

≈ 1 din 5

copii între 12 și 17 ani care folosesc internetul, din 21 de țări, a fost victimă a exploatării sau a abuzului sexual facilitat de tehnologie, într-un singur an.

Sursa: UNICEF Innocenti, raportul Through Children's Eyes, publicat pe 3 septembrie 2026, date din cercetarea Disrupting Harm

1 din 6

elevi de 11, 13 și 15 ani, din 44 de țări din Europa, Asia Centrală și Canada, a trecut prin cyberbullying.

Sursa: OMS Europa, studiul HBSC despre cyberbullying, 27 martie 2024, date pentru 2022

2 din 5

copii participanți la studiul Salvați Copiii spun că au fost jigniți sau au primit mesaje dureroase online.

Sursa: Salvați Copiii România, comunicat de presă din 28 martie 2025

Peste 4 din 10

cazuri de abuz sau exploatare sexuală facilitată de tehnologie, din cercetarea sintetizată de UNICEF, nu au fost dezvăluite nimănui.

Sursa: UNICEF Innocenti, raportul Through Children's Eyes, publicat pe 3 septembrie 2026, date din cercetarea Disrupting Harm

Ultima cifră e poate cea mai importantă. Multe probleme cresc tocmai pentru că rămân nespuse. Dacă ți se întâmplă ceva, nu trebuie să ai toate dovezile sau toate răspunsurile ca să ceri ajutor. Iar dacă recunoști trucul la timp și știi ce faci în clipa următoare, multe dintre ele nici nu mai ajung să se întâmple.

Modelul **APDR**: patru întrebări care te apără

În acest ghid folosim patru întrebări simple, grupate sub numele APDR. Le poți aplica la orice: un cont, telefonul, pozele tale.

1. Anticipare

Ce ar putea merge prost? Cine ar vrea acces la ce am eu?

2. Prevenție

Ce fac de acum ca să nu se întâmple? Parole, setări, prudență.

3. Detectie

Cum îmi dau seama repede dacă s-a întâmplat ceva?

4. Răspuns

Ce fac în primele minute? Pe cine anunț?

Exemplu: pozele din telefonul tău

Anticipare: telefonul se poate pierde, poate fi furat sau cineva îți poate afla codul. Pozele personale ar putea ajunge la oameni care nu ar trebui să le vadă. **Prevenție:** pui un cod de deblocare de cel puțin 6 cifre, activezi copia de siguranță în cloud cu autentificare în doi pași și verifici ce aplicații au acces la galerie. **Detectie:** primești alertă când cineva intră în contul tău de pe alt dispozitiv. **Răspuns:** blochezi și ștergi telefonul de la distanță, schimbi parola contului de cloud și anunți un adult.

Ține minte ordinea. Cei mai mulți oameni se gândesc la securitate abia la pasul patru, când răul s-a produs deja. Tu poți începe cu pasul unu.

Pe scurt

- Multe atacuri se bazează pe manipularea oamenilor, nu doar pe tehnologie.
- Problemele nespuse cresc. Cere ajutor din prima zi.
- APDR: anticipezi, previi, detectezi, răspunzi.

CAPITOLUL 2

Cum lucrează atacatorii

Uită de hackerul singuratic din filme. Infraționalitatea online de azi seamănă mai mult cu o firmă, cu echipe, roluri și termene.



Atacurile mari sunt făcute de echipe, nu de un singur om.

O rețea de infractori cibernetici funcționează ca o fabrică. Fiecare echipă face un singur lucru și îl face bine. Dacă înțelegi lanțul, înțelegi și unde îl poți rupe: de multe ori, chiar la tine.

Profilerii adună informații despre ținte: ce postezi, unde mergi la școală, cum îi cheamă pe prietenii tăi, ce jocuri joci. **Echipa de penetrare** caută o cale de intrare, de cele mai multe ori un mesaj de phishing sau o parolă refolosită. **Echipa de atac** instalează programe malițioase sau preia contul. **Echipa de extragere** copiază datele, pozele și contactele. **Negociatorii** cer bani, iar **echipa de „curățenie”** șterge urmele și vinde datele mai departe.

Nu toți hackerii sunt infractori

Cuvântul „hacker” înseamnă de fapt cineva care înțelege un sistem atât de bine încât îl poate face să funcționeze altfel decât a fost gândit. Unii folosesc asta ca să fure. Alții, numiți hackeri etici, caută vulnerabilitățile ca să le repare înainte să le găsească infractorii. Marile companii îi plătesc prin programe de recompense, numite bug bounty.

Știai că?

În 2016, un băiat de 10 ani din Finlanda, Jani, a descoperit o vulnerabilitate prin care putea șterge comentariile oricui de pe Instagram. A raportat-o, iar Facebook i-a plătit 10.000 de dolari. Securitatea cibernetică este una dintre puținele meserii în care poți începe foarte devreme, cu condiția să rămâi de partea bună.

Sursa: NBC News, despre recompensa primită de un copil de 10 ani pentru o vulnerabilitate Instagram, mai 2016.

Știai că?

România are o tradiție serioasă în securitate. Bitdefender, unul dintre cele mai cunoscute antivirusuri din lume, a fost fondat la București în 2001. Iar tehnologia antivirus RAV, dezvoltată de firma românească GeCAD, a fost cumpărată de Microsoft în 2003.

De ce ar fi interesați de tine?

„N-am nimic de furat” e cea mai des întâlnită greșeală. Contul tău de Instagram poate fi folosit ca să-ți păcălească prietenii, contul de joc are skinuri care se vând, numărul tău de telefon deschide conturi de WhatsApp, iar pozele tale pot fi folosite pentru șantaj. Pentru un atacator, nu contează că ești „doar un elev”. Contează că ai acces la oameni care au încredere în tine.

Internetul are **trei straturi**

Surface web este partea pe care o găsești cu Google: pagina publică a unui restaurant, profilul public al unui influencer, videoclipurile publice de pe YouTube. **Deep web** sună misterios, dar e pur și simplu tot ce se află în spatele unei parole: inboxul tău, mesajele private, contul de la bancă al părinților, biblioteca ta de jocuri de pe Steam. Nu e nimic ilegal acolo, e zona ta privată, și exact pe ea vor atacatorii să pună mâna.

Dark web este o parte mică a internetului, accesibilă doar prin programe speciale, unde identitatea utilizatorilor e ascunsă. Are și utilizări legitime, de exemplu pentru jurnaliștii din țări fără libertate de exprimare. Dar e și locul în care se vând date furate, conturi sparte și lucruri mult mai rele.



De ce nu ai ce căuta pe dark web

Nu e un loc „cool” de explorat din curiozitate. Poți da peste conținut ilegal și traumatizant, poți descărca programe malițioase, iar unele site-uri sunt chiar capcane puse de infractori sau monitorizate de poliție. Dacă cineva îți propune să intri „doar să vezi”, răspunsul e nu. Dacă vezi un link cu conținut ilegal care implică un copil, nu îl deschide și raportează-l anonim pe linia esc_ABUZ (capitolul 10).

Pe scurt

- Infracționalitatea online e organizată ca o afacere, cu echipe și roluri.
- Unele atacuri sunt personalizate cu informații despre tine, altele sunt trimise automat la mii de oameni. În ambele cazuri, ce postezi contează.
- Deep web înseamnă conturile tale private, nu ceva ilegal. Dark web e alt lucru și nu e un loc de explorat.
- Nu ești prea mic ca să fii o țintă: ai conturi, contacte și încrederea altora.

Exercițiu: cât de ușor te găsește un profiler?

Ia-ți cinci minute și caută-te pe Google, cu numele complet între ghilimele. Apoi deschide-ți profilul de Instagram sau TikTok ca și cum ai fi un străin. Notează tot ce poate afla cineva care nu te cunoaște: școala, cartierul, sala unde te antrenezi, numele părinților sau al fratelui, ziua de naștere, programul tău zilnic.

Apoi întreabă-te: dacă un necunoscut ar avea toate aceste informații, ce mesaj credibil mi-ar putea scrie? „Salut, sunt antrenorul nou de la sală” sau „Te-a căutat diriginta, uite linkul cu orarul nou” sună mult mai convingător când vine de la cineva care știe deja detalii despre tine. Așa lucrează profilerii, și așa te poți apăra: cu cât lași mai puține indicii, cu atât e mai greu să fii păcălit.

Cum recunoști un profil fals

- Cont nou, cu puține postări, dar cu mulți urmăritori sau cu mulți prieteni comuni adăugați recent.
- Poze prea perfecte, de tip model, sau poze care apar și pe alte conturi (le poți căuta cu Google Lens).
- Îți scrie primul, te laudă mult și grăbește trecerea pe altă aplicație.
- Nu acceptă niciodată un apel video sau inventează mereu scuze.

Ce faci acum

- Fă-ți contul privat acolo unde nu ai nevoie să fie public.
- Scoate din bio școala, clasa și orașul, dacă nu sunt necesare.
- Nu posta în timp real unde ești. Postează după ce ai plecat.
- Verifică cine te urmărește și elimină conturile pe care nu le cunoști.

CAPITOLUL 3

Capcanele clasice

Phishing, mesaje false, apeluri care te grăbesc și programe care se instalează pe ascuns. Sunt vechi, dar funcționează în continuare, pentru că se adaptează mereu.



Phishing vine de la „fishing”, pescuit. Atacatorul aruncă o momeală, un email, un SMS sau un mesaj pe rețelele sociale, și așteaptă să muști. Mesajul pare să vină de la cineva de încredere: o bancă, o firmă de curierat, Instagram, școala sau un prieten. Scopul e unul singur: să dai click, să introduci parola sau un cod, ori să descarci un fișier.

Cum recunoști un mesaj de phishing

Aproape toate mesajele false folosesc aceleași câteva pârgii psihologice. Dacă înveți să le simți, nu mai contează cât de bine e făcut mesajul.

Grabă

„Contul tău va fi șters în 24 de ore.” Când ești grăbit, nu mai verifici.

Frică

„Cineva a intrat în contul tău.” Frica te face să acționezi fără să gândești.

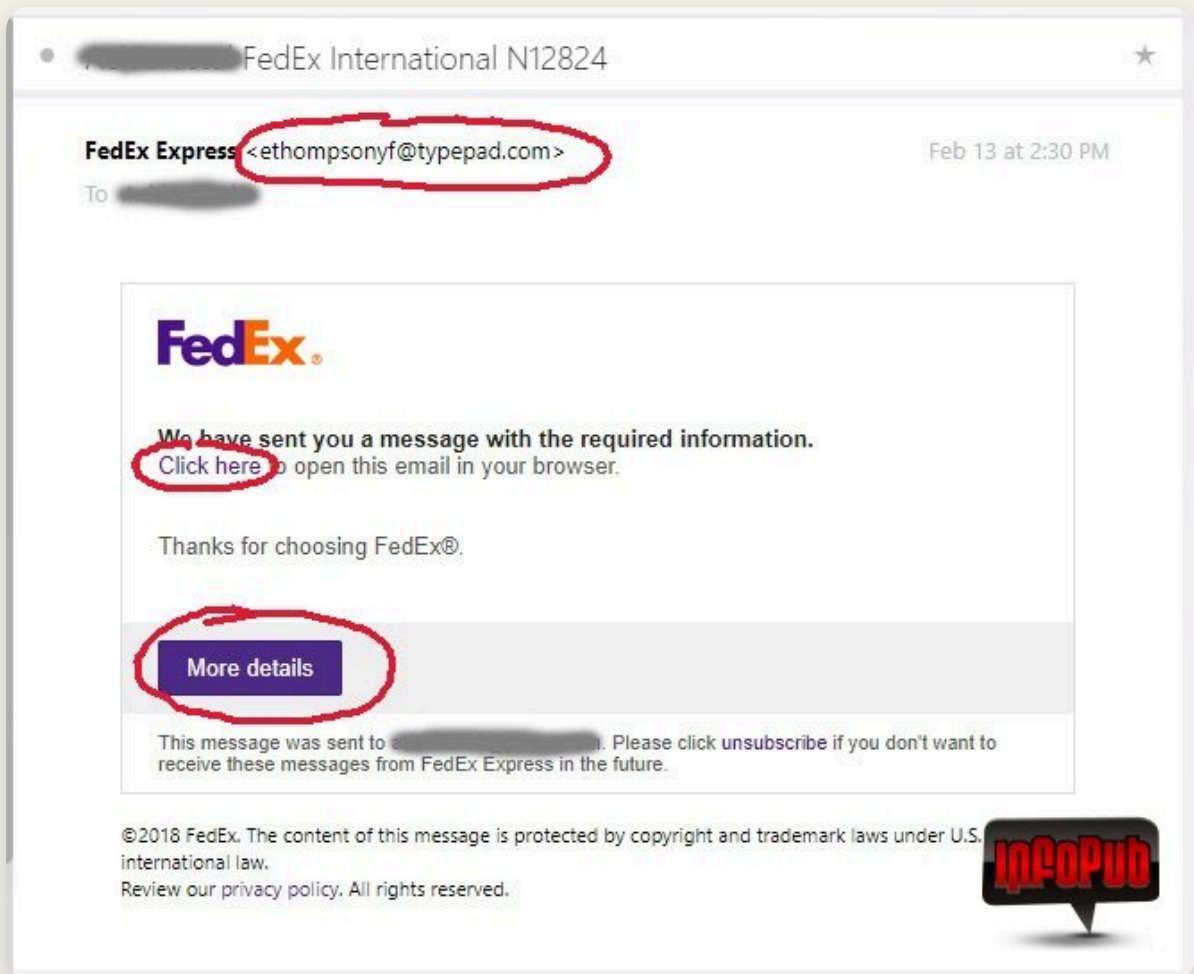
Curiozitate

„Uite ce poză cu tine circulă.” Vrei să vezi, deci dai click.

Câștig

„Ai câștigat un iPhone.” Dacă sună prea bine ca să fie adevărat, nu e.

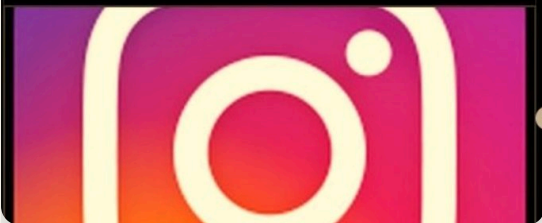
Pe lângă emoție, verifică trei lucruri concrete. Primul este adresa reală a expeditorului sau a linkului, nu numele afișat: un mesaj „de la FedEx” trimis de pe o adresă de tipul ethompsonyf@typepad.com nu e de la FedEx. Al doilea este domeniul: [instagram.com](https://www.instagram.com) e real, dar [instagram-help.buzz](https://www.instagram-help.buzz) sau [lgotyou125.xyz](https://www.lgotyou125.xyz) nu sunt. Al treilea este cererea în sine: nicio platformă serioasă nu îți cere parola sau codul primit prin SMS printr-un mesaj.



Exemplu real de phishing: numele spune FedEx, adresa spune altceva.

Este sau nu un atac?

This took me about 3 hours to make. I really hope you love it, Look: http://lGotYouThis125.xyz/g/?&ure=dnf_tweets



Mesajul: „Took me about 3 hours to make. I really hope you love it. Look: <http://lGotYouThis125.xyz/g/?&ure=...>”, primit în privat de la un prieten.

Da, este un atac. Textul e gândit să îți stârnească curiozitatea, iar linkul conține uneori chiar numele tău de utilizator, ca să pară personal. Pagina la care ajungi arată ca ecranul de logare Instagram, dar domeniul e cu totul altul. Imediat ce îți introduci parola, contul e preluat, iar același mesaj pleacă automat către toți cei care te urmăresc. De asta pare să vină de la un prieten: chiar vine din contul lui, doar că nu el l-a scris.

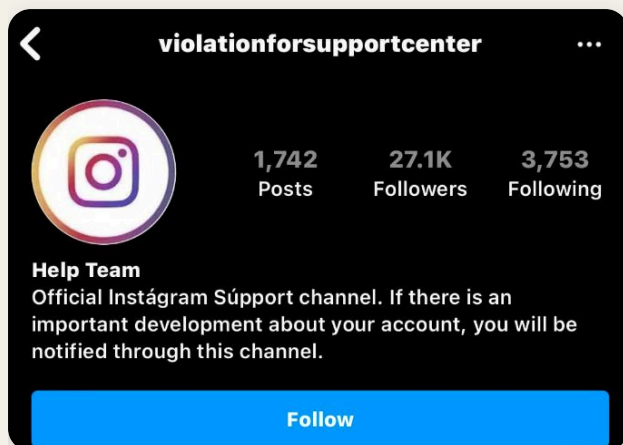
Cum verifici un link fără să-l deschizi

- Pe calculator, ține mouse-ul deasupra linkului și citește adresa care apare în colțul ecranului.
- Pe telefon, ține degetul apăsător pe link și citește adresa, fără să o deschizi.
- Citește adresa dintre „https://” și următorul „/”. Un nume cunoscut pus la început nu înseamnă că site-ul îi aparține: în „instagram.com.verificare-cont.example”, domeniul este „verificare-cont.example”, nu „instagram.com”.
- Dacă nu ești sigur, deschide direct aplicația oficială sau scrie tu adresa, nu folosi linkul.

Ce faci dacă ai dat deja click și ți-ai pus parola

- Schimbă imediat parola contului și pe a oricărui alt cont unde ai folosit-o.
- Activează autentificarea în doi pași.
- Intră la Setări, Activitate de conectare (Login Activity), și deconectează sesiunile pe care nu le recunoști.
- Anunță-ți urmăritorii să nu dea click pe mesajele trimise din contul tău.
- Dacă nu mai poți intra, folosește pagina oficială de recuperare a platformei, nu „ajutorul” care îți scrie în privat.

„Suportul” care îți scrie primul



Cont fals de „Help Team”, cu logo Instagram și mii de urmăritori.



„Last Warning: your account will be disabled.” Clasicul mesaj de frică.

Un cont care se prezintă drept echipa de suport, cu logo oficial și cifre mari la urmăritori, îți spune că ai încălcat regulile și că trebuie să-ți „confirmi” contul printr-un link. Nu verifica avertismentul prin linkul primit. Deschide direct aplicația și caută notificarea în secțiunea oficială de securitate sau de suport.

Concursurile care îți adună datele



„Giveaway alert: dă like, etichetează 3 prieteni și distribuie.” Pare inofensiv, dar fiecare pas are un rost pentru cine a creat concursul. **Like-ul** confirmă că ești un cont activ, deci te poți aștepta la și mai multe mesaje. **Etichetarea** îi expune pe prietenii tăi, care devin următoarele ținte. **Distribuirea** creează cadrul ca și alți prieteni să fie expuși. Înainte să participi, verifică dacă organizatorul e contul oficial și verificat al firmei.

SMS, apeluri și coduri



Smishing înseamnă phishing prin SMS: „Coletul tău e blocat, plătește taxa de 2 lei aici.”

Vishing înseamnă phishing prin apel vocal: cineva se prezintă de la bancă, de la poliție sau de la un operator și îți cere date „pentru verificare”. Cu inteligența artificială, vocea poate fi chiar a unei persoane pe care o cunoști (vezi capitolul 8).

Regula de aur a codurilor

Un cod primit prin SMS sau în aplicație este cheia contului tău. **Nu îl dai nimănui, niciodată**, nici unui „prieten” care spune că ți l-a trimis din greșeală, nici unui „angajat” de la bancă sau de la WhatsApp. Un angajat adevărat nu îți va cere niciodată codul. Dacă cineva insistă, e un atac.

Dacă primești un apel suspect, închide și sună tu înapoi la numărul oficial, pe care îl găsești pe site-ul instituției sau pe spatele cardului. Nu suna la numărul din SMS și nu apăsă pe linkul primit.

Două capcane care nu seamănă cu phishingul

Codul QR

Un cod QR poate conține un link sau datele pentru o anumită acțiune, iar tu nu vezi ce conține înainte să îl scanezi. Nu e o dovadă de siguranță. Înainte să continui, citește adresa pe care ți-o arată telefonul. Fii foarte atent la codurile QR primite ca să „votezi”, să primești un premiu sau să îți „confirmi” contul: unele sunt de fapt coduri care conectează un dispozitiv străin la contul tău de WhatsApp, Telegram sau Discord. Nu confirma niciodată o asociere de dispozitiv pe care nu ai pornit-o tu.

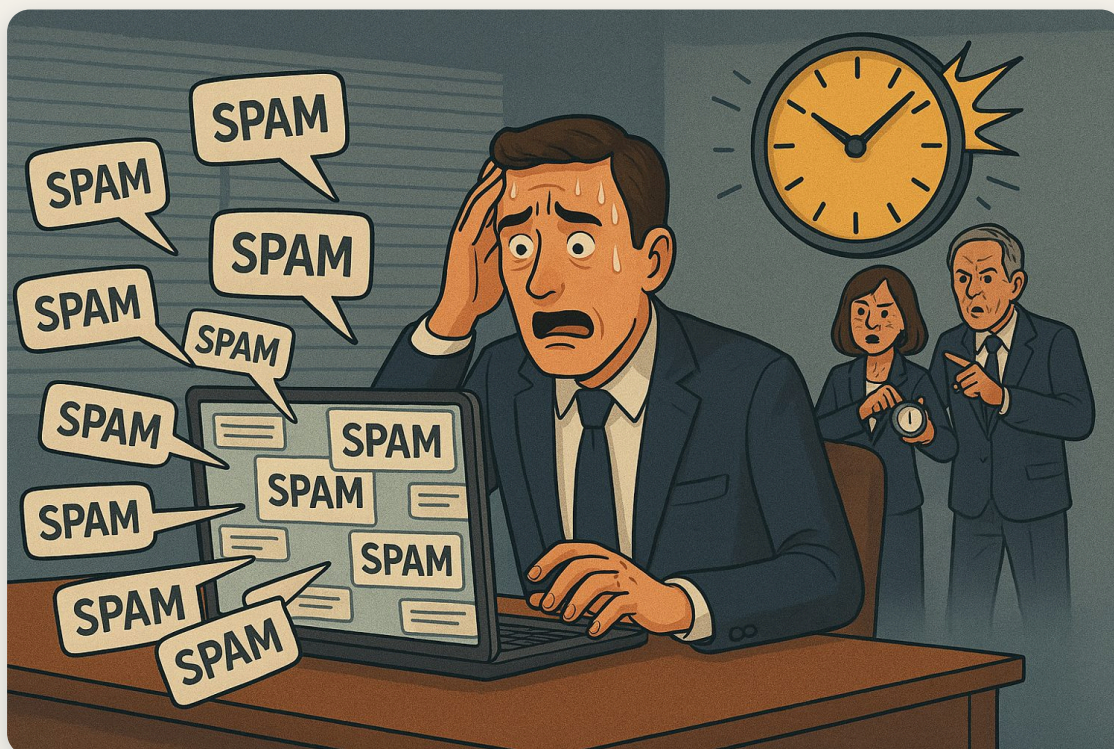
Verificarea falsă „Nu sunt robot”

O verificare adevărată de tip CAPTCHA îți cere să bifezi o căsuță sau să alegi niște imagini. Dacă o pagină îți cere să deschizi o fereastră de comenzi, să lipești acolo un text și să apeși Enter „ca să dovedești că ești om”, oprește-te imediat. Este o metodă prin care ajungi să instalezi singur un program malițios. Microsoft a descris în august 2026 o campanie care folosea exact astfel de verificări false.

Sursa: Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 august 2026.

Dacă ai executat deja comanda

- Deconectează dispozitivul de la internet.
- Cere ajutor unui adult sau unui specialist ca să verifice dispozitivul.
- Schimbă parolele importante de pe un alt dispozitiv, sigur, nu de pe cel afectat.



Programele care se instalează pe ascuns

Malware e numele general pentru orice program făcut să îți facă rău. Ajunge adesea pe dispozitiv printr-o instalare înșelătoare, când crezi că instalezi altceva: un „cheat” pentru un joc, o aplicație piratată, un fișier primit pe Discord. Poate intra însă și prin vulnerabilități ale sistemului care nu au fost încă reparate prin actualizări.

Tip	Ce face
Virus	Se atașează de alte fișiere și se răspândește când le deschizi sau le trimiți mai departe.
Troian	Se ascunde într-un program care pare util, ca soldații din calul troian, și îi dă atacatorului acces la dispozitiv.
Spyware	Te spionează: ce tastezi, ce parole folosești, ce mesaje scrii, uneori chiar camera și microfonul.
Ransomware	Îți blochează sau îți criptează fișierele și cere bani ca să ți le „dea înapoi”.
Adware	Te inundă cu reclame și ferestre pop-up, multe dintre ele cu linkuri periculoase.



Știai că?

Primul ransomware cunoscut a apărut în 1989 și a fost distribuit pe dischete, la o conferință despre SIDA. Peste 35 de ani mai târziu, în februarie 2024, un atac ransomware asupra platformei Hipocrate a afectat direct 26 de spitale din România, iar alte zeci au fost deconectate preventiv. Atacatorii au cerut 3,5 bitcoin, aproximativ 157.000 de euro. DNSC a recomandat ferm să nu se plătească răscumpărarea.

Sursa: TVR Info, despre atacul asupra platformei Hipocrate, 13 februarie 2024.

Cum te **aperi** de malware

Nu ai nevoie de zece programe de securitate. Ai nevoie de câteva obiceiuri bune, repetate până devin automate.

- Instalezi aplicații doar din magazinele oficiale (Google Play, App Store) și jocuri doar de pe platformele oficiale (Steam, Epic, site-ul producătorului).
- Nu descarci „cheats”, „generatoare” sau versiuni „crackuite”. Sunt cel mai sigur mod de a-ți instala singur un troian.
- Faci actualizările de sistem imediat ce apar. Multe dintre ele repară exact breșele folosite de atacatori.
- Verifici ce permisiuni cere o aplicație. Un joc simplu nu are nevoie de contactele, microfonul și locația ta.
- Ai o copie de siguranță a fișierelor importante, ca un eventual ransomware să nu te poată șantaja.
- Dacă pe ecran apare un mesaj că „ai virus” și trebuie să suni sau să plătești ceva, e aproape sigur o înșelătorie. Închide pagina și cere ajutor unui adult.



Pe scurt

- Phishingul te prinde prin grabă, frică, curiozitate sau câștig.
- Verifici adresa reală, domeniul și cererea, nu doar numele afișat.
- Nu dai niciodată codurile primite prin SMS.
- Malware-ul poate ajunge prin instalări înșelătoare, dar și prin vulnerabilități. Actualizările și prudența se completează.

CAPITOLUL 4

Oameni care vor să te manipuleze

Cele mai dureroase atacuri nu îți fură parola, ci încrederea. Cyberbullying, grooming, metoda loverboy și sextorsiunea se bazează pe emoții, nu pe tehnologie.



Cyberbullying înseamnă să umilești, să ameninți, să excluzi sau să hărțuiești pe cineva prin mijloace digitale: mesaje, comentarii, poze sau clipuri distribuite fără acord, grupuri create ca să râdă de cineva, conturi false. Spre deosebire de bullyingul din curtea școlii, cel online te urmărește și acasă, la orice oră, iar publicul poate fi uriaș.

Cyberbullying: cât de des se întâmplă

49%

dintre cei 4.449 de elevi care au răspuns la un sondaj Salvați Copiii spun că au fost victime ale bullyingului. 27% recunosc că au fost agresori.

Sursa: Salvați Copiii România, studiu despre bullying în școli, comunicat din 18 octombrie 2022

79%

dintre aceiași elevi spun că au asistat la bullying pe rețelele sociale, iar 45% văd cyberbullying des sau foarte des.

Sursa: Salvați Copiii România, studiu despre bullying în școli, comunicat din 18 octombrie 2022

48,3%

dintre copiii participanți la studiul citat petrec peste șase ore pe zi în mediul digital.

Sursa: Salvați Copiii România, comunicat de presă din 28 martie 2025

45.245

de sesizări (nu victime sau cazuri confirmate) privind conținut online ilegal sau dăunător pentru copii au ajuns la linia esc_ABUZ între 1 ianuarie și 3 decembrie 2025.

Sursa: Salvați Copiii România, linia esc_ABUZ, comunicat din 10 decembrie 2025

Sondajul Salvați Copiii din 2022 a folosit un eșantion neprobabilistic, deci arată o tendință, nu o măsurătoare exactă pentru toți elevii din România.

Ce faci dacă ești ținta

- Nu răspunde pe loc și nu te răzbuna. Agresorul așteaptă exact reacția ta.
- Salvează dovezile: capturi de ecran cu mesajele, numele contului, data și ora.
- Blochează contul și raportează-l platformei.
- Vorbește cu un adult în care ai încredere: un părinte, dirigintele, consilierul școlar. Nu e vina ta și nu trebuie să duci asta singur.
- Dacă primești amenințări cu violență, e o problemă pentru poliție, nu doar pentru școală.

Ce faci dacă ești martor

Martorii au mai multă putere decât cred. Nu da like, nu distribui și nu comenta. Scrie-i în privat persoanei vizate că nu e singură. Raportează postarea și spune-i unui adult. Un singur om care spune „nu e ok” poate schimba atmosfera dintr-un grup întreg.

Grooming: prietenul prea bun ca să fie adevărat

Groomingul este manipularea prin care cineva câștigă treptat încrederea sau supunerea unui copil ori adolescent, de multe ori online, pentru a-l abuza sau exploata. Nu arată ca un pericol. Arată ca o prietenie: cineva atent, care te ascultă, te laudă, îți face cadouri în joc sau îți oferă ce simți că îți lipsește.



Tiparul se repetă aproape mereu. La început apar atenția și complimentele. Urmează mutarea discuției pe o aplicație mai privată și ideea că „ce vorbim noi rămâne între noi”. Apoi persoana încearcă să te îndepărteze de familie și de prieteni („ei nu te înțeleg ca mine”), iar cererile devin tot mai personale. La final pot apărea cererea de poze, propunerea de întâlnire sau amenințările.

Semnale de alarmă

- Un adult care îți cere să păstrezi secretul conversației.
- Cineva care vrea să mute discuția într-o aplicație mai ascunsă.
- Cadouri, bani sau monede virtuale fără niciun motiv.
- Întrebări despre corpul tău sau cereri de poze.
- Presiune să vă întâlniți, mai ales fără să știe cineva.

Nu te baza pe vârsta declarată: presiunea și exploatarea pot veni și de la persoane cunoscute sau de vârsta ta. Dacă recunoști unul dintre aceste semnale, oprește conversația, nu șterge mesajele text (sunt dovezi) și spune-i imediat unui adult. Nu ai greșit cu nimic. Cei care fac asta sunt pricepuți la manipulare și se bazează exact pe rușinea și pe tăcerea ta.

„Dacă ai încredere în mine, dă-mi parola”

Riscul nu vine doar de la necunoscuți. Uneori vine de la cineva pe care îl cunoști bine: un iubit, o iubită, un prieten apropiat. Nu trebuie să dovedești iubirea sau prietenia oferind acces la conturi, localizare permanentă ori imagini intime. Presiunea, verificarea telefonului, cererea parolelor și amenințarea că va publica ceva despre tine sunt semnale de control, nu de dragoste.

Publicarea adresei, a numărului de telefon sau a programului tău pentru a te expune se numește **doxing**. Dacă ți se întâmplă, păstrează linkurile și amenințările, raportează postările și cere ajutor unui adult. Dacă sunt implicate școala sau sala unde te antrenezi, anunță și un adult responsabil de acolo.

Dacă te temi că persoana va deveni violentă

Cere ajutor de pe un dispozitiv la care persoana nu are acces. Pregătește împreună cu un adult de încredere sau cu un specialist schimbările de parole și de localizare: unele pot trimite notificări sau pot fi observate. Siguranța ta fizică are prioritate. În pericol imediat, sună la 112.

Sursa: eSafety Commissioner (Australia), urmărirea, monitorizarea și hărțuirea fără consimțământ în rândul copiilor, actualizat la 1 iulie 2025, sondaj din decembrie 2024 - februarie 2025.

Acordul pentru o fotografie nu înseamnă acordul pentru distribuire

Faptul că cineva ți-a trimis o poză sau a fost de acord să fie fotografiat nu îți dă dreptul să o trimiți mai departe. Regula se aplică și între colegi sau parteneri, inclusiv când imaginea a fost modificată cu AI. Cine distribuie fără acord face rău, chiar dacă „toată lumea a văzut-o deja”.

Dacă primul adult nu te ajută

Cere ajutor altui adult: consilierul școlar, un profesor, antrenorul sau un serviciu de protecție a copilului. Nu renunța pentru că prima persoană te-a ignorat sau te-a învinovățit.

Metoda **loverboy**



Metoda „loverboy” este una dintre cele mai folosite de traficanții de persoane pentru a racola fete, de multe ori minore. Traficantul o face pe victimă să creadă că s-a îndrăgostit de ea. Îi promite o viață de vis, siguranța emoțională pe care poate nu o are acasă, uneori o plecare „pentru puțin timp” în străinătate, ca să strângă bani pentru viitorul lor împreună. Treptat, victima devine dependentă emoțional, apoi controlată, iar exploatarea începe adesea cu „fă asta pentru noi, doar o dată”.

6,3 milioane

de oameni se aflau, la un moment dat în 2021, în situații de exploatare sexuală comercială forțată. 1,7 milioane dintre ei erau copii, iar aproape 4 din 5 victime sunt femei și fete.

Sursa: Organizația Internațională a Muncii (ILO), Walk Free și Organizația Internațională pentru Migrație (IOM), Global Estimates of Modern Slavery, septembrie 2022

Dacă iubitul tău, sau al unei prietene, îi cere să își rupă legăturile cu familia, îi controlează telefonul, îi cere bani sau îi propune o „slujbă” în străinătate, vorbiți cu cineva. În România, ANITP are o linie gratuită: **0800 800 678**.

Sextorsiunea și pozele false create cu AI

Sextorsiunea este șantajul cu imagini intime. Un cont care pare al unei fete sau al unui băiat de vârsta ta începe o conversație, flirtează, trimite o poză și îți cere una în schimb. Imediat ce o primește, tonul se schimbă: „Plătește sau o trimit tuturor prietenilor tăi.” Atacatorii au deja lista cu urmăritorii tăi. Sunt rapizi, agresivi și, de cele mai multe ori, sunt rețele organizate din alte țări, care vor bani.

În ultimii ani a apărut o variantă și mai cinică: nu mai au nevoie de o poză reală. Iau o fotografie obișnuită de pe profilul tău și creează, cu inteligența artificială, o imagine falsă care pare intimă.

137 pe zi

În 2025, centrul american NCMEC a primit peste 50.000 de sesizări de sextorsiune financiară, în medie 137 pe zi.

Sursa: NCMEC, comunicat despre sextorsiune, publicat pe 25 iunie 2026, date pentru 2025

Peste 400.000

de sesizări de exploatare a copiilor cu legătură cu inteligența artificială generativă a primit NCMEC în 2025.

Sursa: NCMEC, datele CyberTipline, publicate în 2026, date pentru 2025

Sunt sesizări primite de un centru de raportare, nu numărul victimelor și nici o măsurătoare pentru România.

Dacă ți se întâmplă

- **Nu plăti.** Plata nu garantează oprirea șantajului și poate duce la alte cereri.
- Oprește conversația. Păstrează mesajele de amenințare și datele contului. Pentru imaginile intime, urmează regulile din capitolul 10.
- Blochează și raportează contul.
- Spune-i unui adult. Șantajistul te vrea singur și rușinat.
- Pentru imagini, folosește [Take It Down](#) (pagina următoare) și linia **esc_ABUZ** a Salvați Copiii. Poți suna și la **119**.

Nu ești tu cel care a greșit. Infracțiunea o comite cel care te șantajează.

Ce poate face **Take It Down**

Dacă aveai sub 18 ani când a fost realizată imaginea intimă, poți folosi gratuit Take It Down (takeitdown.ncmec.org), chiar dacă între timp ai devenit major. Fișierul trebuie să existe deja pe dispozitivul tău: imaginea rămâne acolo, nu o trimiți nimănui, iar serviciul creează doar o amprentă digitală pe care o primesc platformele participante, ca să o poată bloca.

Nu descărca imaginea și nu cere cuiva să ți-o trimită pentru acest scop. Dacă nu o ai, cere ajutor prin raportare: platforma, linia esc_ABUZ, 119 sau poliția. Serviciul poate limita răspândirea, dar nu garantează eliminarea de pe tot internetul și nu funcționează în toate conversațiile criptate. Pentru imaginile false create cu AI, raportează-le platformei, pe linia esc_ABUZ și poliției.

Sursa: NCMEC, Take It Down, întrebări frecvente.

Pentru părinți: dacă vă spune copilul

Păstrați-vă calmul și mulțumiți-i că v-a spus. Faptul că a venit la voi e cel mai important lucru. Nu căutați vinovați, nu luați telefonul ca pedeapsă și nu plătiți. Notați datele contului și păstrați mesajele de amenințare, fără să copiați sau să trimiteți imaginile. Raportați contul și cereți ajutor la 119 sau la poliție.

Când un grup îți cere să **dovedești ceva**

Unele grupuri online încep cu glume, jocuri sau promisiunea că, în sfârșit, aparții undeva. Europol avertizează că astfel de comunități își caută victimele pe platforme de jocuri, de streaming și pe rețelele sociale, apoi mută discuția în canale private. Urmează cererile de „probe”: să umilești pe cineva, să trimiți imagini intime, să rănești un animal, să te rănești sau să faci rău altcuiva. Folosesc amenințări sau informațiile pe care le-au adunat despre tine ca să te oblige să continui.

Nu trebuie să îndeplinești o ultimă cerere

Nu te baza pe promisiunea că te vor lăsa în pace după încă o cerere. Oprește interacțiunea și cere ajutor unui adult. Păstrează numele grupului și mesajele de amenințare, fără să copiezi sau să distribui materialele de abuz. Nu investiga grupul și nu încerca să îl confrunți singur. Dacă există un pericol imediat pentru tine sau pentru altcineva, sună la 112.

Sursa: Europol, The rise of online cult communities dedicated to extremely violent child abuse, ianuarie 2025.

Ce simt victimele și ce le ajută

Cine trece prin cyberbullying, grooming sau sextorsiune trăiește de obicei același amestec: rușine, frică, vinovăție și senzația că nimeni nu poate ajuta. Tocmai de aceea atacatorii insistă pe secret. Cel mai important lucru pe care îl poți face pentru tine sau pentru un prieten este să rupi tăcerea.

Pentru tine

Vorbește cu cineva în aceeași zi. Nu trebuie să ai toate răspunsurile, ajunge să spui „am o problemă și am nevoie de ajutor”.

Pentru un prieten

Ascultă fără să judeci, nu distribui nimic din ce ți-a arătat și ajută-l să meargă la un adult. Nu promite că păstrezi secretul dacă e în pericol.

Pentru părinți

Schimbări bruște de dispoziție, retragere, frica de telefon sau, dimpotrivă, lipirea de el, notele care scad. Întrebați cu calm și nu luați telefonul ca pedeapsă.

Pentru profesori

Tratați fiecare caz raportat ca pe unul real, protejați identitatea elevului și implicați consilierul școlar.



Numărul unic național 119: abuz, neglijare sau exploatare a unui copil. Gratuit și non-stop.

Pe scurt

- Manipularea arată aproape mereu ca o prietenie, o iubire sau un compliment.
- Secretul cerut de un adult este semnalul cel mai clar de pericol.
- Nu plătești niciodată un șantajist.
- Rușinea e a agresorului, nu a ta.

CAPITOLUL 5

Conturile și telefonul tău

Parolele, autentificarea în doi pași și câteva setări bine alese te protejează mai mult decât orice program. Iată ce s-a schimbat în regulile despre parole.

Parolele: lungimea bate complexitatea

Poate ai auzit că o parolă bună trebuie să aibă litere mari și mici, cifre și simboluri, și că trebuie schimbată la câteva luni. Regulile s-au schimbat. Ghidul NIST din august 2025, un standard american pentru serviciile de identitate digitală folosit ca reper de specialiști din multe țări, spune lucruri mai simple: lungimea contează cel mai mult, iar schimbările forțate la intervale fixe nu ajută.

Folosește o frază-parolă

Patru-cinci cuvinte fără legătură între ele, de exemplu „cactus mov aleargă la Constanța”. E lungă, ușor de ținut minte și greu de ghicit.

Cel puțin 15 caractere

Pentru conturile protejate doar cu parolă, NIST recomandă minimum 15 caractere.

O parolă pentru fiecare cont

Dacă un site e spart, atacatorii încearcă aceeași parolă peste tot. O parolă refolosită pune în pericol mai multe conturi deodată.

Schimb-o când e nevoie

Nu la calendar, ci atunci când ai motive să crezi că a fost compromisă.

Parola	De ce
Andrei2009	Slabă: nume și an, primele lucruri pe care le încearcă un atacator.
M@r1aB3st!	Pare complicată, dar e scurtă, iar trucurile cu simboluri sunt cunoscute de programele de spart parole.
cactus mov aleargă la Constanța	Bună ca idee: lungă, fără legătură cu tine, ușor de ținut minte. Nu o folosi chiar pe aceasta: a apărut într-un ghid public.

Ce nu mai funcționează

Înlocuirea literelor cu simboluri („p@r0l@”) nu păcălește programele de spart parole, care cunosc toate aceste trucuri. Nu folosi nici numele, data nașterii, numele animalului sau șiruri de tipul „123456” și „qwerty”.

Sursa: NIST, SP 800-63B-4, Digital Identity Guidelines, august 2025.

Managerul de parole și passkeys

Nimeni nu poate ține minte 40 de fraze-parolă diferite. De aceea există managerele de parole: aplicații care generează, păstrează și completează parolele în locul tău. Ții minte una singură, foarte bună, iar restul le gestionează aplicația. telefoanele și browserele au deja manageri incluși (Parole Google, Parole Apple), iar aplicații precum Bitwarden sau 1Password fac același lucru pe toate dispozitivele.

Passkeys sunt următorul pas: o cheie digitală legată de telefonul tău, deblocată cu amprenta, fața sau codul ecranului. Nu ai ce să scrii greșit pe un site fals, iar o cheie de acces nu poate fi furată prin phishing ca o parolă. Dacă un cont îți oferă opțiunea, activeaz-o.

Autentificarea în doi pași

Autentificarea în doi pași (2FA) cere, pe lângă parolă, ceva ce ai doar tu: un cod dintr-o aplicație, o confirmare pe telefon sau o cheie de acces. Reduce mult riscul ca o parolă furată să fie suficientă pentru preluarea contului. Nu te protejează însă de orice atac: un site fals îți poate cere și codul, iar un program malițios poate fura o sesiune în care erai deja conectat. Alege passkeys sau chei de securitate când sunt disponibile. Dacă folosești coduri, o aplicație de autentificare e în general preferabilă SMS-ului, dar dacă SMS-ul e singura opțiune, activează-l: e mai bine decât doar parola. Nu aproba niciodată o conectare pe care nu ai pornit-o tu. Activează autentificarea în doi pași în primul rând pe email, pe contul principal de Google sau Apple, pe rețelele sociale, pe WhatsApp (verificare în doi pași, cu PIN) și pe conturile de jocuri.

Sursa: CISA, Implementing Phishing-Resistant MFA (fișă informativă); Microsoft, Token theft playbook.

Ordinea corectă

1. Emailul principal: cine îl controlează poate reseta parola oricărui alt cont.
2. Contul Google sau Apple al telefonului.
3. WhatsApp, Instagram, TikTok, Snapchat.
4. Conturile de jocuri și platformele cu bani sau carduri salvate.

Rețelele WiFi publice



Cafenele, aeroporturi, hoteluri, mall-uri: peste tot găsești WiFi gratuit. Astăzi, majoritatea site-urilor și aplicațiilor criptează datele (adresa începe cu **https**), deci conectarea la o rețea publică e de obicei mai sigură decât acum zece ani. Pericolul rămâne la rețelele false: oricine poate crea o rețea numită „Free_Airport_WiFi”. O astfel de rețea te poate trimite spre pagini frauduloase sau îți poate cere să instalezi ceva. Simpla conectare nu îți permite însă automat celui care o controlează să citească parolele și mesajele trimise prin conexiuni criptate corect.

Nu ignora avertismentele de securitate ale browserului și nu instala certificate, aplicații sau „actualizări” cerute pentru conectare. HTTPS protejează legătura cu site-ul, dar nu dovedește că site-ul e legitim. Un VPN nu transformă un site fals într-unul sigur.

Sursa: FTC (Statele Unite), Are Public Wi-Fi Networks Safe? What You Need To Know.

Știi că?

Când activezi autentificarea în doi pași, majoritatea platformelor îți oferă și **coduri de rezervă**. Salvează-le într-un loc sigur, de exemplu în managerul de parole sau tipărite acasă. Te pot ajuta să recuperezi accesul dacă pierzi telefonul. Verifică dinainte și celelalte metode de recuperare oferite de platformă.

Reguli simple pentru WiFi public

- Întreabă personalul care e numele exact al rețelei.
- Pentru bancă, plăți sau parole importante, folosește datele mobile.
- Nu instala nimic și nu accepta „actualizări” cerute de pagina de conectare.
- Dezactivează conectarea automată la rețele deschise.
- Dacă folosești des rețele publice, un VPN de la o firmă cunoscută adaugă un strat de protecție, dar nu ține locul atenției.

Telefonul tău, seiful tău

Telefonul are pozele, conversațiile, conturile, locația și uneori cardul tău. Merită protejat ca un seif.

Blocarea ecranului

Cod de cel puțin 6 cifre, plus amprentă sau recunoaștere facială. Nu 123456, nu anul nașterii.

Actualizări

Instalezi actualizările de sistem și de aplicații imediat. Cele mai multe repară breșe de securitate.

Permisii

Verifici lunar ce aplicații au acces la cameră, microfon, locație și contacte. Ștergi aplicațiile pe care nu le mai folosești.

Backup

Copie de siguranță automată în cloud, protejată cu autentificare în doi pași.

Locație și partajare

Limitează accesul aplicațiilor la locație și verifică persoanele care îți pot vedea poziția. Păstrează setările necesare serviciului de găsire a telefonului. Partajarea permanentă cu alte persoane nu trebuie să fie o condiție a prieteniei sau a unei relații.

Găsește-mi dispozitivul

Activezi Find My iPhone sau Găsește-mi dispozitivul înainte să ai nevoie de ele.

Sursa: Google, Ajutor Cont Google: Be ready to find a lost Android device.

Verifică din când în când pe **haveibeenpwned.com** dacă adresa ta de email a apărut într-o breșă de date. Dacă da, schimbă parola aceluia cont și a oricărui cont unde ai folosit-o.

Dacă ți-ai pierdut telefonul sau ți-a fost furat

1. Îl localizezi sau îl blochezi de la distanță, din contul Google sau Apple.
2. Schimbi parola emailului și a conturilor importante.
3. Anunți operatorul ca să blocheze cartela SIM, ca nimeni să nu primească codurile tale prin SMS.
4. Dacă e nevoie, ștergi datele de la distanță.

Pe scurt

- Frază-parolă lungi, câte una pentru fiecare cont, ținute într-un manager de parole.
- Autentificare în doi pași peste tot, începând cu emailul.
- Pe WiFi public verifici rețeaua, respecți avertismentele de securitate și nu instalezi nimic pentru conectare.
- Telefonul blocat, actualizat și cu backup.

CAPITOLUL 6

Gaming sigur

Jocurile sunt printre locurile preferate ale escrocilor, pentru că acolo sunt mulți tineri, bani virtuali și multă încredere între jucători.



Contul tău de Fortnite, Roblox, Minecraft, Counter-Strike, League of Legends, EA Sports FC sau NBA 2K are valoare reală: skinuri, monede, progres, uneori un card salvat. Escrocii știu asta și au inventat câteva capcane care se repetă de la un joc la altul.

Capcanele care se repetă în toate jocurile

„Generatoare” de monede

Site-uri care promit V-Bucks, Robux sau monede gratis în schimbul datelor de logare. Recompensele gratuite reale le găsești doar în joc sau pe site-ul oficial.

Skinuri și schimburi false

Site-uri de trading sau de pariuri care arată oficial, dar îți golesc inventarul imediat ce te conectezi.

Turnee și evenimente false

Servere de Discord care promit premii și cer o „taxă de înscriere” sau logarea printr-un link.

Cheats și moduri

Programe care îți promit avantaje în joc, dar instalează de fapt un troian sau un program care îți fură parolele.

Stream-uri false

Transmisiuni care promit skinuri gratuite celor care intră pe un link și se loghează.

Vânzarea conturilor

Cumperi un cont „cu tot cu skinuri”, iar vânzătorul ți-l ia înapoi prin recuperarea parolei. Poți pierde și banii, și contul.

Știai că?

În ianuarie 2019, cercetătorii Check Point au arătat că atacatorii ar fi putut prelua conturile de Fortnite doar convingând jucătorul să apese pe un link, fără să afle parola. Epic Games a reparat problema, dar cazul a arătat că și cel mai popular joc din lume poate avea breșe.

Sursa: Check Point Research, Hacking Fortnite, 16 ianuarie 2019.

Atenție la „prietenii” din joc

Chatul din joc și serverele de Discord sunt și ele locuri în care adulții rău intenționați caută adolescenți. Tiparul e cel din capitolul 4: atenție, cadouri în joc, mutarea discuției în privat, cereri de poze sau de „probe”. Dacă cineva pe care nu îl cunoști în realitate îți oferă skinuri sau monede fără motiv, întreabă-te ce vrea în schimb.

Când jocul te face să mai **cumperi** o dată

Nu toate pierderile din jocuri vin de la escroci. Unele pachete, cufere sau loot boxes îți oferă recompense aleatorii: plătești fără să știi exact ce primești. Monedele virtuale fac mai greu de observat cât ai cheltuit de fapt în lei, iar skinurile pot ajunge pe site-uri de pariuri din afara jocului.

Ce faci

- Stabilești un buget înainte să începi și activezi confirmarea fiecărei achiziții.
- Nu împrumuți bani ca să recuperezi ce ai pierdut.
- Nu folosești contul unui adult ca să ocolești restricțiile.
- Dacă ascunzi cheltuielile sau continui pentru că „următoarea încercare trebuie să iasă”, oprești plățile și vorbești cu un adult.

Sursa: eSafety Commissioner, How to manage money in games.

Dacă ți-a fost furat contul de joc

1. Încearcă recuperarea din pagina oficială de suport a jocului, nu prin cineva care îți scrie că te poate ajuta.
2. Schimbă parola emailului asociat contului.
3. Anunță-ți prietenii din joc că nu tu le scrii.
4. Dacă erau carduri salvate, anunță-ți părinții să le blocheze.



Gaming sigur: **cinci reguli**

- 1** Autentificare în doi pași pe fiecare cont de joc. Epic, Roblox, Steam, Riot, EA și ceilalți o oferă gratuit.
- 2** Recompensele „gratuite” le verifici în joc sau pe site-ul oficial. Nu dai parola sau codurile unui intermediar.
- 3** Nu descărca niciodată hackuri, cheats sau generatoare. Sunt cel mai sigur mod de a-ți pierde contul și calculatorul.
- 4** Nu-ți împărtăși parola cu nimeni. Nici cu cel mai bun prieten, nici cu cineva care promite să îți urce rangul.
- 5** Verifică fiecare link înainte să dai click, mai ales pe cele primite pe Discord sau în chatul jocului.

Pentru părinți

Activați controlul parental din consolă sau din cont, pentru limitele de cheltuieli și de timp, nu pentru supraveghere permanentă. Nu salvați cardul în cont fără o confirmare la fiecare plată. Și, cel mai important, jucați din când în când împreună: e cel mai simplu mod de a afla cu cine vorbește copilul vostru online.

Pe scurt

- Contul de joc are valoare reală și e o țintă reală.
- Ofertele „gratuite” din afara jocului oficial sunt, de obicei, momeli.
- Loot boxes înseamnă cheltuieli aleatorii: îți fixezi un buget.
- Cheats și generatoarele aduc malware.
- Un străin generos din joc vrea ceva în schimb.

CAPITOLUL 7

Social media și creierul tău

Aplicațiile pe care le folosești în fiecare zi sunt construite de oameni foarte pricepuți, al căror scop e să te țină cât mai mult în fața ecranului.



Rețelele sociale te ajută să îți legătura cu prietenii și cu rudele din alte orașe, îți arată lucruri care te interesează și te scapă de plictiseală. Dar sunt și produse comerciale. Cu cât stai mai mult, cu atât vezi mai multe reclame, iar platforma câștigă mai mulți bani. De aceea, în spatele lor lucrează adevărați „ingineri ai atenției”, care folosesc psihologia comportamentală ca să facă aplicația cât mai greu de închis.

Puțină chimie: de ce e greu să te oprești

Creierul are un sistem de recompensă care ne motivează să repetăm lucrurile care ne fac bine. Dopamina joacă un rol important în acest sistem, mai ales în așteptarea recompensei. Fiecare like, fiecare notificare și fiecare clip nou poate fi o mică recompensă, dar nu știi niciodată când vine următoarea. Această incertitudine, numită recompensă variabilă, e același mecanism care face jocurile de noroc atât de greu de lăsat.

La adolescenți, zonele creierului legate de recompensă sunt foarte active, iar zonele implicate în planificare, în luarea deciziilor și în controlul impulsurilor continuă să se maturizeze în tinerețe. Asta nu înseamnă că ești „dependent” doar pentru că îți place TikTok. Înseamnă că e normal să-ți fie greu să te oprești și că merită să îți construiești câteva frâne.

Sursa: National Institute of Mental Health (SUA), The Teen Brain: 7 Things to Know.

Experimentul de o săptămână

Notează timpul de ecran din setările telefonului. Apoi, timp de o săptămână, oprește notificările de la rețelele sociale și lasă telefonul în altă cameră noaptea. La final, compară timpul de ecran, somnul și starea ta. Mulți adolescenți care încearcă asta sunt surprinși de rezultat.

11%

dintre adolescenții de 11, 13 și 15 ani din 44 de țări aveau, în 2022, semne de utilizare problematică a rețelelor sociale (7% în 2018). Cei care folosesc mult, dar fără să-și piardă controlul, raportează chiar mai mult sprijin de la prieteni.

Sursa: OMS Europa, studiul HBSC despre adolescenți, ecrane și sănătate mintală, 25 septembrie 2024, date pentru 2022

Semne că social media îți ia mai mult decât îți dă

- Intri „doar două minute” și ieși după o oră, fără să știi unde a trecut timpul.
- Telefonul e ultimul lucru pe care îl vezi seara și primul dimineața, iar somnul are de suferit.
- Te simți iritat sau neliniștit când nu ai acces la internet.
- Te întâlnești tot mai rar cu prietenii în realitate.
- Te afectează când nu primești like-urile sau comentariile la care te așteptai.
- Amâni temele, antrenamentul sau somnul pentru încă un clip.

Cum îți **recapeți** controlul

Notificări

Oprește-le pe toate, în afară de mesajele de la oameni reali. Tu decizi când intri, nu aplicația.

Limite de timp

Folosește Timp de utilizare (iPhone) sau Bunăstare digitală (Android) pentru limite zilnice.

Telefonul în altă cameră

Noaptea, telefonul stă la încărcat în afara dormitorului. Somnul e cel mai bun upgrade pe care ți-l poți face.

Feed ales de tine

Dă unfollow conturilor după care te simți mai prost. Algoritmul învață din ce urmărești.

Nu contează doar cât stai, ci și ce îți face **conținutul**

Dacă un cont te împinge să te înfometezi, să te rănești, să urăști un grup sau să faci ceva periculos ca să fii acceptat, nu trebuie să continui să îl urmărești. Nici numărul de urmăritori, nici faptul că apare în feed nu îl transformă într-o sursă sigură.

Folosește „Nu mă interesează”, blochează sau raportează contul și caută informația în surse independente. Nu trimite unui prieten un clip traumatizant ca să îi arăți ce ai văzut: poți cere ajutor descriind situația. Dacă te afectează în continuare, vorbește cu un adult sau cu un consilier.

Pe scurt

- Aplicațiile sunt gândite să te țină cât mai mult în fața ecranului.
- Recompensele imprevizibile fac greu de oprit scrollul.
- Notificările oprite și telefonul scos din dormitor fac o diferență uriașă.
- Conținutul care te rănește se blochează și se raportează, nu se distribuie.

CAPITOLUL 8

Deepfake și inteligența artificială

Ce vezi și ce auzi nu mai e o dovadă în sine. O față, o voce sau un clip pot fi create în câteva minute.



Deepfake vine din alăturarea a două cuvinte: deep learning, metoda prin care calculatoarele învață din foarte multe exemple, și fake, fals. Un deepfake este o imagine, un clip video sau o înregistrare audio modificată ori creată cu inteligența artificială, care arată sau sună ca o persoană reală. Pentru asta, programul are nevoie de poze, clipuri și înregistrări cu persoana respectivă, iar cu cât are mai multe, cu atât rezultatul e mai convingător.

Cum e folosit împotriva oamenilor

Deepfake-ul poate fi folosit pentru glume și filme, dar și pentru a înșela, a șantaja sau a distruge reputația cuiva. Trei riscuri importante pentru adolescenți sunt: pozele false cu caracter intim create din fotografii obișnuite (capitolul 4), clipurile false cu persoane cunoscute care recomandă investiții sau concursuri și apelurile în care o voce clonată a unui membru al familiei cere bani urgent.

Un caz real

În 2024, un angajat al firmei de inginerie Arup din Hong Kong a participat la o videoconferință cu directorul financiar și cu alți colegi. Toți erau falși, creați cu inteligența artificială. Convins că vorbește cu oameni reali, angajatul a transferat 200 de milioane de dolari Hong Kong, aproximativ 25 de milioane de dolari americani, în conturile escrocilor.

Sursa: CNN, despre fraudă deepfake de la Arup, 16 mai 2024.

Cum verifici, fără să te bazezi doar pe aparențe

Degetele deformate, umbrele imposibile, nasturii care apar și dispar sau buzele nesincronizate pot ridica suspiciuni. Absența lor nu dovedește însă că imaginea sau înregistrarea e autentică. Niciun detector AI nu trebuie tratat ca verdict final: un studiu publicat de guvernul britanic în 2026 arată că astfel de instrumente funcționează mai slab în condiții reale decât în laborator.

Caută sursa inițială, data și contextul. Verifică dacă informația e confirmată independent. O fotografie reală poate fi folosită cu o poveste falsă, iar o imagine generată poate arăta impecabil. Dacă mesajul cere bani, date, imagini intime sau o acțiune urgentă, verifică persoana printr-un canal pe care îl cunoșteai deja. Nu lua decizia doar pentru că ai recunoscut o față sau o voce.

Sursa: Department for Science, Innovation and Technology (Marea Britanie), Deepfake detection technology, 26 martie 2026.

Verificarea unei urgențe în familie

Stabiliți un cuvânt de siguranță pe care nu îl publicați și nu îl folosiți în conversații obișnuite. E un indiciu în plus, nu o garanție. Dacă cineva cere bani urgent, închide și sună persoana la numărul pe care îl aveai deja salvat. Dacă nu răspunde, verifică printr-un alt membru al familiei. Nu transfera bani doar pe baza vocii, a unui apel video sau a răspunsului corect la o singură întrebare.

Exercițiu: reală sau generată cu AI?

Cele două imagini de mai jos fac parte din modulul REAL / FAKE / AI al platformei TRUST // NO TRUST. Știm exact de unde vin, pentru că le-am creat noi pentru exercițiu. Uită-te la ele ca și cum le-ai vedea în feed, înainte să citești răspunsul.



„ULTIMA ORĂ: bulevardul e un râu acum!”

Răspuns: **imagine generată cu AI pentru acest exercițiu**. Știm asta din proveniența ei. Dacă ai întâlni postarea online, ai verifica locul, data și confirmările independente. Lipsa confirmărilor ar însemna că informația rămâne neverificată, nu că ai demonstrat folosirea AI.



„Dau 10 telefoane, trimite-mi adresa!” Răspuns: **generată cu AI**; persoana nu există. Pielea fără textură poate fi un indiciu, dar mai important e mesajul: un necunoscut care cere adresa ta în schimbul unui premiu e o capcană, indiferent dacă fața e reală.

Lecția: știm că imaginile sunt generate pentru că le cunoaștem proveniența. Într-o postare necunoscută, separă două întrebări: „Este imaginea autentică?” și „Este mesajul credibil?”. Nu trebuie să demonstrezi folosirea AI ca să refuzi o cerere suspectă.

Pe scurt

- O imagine sau o voce nu mai e o dovadă în sine.
- Lipsa defectelor nu dovedește că ceva e real.
- Verifici sursa și pe alt canal, mai ales când ți se cer bani sau date.

AI-ul care pare că te înțelege

Un chatbot poate explica o lecție sau te poate ajuta să formulezi o idee. Poate însă și să greșească, să inventeze surse sau să ofere un sfat nepotrivit, chiar dacă răspunde foarte convingător.

Unele aplicații sunt construite să pară prieteni sau parteneri. Faptul că îți răspund cu empatie nu înseamnă că te cunosc, că au sentimente sau că pot avea grijă de tine.

32%

dintre copiii australieni de 10-17 ani care folosiseră un asistent sau un companion AI spuneau că i-au împărtășit informații personale sau sensibile, inclusiv poze sau secrete. Sondajul a cuprins aproape 2.000 de copii.

Sursa: eSafety Commissioner (Australia), Talking to machines, raport publicat în august 2026, sondaj realizat în 2026

Ce nu spui unui chatbot

- Parole, coduri, date din acte, adresa ta.
- Imagini intime, ale tale sau ale altcuiva.
- Conversațiile private ale altor oameni.

Nu presupune că discuția are confidențialitatea unei întâlniri cu un psiholog. Verifică setările și regulile serviciului despre păstrarea și folosirea datelor.

Dacă discuțiile cu un chatbot încep să îți înlocuiască somnul, prietenii sau ajutorul oamenilor, vorbește cu cineva în care ai încredere. Pentru abuz, șantaj, sănătate sau pericol, cere ajutor unui adult ori unui profesionist. Nu lăsa un chatbot să fie singurul tău sprijin.

Poți exersa mai mult în modulul REAL / FAKE / AI de pe platforma TRUST // NO TRUST, unde ai de ales între fotografii reale, imagini editate și imagini generate complet de AI.

CAPITOLUL 9

Escrocheriile virale

Unele țepe nu par atacuri, ci favoruri: un vot pentru fiica unei prietene, un job ușor de acasă, un premiu de la un magazin cunoscut.

„Votează, te rog, pentru Adeline”

Bună, ați putea vota pentru Adeline aici, vă rog? Aceasta este fiica prietenilor mei. Școala organizează un concurs pentru ei, al cărui premiu este grantul educațional al anului. Vă mulțumesc foarte mult pentru ajutor!

<https://dancingvot.top/home/vote1>

18:03

Mesajul vine pe WhatsApp, de obicei de la o persoană cunoscută: „Bună! Vă rog să o votați pe Adeline în acest sondaj, este fiica prietenei mele, premiul principal este o bursă de studii. Mulțumesc mult!” Linkul duce la un site cu două fete și un buton de vot.

Când apeși „Votează”, apare o fereastră care îți cere numărul de telefon și apoi codul pe care tocmai l-ai primit pe WhatsApp. Crezi că ai votat. În realitate, ai introdus codul de asociere a unui dispozitiv nou, iar atacatorii au acum acces la contul tău de WhatsApp. Imediat, același mesaj pleacă la toate contactele tale, iar uneori contul îți este suspendat pentru spam.

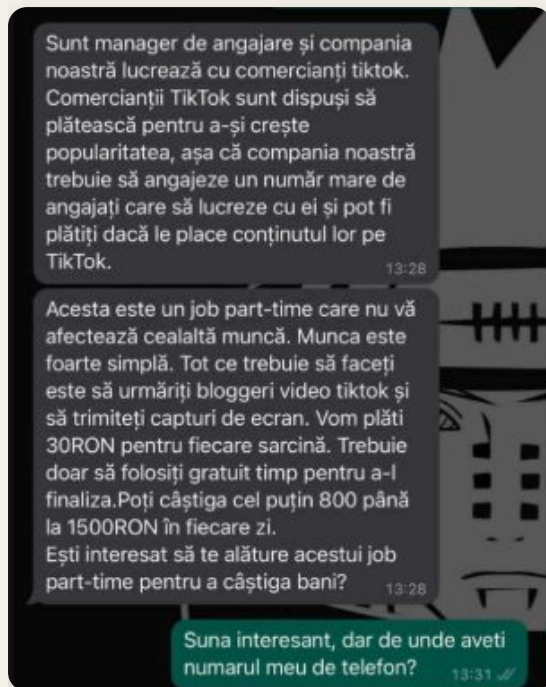
Cum te protejezi

- Nu introduci un cod primit pe WhatsApp într-o pagină deschisă dintr-un mesaj.
- Activezi Verificarea în doi pași din WhatsApp: Setări, Cont, Verificare în doi pași.
- Verifici des Setări, Dispozitive asociate și deconectezi ce nu recunoști.
- Dacă un prieten îți cere ceva neobișnuit, îl suni.

Același truc, alte haine

- **Cumpărătorul grăbit** de pe un site de anunțuri, care îți trimite un link „ca să primești banii” și îți cere datele cardului.
- **Biletele la concert** vândute de „cineva care nu mai poate ajunge”, plătite în avans și niciodată primite.
- **SMS-ul de la curier** care cere o taxă mică pentru un colet pe care nu l-ai comandat.

Jobul de acasă care te **costă**



„Ești interesat de un job part-time? Dai like la clipuri pe TikTok și primești 30 de lei pe fiecare captură de ecran. Poți câștiga 800-1.500 de lei pe zi.” La început chiar primești câțiva lei, ca să capeți încredere. Apoi ți se cere să „investești” o sumă ca să deblochezi sarcini mai bine plătite. Banii aceia nu se mai întorc niciodată.

Canalul pe care te contactează nu dovedește că oferta e reală. Verifică angajatorul independent și nu plăti niciodată ca să primești salariul sau ca să deblochezi sarcini.

Ce oferi **în schimb**?



Concursurile cu premii mari, cadourile de la magazine cunoscute, aplicațiile care îți arată „cum vei arăta peste 30 de ani” și testele care îți spun „ce personaj ești” au adesea un preț ascuns: datele tale, contactele tale sau accesul la contul tău. Nu tot ce e gratuit e o capcană, iar acest ghid e chiar un exemplu. Înainte să accepți ceva, întreabă-te ce oferi în schimb și cine primește.

Contul tău nu e un serviciu de **transfer** pentru alții

„Primești niște bani în cont, îi trimiți mai departe și păstrezi un comision.” Poate părea un job simplu sau un favor pentru un prieten. În realitate, poți fi folosit pentru mutarea unor bani proveniți din fraude. Europol descrie această schemă drept **money muling**, o formă de spălare de bani, iar persoana care primește și transferă banii pentru altcineva este numită „money mule”.

Ce faci

- Nu împrumuți accesul la contul bancar și nu deschizi conturi pentru altcineva.
- Nu oferi cardul, codurile sau fotografii ale actului pentru o ofertă neverificată.
- Dacă banii au ajuns deja, nu îi retragi și nu îi trimiți la indicațiile celui care te-a contactat.
- Anunți imediat banca, spui unui adult și ceri îndrumare poliției. Păstrezi conversația și detaliile transferului.

Sursa: Europol, ghidul de prevenire despre money muling.



Pe scurt

- Codurile se folosesc numai în procedura oficială pe care ai pornit-o tu; nu le comunică altora și nu le introduci în pagini primite pentru voturi sau premii.
- O plată mică primită la început nu dovedește că jobul e real. Nu trimiți bani ca să continui sau ca să retragi presupusele câștiguri.
- Un job care îți cere bani ca să începi e o țepă.
- Contul tău bancar nu e de împrumutat.

CAPITOLUL 10

Dacă ți s-a întâmplat

Oricine poate fi păcălit, inclusiv adulții și specialiștii. Contează ce faci în primele minute și să nu rămâi singur cu problema.

- 1 Oprește-te.** Nu mai răspunde, nu mai da click, nu plăti nimic. Respiră. Atacatorul mizează pe panica ta.
- 2 Păstrează dovezile fără să răspândești abuzul.** Notează numele contului, linkul profilului sau al postării, data și ora. Păstrează mesajele de amenințare și cererile de bani. Dacă apar imagini sexuale cu un minor, nu le descărca, nu le copia și nu le trimite mai departe „ca dovadă”: cere poliției sau serviciului de raportare instrucțiuni. Nu șterge în panică mesajele sau contul.
- 3 Spune-i unui adult în care ai încredere.** Părinte, diriginte, consilier școlar, antrenor. Astăzi, nu mâine.
- 4 Securizează conturile de pe un dispozitiv sigur.** Schimbă parolele, începând cu emailul, verifică metodele de recuperare și închide sesiunile necunoscute. Dacă ai instalat ceva suspect, nu introduce parole noi pe dispozitivul afectat. Urmează pașii potriviți situației tale de pe pagina următoare.
- 5 Raportează.** Platformei (butonul Raportează), apoi instituțiilor potrivite, de pe pagina următoare.
- 6 Ai grijă de tine.** Ce simți e normal. Dacă te apasă, vorbește cu un consilier, de exemplu la 116 111.

Ce nu faci

- Nu plătești și nu trimiți alte poze sau date, oricât de mult ești presat.
- Nu te răzbuni și nu ameninți înapoi.
- Nu ștergi conversațiile și nu îți ștergi contul în panică.
- Nu plătești pe cineva care îți promite recuperarea contului contra cost și nu îi dai acces la telefon sau coduri.
- Nu încerci să rezolvi singur. Problemele online se rezolvă mai repede cu un adult alături.

Primul pas depinde de **ce s-a întâmplat**

Ai introdus parola pe un site fals

De pe un dispozitiv sigur, intră direct în aplicația sau site-ul oficial, schimbă parola și închide sesiunile necunoscute. Verifică metodele de recuperare (email, telefon) și aplicațiile conectate. Dacă parola era folosită și în altă parte, schimb-o și acolo.

Ai dat datele cardului sau ai trimis bani

Contactează imediat banca, prin aplicația oficială sau la numărul de pe spatele cardului, și cere sprijinul unui părinte sau al unui adult de încredere. Cere blocarea cardului și verificarea tranzacțiilor. Nu aștepta răspunsul unui site de raportare.

Ai instalat ceva suspect sau ai executat o comandă

Deconectează dispozitivul de la internet și cere ajutor tehnic. Nu introduce parole noi pe el până nu e verificat. Schimbă parolele importante de pe alt dispozitiv.

Ești șantajat cu imagini

Nu plăti, nu trimite alte materiale și cere ajutor unui adult. Păstrează mesajele de amenințare fără să răspândești imaginile. Folosește Take It Down, esc_ABUZ sau 119.

Cineva îți promite recuperarea contra cost

Nu îi da acces la telefon, bani sau coduri. Folosește numai recuperarea oficială a platformei și instituțiile de pe pagina următoare.

Sursa: Microsoft, Token theft playbook.

Unde ceri ajutor

112

Urgențe. Suni dacă cineva este în pericol imediat sau dacă ești amenințat cu violență.

119

Protecția copilului: abuz, neglijare sau exploatare a unui copil. Gratuit, non-stop, și poți cere să rămâi anonim.

116 111

Telefonul Copilului: vorbești cu un consilier. Gratuit din Orange, Telekom și Vodafone, de luni până vineri, între 10:00 și 20:00, sau scrii la vorbestecunoi@telefonulcopilului.ro
Programul actualizat e pe telefonulcopilului.ro

0744 360 446

Helpline-ul Ora de Net (Salvați Copiii): întrebări despre siguranța online, între 10:00 și 17:00. Datele de contact actualizate sunt pe oradenet.ro/helpline

esc_ABUZ

Linia de raportare Salvați Copiii pentru conținut ilegal cu copii. Poți raporta doar linkul, anonim, pe oradenet.ro/linia-de-raportare

Take It Down

NCMEC: ajută la eliminarea imaginilor intime ale minorilor de pe platformele participante, fără să trimiți imaginea, pe takeitdown.ncmec.org

1911

DNSC: phishing, conturi sparte și fraude online. Poți scrie și la alerts@dnsc.ro

0800 800 678

ANITP, trafic de persoane: apel gratuit în România. Din străinătate: +40 21 313 31 00.

Poliția

Cere ajutor poliției. Dacă poți, mergi cu un adult de încredere, dar nu amâna cererea de ajutor dacă nu ai imediat pe cineva alături. În urgență, suni la 112.

Surse și pagini de contact: 112.ro, servicii publice.gov.ro, edupedu.ro (lansarea 119), telefonulcopilului.ro, oradenet.ro, takeitdown.ncmec.org, dnsc.ro, anitp.mai.gov.ro. Informații verificate în octombrie 2026; programul și condițiile pot fi actualizate de fiecare serviciu.

Când suni sau scrii, pregătește

Ce s-a întâmplat și când, numele conturilor implicate, linkurile și mesajele de amenințare. Pentru imaginile intime, nu face copii: urmează regula de la pasul 2. Nu e nevoie să ai totul. Spune ce știi, iar cei de la celălalt capăt te vor ajuta cu restul.

Ai nevoie de ajutor și pentru alte situații? Modulul HELP de pe platforma TRUST // NO TRUST te întreabă ce s-a întâmplat și îți arată exact cui te adresezi.

Ce reții după acest ghid

Mintea

- Problemele nespuse cresc: ceri ajutor din prima zi.
- Graba, frica, curiozitatea și câștigul sunt semnale de alarmă.
- Dacă sună prea bine ca să fie adevărat, nu e.
- O imagine sau o voce nu mai e o dovadă în sine.

Conturile

- Frazе-parolă lungi, diferite, într-un manager de parole.
- Autentificare în doi pași, începând cu emailul; nu aprobi conectări pe care nu le-ai pornit.
- Codurile primite prin SMS sau WhatsApp nu se dau nimănui.
- Passkeys oriunde sunt disponibile.

Dispozitivele

- Actualizări imediat ce apar.
- Aplicații doar din magazinele oficiale.
- Fără cheats, generatoare sau programe piratate.
- Backup și localizare activate.

Oamenii

- Cineva care îți cere să ascunzi presiuni, cereri intime sau amenințări e un semnal de pericol.
- Nu plătești niciodată un șantajist.
- Nu distribui, nu da like la umilirea altcuiva.
- Ceri ajutor din prima zi. Rușinea e a agresorului.

Testul de 10 secunde înainte de orice click

1. Cine îmi scrie, de fapt? Adresa reală, nu numele afișat.
2. Mă grăbește, mă sperie sau îmi promite ceva?
3. Îmi cere o parolă, un cod, bani sau o poză?
4. Pot verifica pe alt canal, sunând sau intrând direct în aplicație?
5. Am acordul persoanei vizate și înțeleg ce se poate întâmpla cu acest conținut?

Poți întâlni tentative de fraudă chiar dacă ești atent. Pregătirea te ajută să le recunoști și să limitezi consecințele.

CAPITOLUL 11

Tridentul: de ce cursul în școli

Siguranța online nu se construiește doar în telefonul unui adolescent. Are nevoie de trei vârfuli care lucrează împreună: elevii, părinții și profesorii.

Elevii

Învăț să recunosc manipulare pe exemple reale, din viața lor: Instagram, WhatsApp, jocuri, TikTok. Primesc un limbaj comun cu colegii, astfel încât un „ăsta e phishing” sau „nu da codul” să devină reflex de grup. Află unde cer ajutor înainte să aibă nevoie și află că nu sunt singuri, ceea ce scade rușinea și tăcerea, exact armele atacatorilor.

Părinții

Înțeleg riscurile reale, nu pe cele din titlurile de știri, și primesc semnalele la care să fie atenți. Învăț cum să vorbesc cu copilul fără să-l sperie și fără să-i ia telefonul ca pedeapsă, ceea ce l-ar face să ascundă următoarea problemă. Pot securiza conturile familiei și pot stabili împreună reguli și un cuvânt de siguranță.

Profesorii

Primesc un material gata de folosit la orele de dirigentie, de informatică sau de educație socială și un mod de a recunoaște și de a trata cazurile de cyberbullying sau de grooming. Școala devine un loc în care elevii raportează, nu ascund.

Platforma TRUST // NO TRUST include exerciții și un instrument educațional de evaluare, CDRS, aflat în dezvoltare și pilotare. Rezultatele pot arăta răspunsurile pe care elevii le stăpânesc și temele care trebuie reluate. Scorul nu e un diagnostic și nu garantează că un elev sau o școală e protejată de incidente.

Când cele trei vârfuli lucrează împreună, adolescentul nu mai e singur în fața unui ecran. Are colegi care recunosc aceleași trucuri, părinți care știu ce să întrebe și profesori care știu ce să facă. Asta transformă o lecție de câteva ore într-o cultură a siguranței.

Aduceți cursul în școala voastră

SMART ONLINE = SAFE OFFLINE este gratuit pentru școli, elevi, profesori și părinți. O sesiune durează o zi, într-o sală cu videoproiector, și nu cere niciun echipament special. Pentru programare, scrieți la nicholas.carstoiu@gmail.com sau sunați la 0743.332.318.

Surse

Fiecare cifră din ghid a fost verificată la sursa ei în octombrie 2026. Sursele includ rapoarte, comunicate și pagini oficiale. Acolo unde contează, am separat data publicării de perioada la care se referă datele.

1. UNICEF Innocenti, raportul Through Children's Eyes, publicat pe 3 septembrie 2026, date din cercetarea Disrupting Harm.
<https://www.unicef.org/innocenti/reports/through-childrens-eyes>
2. OMS Europa, studiul HBSC despre cyberbullying, 27 martie 2024, date pentru 2022.
<https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study>
3. OMS Europa, studiul HBSC despre adolescenți, ecrane și sănătate mintală, 25 septembrie 2024, date pentru 2022.
<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>
4. National Institute of Mental Health (SUA), The Teen Brain: 7 Things to Know.
<https://www.nimh.nih.gov/health/publications/the-teen-brain-7-things-to-know>
5. Salvați Copiii România, studiu despre bullying în școli, comunicat din 18 octombrie 2022.
<https://www.salvaticopiii.ro/sites/ro/files/2023-11/studiu-pest-un-sfert-dintre-copii-au-fost-agresori-jumatate-spun-ca-au-fost-victime-ale-bullying-ului.pdf>
6. Salvați Copiii România, comunicat de presă din 28 martie 2025.
<https://salvaticopiii.ro/sites/ro/files/2025-03/5-ani-a-scazut-pragul-de-varsta-pentru-copii-pe-retele-sociale-avertisment.pdf>
7. Salvați Copiii România, linia esc_ABUZ, comunicat din 10 decembrie 2025.
<https://www.salvaticopiii.ro/sites/ro/files/2025-12/expunere-si-continut-daunator-copii-online-crestere-alarmana-a-sesizarilor.pdf>
8. NCMEC, comunicat despre sextorsiune, publicat pe 25 iunie 2026, date pentru 2025.
<https://www.missingkids.org/blog/2026/ncmec-releases-new-sex-tortion-data-2025>
9. NCMEC, datele CyberTipline, publicate în 2026, date pentru 2025.
<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>
10. NCMEC, Take It Down, întrebări frecvente.
<https://takeitdown.ncmec.org/faq/>
11. Europol, The rise of online cult communities dedicated to extremely violent child abuse, ianuarie 2025.
https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The_rise_of_online_cult_communities_dedicated_to_extremely_violent_child_abuse.pdf
12. eSafety Commissioner (Australia), urmărirea, monitorizarea și hărțuirea fără consimțământ în rândul copiilor, actualizat la 1 iulie 2025, sondaj din decembrie 2024 - februarie 2025.
<https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-non-consensual-tracking-monitoring-harassment>

Surse (continuate)

13. eSafety Commissioner (Australia), Talking to machines, raport publicat în august 2026, sondaj realizat în 2026.
<https://www.esafety.gov.au/research/talking-to-machines-childrens-experiences-with-ai-assistants-and-companions>
14. Europol, ghidul de prevenire despre money muling.
<https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
15. NIST, SP 800-63B-4, Digital Identity Guidelines, august 2025.
<https://pages.nist.gov/800-63-4/sp800-63b.html>
16. CISA, Implementing Phishing-Resistant MFA (fișă informativă).
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
17. Microsoft, Token theft playbook.
<https://learn.microsoft.com/en-us/security/operations/token-theft-playbook>
18. FTC (Statele Unite), Are Public Wi-Fi Networks Safe? What You Need To Know.
<https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know>
19. Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 august 2026.
<https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/>
20. Department for Science, Innovation and Technology (Marea Britanie), Deepfake detection technology, 26 martie 2026.
<https://www.gov.uk/government/publications/deepfake-detection-technology/deepfake-detection-technology>
21. Organizația Internațională a Muncii (ILO), Walk Free și Organizația Internațională pentru Migrație (IOM), Global Estimates of Modern Slavery, septembrie 2022.
<https://www.ilo.org/publications/major-publications/global-estimates-modern-slavery-forced-labour-and-forced-marriage>
22. TVR Info, despre atacul asupra platformei Hipocrate, 13 februarie 2024.
<https://tvrinfo.ro/blocajul-generat-de-atacul-cibernetice-asupra-spitalelor-continua-hackerii-au-cerut-o-rascumparare-de-peste-150-de-mii-de-euro-in-bitcoin/>
23. CNN, despre fraudă deepfake de la Arup, 16 mai 2024.
<https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>
24. Check Point Research, Hacking Fortnite, 16 ianuarie 2019.
<https://research.checkpoint.com/2019/hacking-fortnite/>
25. NBC News, despre recompensa primită de un copil de 10 ani pentru o vulnerabilitate Instagram, mai 2016.
<https://www.nbcnews.com/tech/social-media/facebook-pays-10-000-10-year-old-instagram-hacker-n568026>

Surse (continuare)

26. Google, Ajutor Cont Google: Be ready to find a lost Android device.
<https://support.google.com/accounts/answer/3265955?hl=en>
27. eSafety Commissioner, How to manage money in games.
<https://www.esafety.gov.au/parents/issues-and-advice/gaming/how-to-manage-money-in-games>
28. TRUST // NO TRUST, modulul REAL / FAKE / AI (imagini generate cu AI pentru exercițiu).
<https://www.looksmart.ro/trustnotrust/ro/real-fake-ai/>
29. DNSC, Directoratul Național de Securitate Cibernetică, numărul 1911 pentru raportarea incidentelor.
<https://www.dnsc.ro/>
30. Have I Been Pwned, verificarea adreselor de email compromise.
<https://haveibeenpwned.com/>
31. Ora de Net, Salvați Copiii: helpline și linia de raportare esc_ABUZ.
<https://www.oradenet.ro/linia-de-raportare/>
32. Asociația Telefonul Copilului, cum funcționează 116 111.
<https://telefonulcopilului.ro/116111/afla-cum-functioneaza-telefonul-copilului-116111/>
33. Servicii publice gov.ro, asistență socială și protecția copilului (119).
<https://serviciipublice.gov.ro/servicii?domainSlug=asistenta-sociala-si-adoptii>
34. Edupedu, despre lansarea numărului 119, 5 ianuarie 2022.
<https://www.edupedu.ro/cazurile-de-copii-abuzati-pot-fi-semnalate-la-numarul-de-telefon-unic-national-gratuit-119-numarul-este-corelat-cu-112-si-echipe-mobile-pot-intervenii-imediat/>
35. ANITP, Agenția Națională Împotriva Traficului de Persoane.
<https://anitp.mai.gov.ro/contact/>
36. Sistemul Național Unic pentru Apeluri de Urgență 112.
<https://www.112.ro/>
37. Programul SMART ONLINE = SAFE OFFLINE.
<https://www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html>
38. Platforma TRUST // NO TRUST.
<https://www.looksmart.ro/trustnotrust/ro/>

Despre imagini

Ilustrațiile de capitol provin din materialele cursului SMART ONLINE = SAFE OFFLINE și au fost create cu ajutorul inteligenței artificiale. Capturile de ecran ale unor mesaje frauduloase sunt reproduse exclusiv în scop educațional, pentru a-i ajuta pe cititori să recunoască fraudele. Mărcile și logourile vizibile în ele aparțin proprietarilor lor, care nu au nicio legătură cu mesajele respective. Cele două imagini din exercițiul de la capitolul 8 au fost generate cu AI pentru modulul REAL / FAKE / AI al platformei TRUST // NO TRUST.



Better **safe** than sorry

Ai terminat ghidul. Acum exersează: platforma **TRUST // NO TRUST** te pune în situații fictive, inspirate din riscuri reale, în care decizi singur ce faci.

www.looksmart.ro/trustnotrust

CONTACT

Nicholas Cârstoiu

nicholas.carstoiu@gmail.com · 0743.332.318

www.looksmart.ro/nicholas

Drepturi de autor. © 2026 Nicholas Cârstoiu. Toate drepturile rezervate. Ghidul poate fi descărcat, tipărit și distribuit gratuit, integral și fără modificări, în scop educațional necomercial, cu menționarea sursei. Este interzisă vânzarea, modificarea sau preluarea parțială a conținutului fără acordul scris al autorului.

Despre siguranță. Acest ghid are scop exclusiv informativ și educațional. Respectarea recomandărilor din el reduce riscurile, dar nu garantează protecția împotriva tuturor amenințărilor online, care se schimbă permanent. Ghidul este o cărămidă în educația voastră digitală, nu un înlocuitor pentru discuția cu părinții, profesorii sau specialiștii. În orice situație de pericol, contactați imediat 112 sau serviciile de ajutor din capitolul 10.